Digital Transformation in the Cloud

What enterprise leaders and their legal and compliance advisors need to know

Foreword by Julie Brill and Rich Sauer


Microsoft

Table of contents

Technology is transforming the world

Foreword

Wherever you look, technology is transforming the world. Our jobs require us to travel constantly, and we see it every day. One of us leads a global team of 350 commercial lawyers and public policy professionals at Microsoft. The other is a former Commissioner at the U.S. Federal Trade Commission who now oversees Microsoft's global privacy and regulatory compliance efforts. We spend our time on the road listening to policymakers and regulators, business and technology leaders, researchers and academics—and of course our customers. The people we meet hail from many nations. Yet they nearly all express the same high degree of both excitement and uncertainty about the social and economic impact of technological change.

In this moment of profound technology-driven change, people everywhere are inspired by the promise of a new generation of innovations unleashed by cloud computing, Artificial Intelligence, the Internet of Things, universal network connectivity, and a host of other developments. For organizations of every size, the potential impact of digital transformation on strategy and operations is palpable. Deeper knowledge of customers. Access to new markets. Fresh ways for employees to share ideas and work in collaborative teams. Increased efficiency. Better protection of proprietary information and the privacy of customer data. And last but not least, a dramatic acceleration in the pace of research, development, and innovation. These are just a few of the benefits organizations and businesses are experiencing as they work in partnership with cloud leaders like Microsoft to build a new kind of IT infrastructure, one that is more powerful, more flexible, and more scalable than its predecessors.

But it's also apparent that the leaders we meet have many important concerns and questions about the new challenges they face. Privacy, security, trust, compliance with new regulations, corporate social responsibility—these deeply interrelated issues have all come to the fore as we move ahead in the cloud era. The choices companies make as they explore the opportunities and risks of digital innovation will have a long-lasting impact on their ability to create value and thrive in an ever more competitive global market.

In times of great change, it is natural that policymakers respond with new policies and legislation. One prominent example of a policy response to the present wave of technological change is the European Union's new data protection law, the General Data Protection Regulation. Set to go into effect in May of this year, the GDPR is likely to affect the way nations and businesses approach privacy all over the world, not just in Europe. It is already driving organizations to rethink the way they work with personal data in order to comply with the new requirements. We believe the GDPR is an important step forward in the global effort to protect individual privacy, which is both a prerequisite for trust in technology and, more fundamentally, an essential human right.

Microsoft is fully engaged in driving the technologies that power digital transformation. At the same time, we seek to address the policy, regulatory, and ethical issues these technologies raise. Achieving the highest compliance with data protection laws and standards for ourselves and for our customers is a long-standing priority. In the United States, for example, we were the first major cloud provider to take the steps needed to enable our customers to comply with demanding data protection regulations in healthcare and law enforcement. We have pursued similar efforts in every market around the world, and we strive to offer the largest possible

portfolio of global standards and certifications. Our engineers are building advanced legal compliance, privacy protection, and data security features into our cloud services to ensure that our customers can meet the requirements of GDPR and other emerging regulatory regimes. Our legal and policy experts and privacy and security specialists are working to help companies around the globe adapt to a complex and ever-changing regulatory environment.

This book is designed to provide enterprise leaders and their legal and compliance advisors with a framework for thinking about the strategic implications of digital transformation. Our goal is to help you understand the steps you can take to seize the opportunities that lie ahead, while minimizing the risks. This book also reflects more than three decades of knowledge and experience Microsoft has gained as a pioneer in the development of transformational digital technologies, as a partner to businesses large and small, and as an enterprise that itself must continually respond to the changing needs of customers in a world that is forever being reshaped by innovation.

Julie Brill
Corporate Vice President & Deputy General Counsel,
Privacy & Regulatory Affairs

Rich Sauer
Corporate Vice President & Deputy General Counsel, International
Corporate, External, & Legal Affairs

Acknowledgments

As with most research of this nature, it is the product of contributions from a broad range of subject matter experts and talented individuals across the company. The overall project was led by Michael McLoughlin of Microsoft Corporate, External, and Legal Affairs. Jeff Gould was the primary researcher and Bill Miller led the design and layout. Other notable contributors include but are not limited to Rich Sauer, Julie Brill, Neal Suggs, Dominic Carr, Tom Burt, Jeff Bullwinkel, John Seethoff, Carolyn Frantz, Melvin Flowers, John Galligan, John Payseno, Andrea Simandi, Lesley Kyd-Rebenburg, Dale Waterman, Michelle Lancaster, Alison Howard, Craig Shank, Alex Li, Gregg Brown, Laura Ruby, Tina Ying, Nicolas Schifano, Sanjay Batra, Geff Brown, Doug Miller, Karin Fletcher, Jeorjina Tegel and Charlyne Fabi of Right Hat.

Introduction

Security, privacy, and compliance in the cloud-first enterprise

Today no enterprise is an island

We live in a time when enterprises large and small are racing to transform themselves with unprecedented new technologies. In every region and country of the world, organizations of all kinds are striving to create more value than ever before for customers, shareholders, employees, citizens, and society at large. Cloud computing, mobile devices, software-based intelligence, universal access to information—these digital technologies are remaking enterprises, government, nonprofit organizations, and the everyday lives of the billions of citizens of planet Earth.

As enterprises instill ever more intelligence into their business processes and automate more tasks, their leaders must grapple with profound existential questions. What is our true purpose as an organization? How do we create more value? Are we doing all the things we should be doing, and only those things?

Today, no enterprise is an island. The days of Henry Ford's magnificent River Rouge plant—a mile-long complex where coal, iron ore, sand, and rubber went in one end and finished automobiles drove out the other—are gone forever. Every enterprise today must focus on the activities it does exceptionally well—and delegate those it does not. Automobile plants no longer make everything under one roof as River Rouge did, relying instead on vast global supply chains linking thousands of suppliers into an orchestrated whole. Ford's leaders today are as preoccupied with software as they are with steel. Indeed, a leading economic journalist has recently written that "Today, automobile manufacturing is first and foremost a software business, as opposed to an industrial operation."[1]

The question of what to delegate and to which partners has become strategic. The benchmark for any value-creating activity is the

market. The enterprise that chooses to keep an activity in-house is saying it can match the best in the world in this activity. The cloud computing revolution is driven by the realization among enterprise leaders—from Fortune 50 behemoths to agile startups—that IT infrastructure and broad business software functions are no longer part of their core value-creating mission.

But delegation inevitably raises questions of confidence and trust. An automobile manufacturer may choose to buy steel and glass and specialized components from outside suppliers. Yet if this supply of vital raw materials is interrupted, if the components prove unreliable or even dangerously defective, the act of delegation can damage or even destroy the enterprise.

Cloud computing means entrusting to partners the critical activities of information processing and dissemination, activities that are as vital to the enterprise as the pumping of blood is to living organisms. The cloud therefore demands a new foundation of trust between cloud service providers and their customers.

This foundation stands on three pillars: security, privacy, and compliance. Data must be secure from deliberate and accidental disclosure or loss. The privacy of all individuals—customers, employees, patients, students, citizens—must be protected. National and international laws governing the use and protection of data must be complied with, as must regulations and standards applicable to specific industries.

We are lucky to live in a time when technology offers unprecedented opportunities for economic and social progress. But it is also a time of heightened risk. While cloud and other technologies such as machine learning surge forward, new dangers have arisen that

Today no enterprise is an island

threaten the stability and safety of our modern technological infrastructure and the better society we hope to build on it. Governments around the world are responding to these threats with new legislation designed to protect privacy and cybersecurity, as we discuss later in this book. But we in the technology sector acknowledge that we must stand in the front line as first responders to these threats. It is our duty to help not just our own customers, but all who rely directly or indirectly on our technology.

This document is intended as a strategic road map to secure, privacy-protecting and compliant cloud computing for enterprise leaders together with their legal and compliance advisors. We review key strategy issues and examples of the challenges that enterprises face as they pursue digital transformation while striving to protect all stakeholders.

At Microsoft, our mission is to empower every person and every organization on the planet to achieve more. We cannot think of a greater contribution to this aim than to provide a cloud computing platform that is safe and productive not only for our customers, but for all whose lives it touches.

Chapter 1

The cloud and value creation

From Diego Rivera's Detroit industry murals, 1932–1933[2]

The past and future of industry

In 1915, Henry Ford bought a 2,000-acre tract of marshy land along the River Rouge, a minor tributary of the Detroit River. For several years Ford seemed to have no clear purpose for the tract. At one point he considered making it a sanctuary for wild birds. During WWI, an early factory on the site made anti-submarine boats for the U.S. Navy. After the war, it made tractors.

But by the mid-1920s, Ford had another, much bigger idea: River Rouge would become the largest, most integrated automobile plant in the world. The first Model A rolled off Rouge's assembly line in 1927. A decade later, Rouge had achieved Ford's goal. It was the largest industrial complex ever built in the United States, employing 110,000 workers and producing 4,000 cars per day.[3]

What made River Rouge extraordinary, beyond its sheer scale, was its unprecedented degree of vertical integration. Rouge made virtually everything it needed within its own walls. Iron ore, coal, sand, and other raw materials went in one end of the mile-long complex, and finished automobiles drove out the other. It was said that from the time a lump of iron ore went in and a Model A made from the ore emerged, less than 48 hours passed.

Rouge made its own steel, glass, and tires. The rubber for the tires came from Ford-owned plantations in Brazil. It made its own shock absorber fluid from sugarcane and its own paint from flax oil. Its iron ore and coal came from Ford-owned mines and were transported on Ford-owned ships and railroad lines. Wood used as paneling and dashboards came from Ford-owned forests and sawmills. Rouge even had machines for grinding soybeans (grown on Ford-owned farms) and making them into gear shift knobs. Rouge also generated its own electricity, producing enough power for a city of 500,000 inhabitants.

Ford River Rouge, aerial view, 1940

Rouge's extraordinary vertical integration had many advantages in Ford's eyes, some real, some only perceived. Like most corporate practitioners of this mode of industrial organization, Ford believed that he could produce the parts and materials that went into a car at less cost than independent suppliers. Also important was his conviction that, by owning and controlling key parts of his supply chain, he could prevent interruptions in the flow of raw materials and components to his factories. Such interruptions had plagued the automobile industry in its early years, even forcing some smaller producers into bankruptcy.

But not every upstream activity that Ford sought to control was profitable. Some lost money, and others proved difficult to manage.

The rubber plantations in Brazil were a particular sore spot. Ford lost $20 million on them from 1927 to 1945, and after WWII he sold them to the Brazilian government.[4] It turned out that buying tires from outside specialists like Firestone and Goodyear was a more profitable way of doing business.

River Rouge represents the culmination of the vertical model in industrial and corporate organization. At its high point in the middle of the 20th century, it made the most effective use of then-existing technologies and can plausibly claim to have been the best model possible for its time. General Motors also pursued vertical integration, although it did so by a different route, acquiring existing suppliers and their factories rather than locating all production under one gigantic roof.

The rise and fall of vertical integration in the American automobile industry is one of the most interesting stories in business history. By the late 1960s the vertical model that had allowed GM and Ford to dominate the industry began to show serious signs of infirmity. Over the next 25 years, less integrated Japanese manufacturers, who had mastered the art of cooperating closely and profitably with a myriad of outside suppliers, seized a large share of the U.S. giants' home market.

By the 1990s, Ford and GM knew it was time to unbundle their in-house parts manufacturing into independent companies. They had reached the painful conclusion that vertical integration had caused them to fall behind their Japanese competitors in both quality and cost of production. The flaw of the vertical model was that it was difficult to reliably benchmark internal operations against the best that a competitive open market could offer. In the words of a leading historian of the industry, "Sheltered from

competition, the parts operations of Ford and GM were widely reckoned to be inefficient money losers."[5]

A century after Ford purchased the River Rouge tract, the automobile industry is organized on utterly different principles. Vertical integration has given way to vast worldwide supply chains managed by software that knits together the activities of thousands of specialized independent firms. Venture capitalist Marc Andreessen popularized the slogan "Software is eating the world" less than a decade ago. But in reality software has been transforming the automobile industry's supply chains since at least the 1980s, when Ford and its rivals began buying thousands of PCs to model business processes with spreadsheets.

Today, the leading global manufacturers still stand at the head of the supply chains, and they still build cars in their factories. But only a small portion of the components and raw materials that go into their cars are produced from scratch by the manufacturers themselves. And the flow of those components and materials into and within the factories is directed by highly sophisticated software systems without which nothing could be built. In the words of journalist Ryan Avent of The Economist, "It would have been nearly impossible for rich Western firms to manage the sprawling global supply chains that wrapped around the world over the last twenty years without powerful information technology."[6]

Design, systems integration, and brand management are now every bit as important to the success of the big auto firms as cost-efficiency and quality control on the assembly line. Indeed, for a company like Ford, the future is likely to depend more on its ability to make the software that pilots self-driving cars than the steel (or carbon fiber) used in their frames.

"It is fascinating to see how this iconic American company with a rich heritage of innovation is using digital technology like mixed reality, AI and the cloud to transform and innovate for the future."

—Satya Nadella, CEO of Microsoft, on a visit to Ford in August 2017

The key lesson to be learned from the evolution of the automobile industry is that the place where enterprises can create the most value—and earn the most profit—changes as their organizational forms change. And those forms are determined by the technologies used to build the organizations. The shape of an auto manufacturer today is profoundly different than in Henry Ford's era, because it is determined by the computing and networking technologies of the 21st century.

Today market forces demand—and technology permits—firms to delegate to partners activities where the partners can create more value than the firms themselves. To survive and thrive, today's enterprise must discipline itself to focus only on those activities where it can rival or surpass the best in its field.

In this book we hope to demonstrate that an enterprise's ability to create value—for shareholders, customers, employees, partners, and society at large—depends more than ever on making the right decisions about which activities to delegate to others and which to retain in the core. We believe that cloud computing, which offloads critical IT infrastructure and information processing tasks to partners, offers a strategic opportunity for enterprises of all sizes to

digitally transform themselves and drive their core value creation to new heights.

Microsoft's global network of cloud data centers, depicted on the following two-page spread, represents an investment whose scale far surpasses Henry Ford's River Rouge. But unlike River Rouge's vertical integration, which sought to perform every task under one roof, Microsoft's cloud is built for a world where organizations are specialists. Our cloud offloads the management of complex IT infrastructure from enterprise customers and provides them with new tools (such as data analytics and machine learning) to pursue the kinds of value creation they do best.

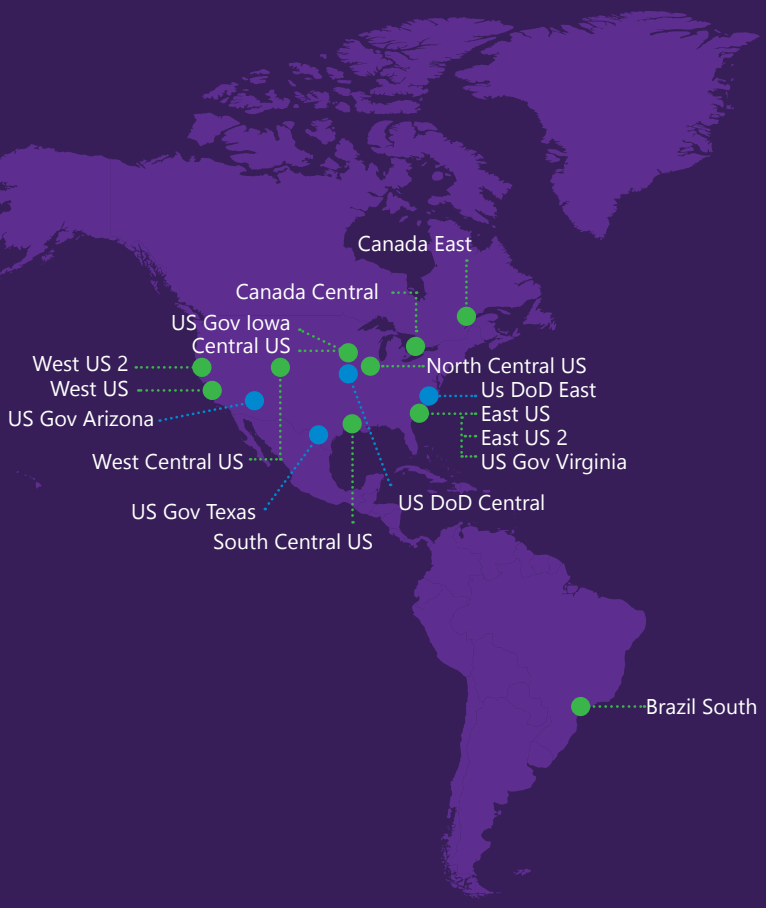
Digital disruption and the focus on value

The first modern hotel chains arose in the period between the two world wars. Hilton was founded in 1919, Westin in 1930, Sheraton in 1933. The chains grew slowly during the Depression years, driven mostly by acquisitions of existing properties. This was a business of small-scale, opportunistic real estate speculation. The brands were little known, and the vast majority of hotels in the world remained in the hands of individual owners.[7]

After WWII, things accelerated. Exploiting the rise of affordable long-distance telephony, Hilton and Westin launched the first centralized hotel reservation systems in the late 1940s. A decade later, Sheraton launched the first reservation system based on the primitive new electronic computers. The brands began to internationalize and became more upscale, opening flagship properties in major cities around the world. They also continued to experiment with computers throughout the 1960s. By the 1970s, the ability of mainframe-based reservation systems to boost occupancy was becoming a key competitive advantage for the chains over independent properties.

Microsoft's global cloud data centers

- Generally available
- Coming soon




North Europe
UK South
West Europe
Germany Northeast
Germany Central
France South
UK West
France Central
Korea Central
Korea South
China North
China East
Japan East
Japan West
East Asia
West India
Central India
South India
Southeast Asia
Australia East
Australia Southeast

By the 1980s, the big chains dominated the industry, capturing an ever-increasing share of business and vacation travel. But as the industry matured, a surprising new variation on this model emerged. The chains realized that the key to their ability to create value lay in their brands and their reservation systems, not in the ownership of brick and mortar. They discovered that it was not actually necessary to own hotels to be global leaders in the hotel business. They began to offload ownership of many of their properties to investors who specialized in real estate. Doing so allowed the chains to invest more in their core value-creating activities and grow their size and profits faster.[8]

This shift in the chains' original model was made possible by (among other things) the dramatic growth in power of transaction-processing mainframes and in the efficiency of the networks that connected them to thousands of reservation terminals in travel agencies around the world. The new model powered the chains to decades of growth and continues to sustain them today.

But the march of technology has also continued, and it has spurred the invention of new business models. In October 2007 a pair of young San Francisco entrepreneurs had an idea that would challenge the global hospitality industry in an entirely new way. Airbnb, the company they founded the following year, now offers more than 3 million lodgings for rent via its Internet-based reservation system.

Their idea was simple: the most scalable value-creation model for the lodging business is to not have any hotels at all. They had no need for complex franchising deals with independent investors who poured billions into real estate. They had no need to hire armies of young hotel school graduates to staff far-flung properties, nor did they need complex, expensive mainframes.[9] Instead, they built a free-standing web reservation system, based entirely in the cloud,

that could serve as a trusted intermediary between hundreds of thousands of individual lodging owners and many tens of millions of consumers. Without the power provided by the cloud to ramp up a brand new reservation system from zero to global scale in just months, it would never have been possible for an upstart like Airbnb to challenge the established giants of the lodging industry.

New technology by itself does not create business innovation. But it creates opportunities for innovation that can reshape entire industries with remarkable speed. Today the major hotel chains are not standing still in the face of Airbnb's challenge. While Airbnb has built its franchise on cost-conscious leisure travelers, groups like Marriott and Hyatt are differentiating through their superior ability to serve higher-spending business travelers and upscale vacationers. They are not only revamping their mainframe reservations systems with Internet-era software,[10] they are also using technology to transform the customer experience—for example, by plotting to do away with the hotel front desk altogether in favor of smartphone check-in apps.[11] They are also using the cloud to valorize their large workforces. Hyatt, for example, has given cloud email addresses to tens of thousands of deskless workers on its premises.[12]

This brief history of the hotel industry shows how the basic technological building blocks firms are made from determine in large measure the value-creation strategies available to them. Introduce new building blocks, and you change the kind of firms that can be built and the ways in which they can create value. Often, when one player in an industry leverages a new technology to transform their business, the other players have little choice but to adopt the same technology or try to leapfrog the innovator with an even more productive innovation. The lesson is always the same: innovate or die.

Digital transformation and the cloud

We live in a period of turbulent technological change where new strategic options are opening up for enterprises with extreme and surprising rapidity. **The power of the cloud is that it allows organizations to focus on their areas of greatest competitive advantage, while delegating capital-intensive and hard-to-manage IT infrastructure to specialists who are the best in the world in that domain.**

Cloud customers and cloud providers are co-evolving in a global economy that pushes all participants to become best-of-breed specialists. Ford and its competitors will strive to make the smartest and most efficient vehicles; Airbnb and the hotel chains will fight for the lodging budgets of the world's travelers; while Microsoft and Amazon will compete to build the most intelligent and productive cloud services for the Fords, Airbnbs, and hotel chains of the world, and for countless other industries pursuing their own digital transformations.

The world's top three cloud providers—Amazon, Microsoft, and Google—invested $30 billion in their cloud data centers in the last year alone.[13] The economies of scale and scope flowing from these investments are immense and almost certainly impossible to match.

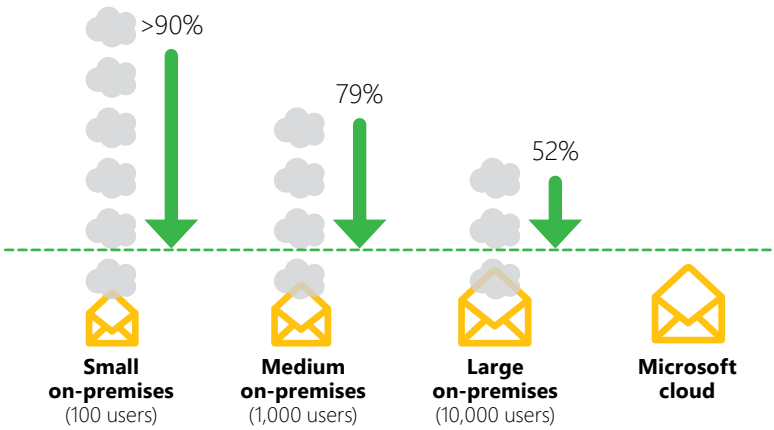
The efficiency derived from cloud computing is more than merely financial: the great cloud data centers are also far more efficient in their use of energy. A recent comparison by Accenture of energy utilization by Microsoft cloud applications and conventional enterprise data centers shows that the cloud uses much less energy and emits much less carbon than equivalent on-premises applications.

"Each year, Microsoft purchases about 10% of all the chips that go into servers in the world."

—Brad Smith, President and Chief Legal Officer of Microsoft

Comparison of email carbon emissions

cloud-based vs. on-premises



The cloud is much more energy-efficient and friendly to the environment than conventional enterprise data centers. A comparison by Accenture of energy utilization by Microsoft cloud applications and conventional enterprise data centers shows that the cloud produces much less CO2 than equivalent on-premises applications: More than 90% less for small deployments of about 100 users; 60% to 90% less for medium-sized deployments of about 1,000 users; 30% to 60% less for large deployments of about 10,000 users.[14]

But the cloud is no longer just about the most efficient use of dollars and kilowatt-hours. It is also about three other key advantages that the cloud giants have gained by virtue of their specialization and can now share with their users.

The first key advantage cloud providers gain from their specialization is the speed of innovation. The early cloud services of a decade ago were simple affairs. They offered the ability to launch "virtual machines" on demand in a remote data center operated by the cloud provider. These virtual machines behaved just like real servers and could run real applications. But because multiple copies of them could be stacked on the same physical server or spawned to new servers, they made it possible for enterprises to treat the flow of compute power just like any other utility service that could be turned up or down according to the needs of the moment. The early cloud services offered few options other than basic virtual machines. They were very much in the "take it or leave it" mold of Henry Ford's Model T: "You can have any color you want, as long as it's black."

Today's cloud services have come a long way from these rudimentary beginnings. The cloud offerings of a Microsoft or an Amazon are now vast catalogs containing dozens of major services and hundreds of sub-variants, all of which can be tuned in real-time to meet precise customer needs.[15] The services are far more complex than simple virtual machines, ranging up the entire "software stack" from basic operating systems to middleware, databases and "data lakes," machine learning and analytics tools, and fully finished applications that users can run off-the-shelf.

The cloud giants have thousands of engineers continually developing new services and options, which are rolled out to customers on an almost weekly basis. In an environment like this,

few if any internal enterprise IT teams can keep up. If those teams attempt to compete with the cloud providers at every level of the stack, they risk falling further and further behind on the innovation curve.

The best use and true mission of in-house IT teams is to build the applications and business logic that drive your firm's distinctive value-creating activities. That mission should not be to manage the ever-more-complex and constantly changing infrastructure needed to operate your value-creating applications.

The second key advantage of the cloud is safety. A cloud service like Microsoft Azure is made up entirely of new code, built with the latest and most rigorous development methodologies. Security and privacy are designed in from the ground up.[16] New code is safer than old code. And new code that is constantly revised and tested by thousands of cybersecurity experts is safer still.

As a global cloud provider, Microsoft invests more than just financial capital in its data centers. We also invest unmatched human resources. At present, we employ 3,500 cybersecurity experts, and we are hiring more every day.

Our safety advantage also comes from the vast and unparalleled volume of data that passes through our services. As we explain in later chapters on cybersecurity, as a global cloud provider we see far more "bad things" on the Internet than even the largest enterprise can on its own. This makes us better able to defend against those threats.

The third key advantage of the cloud is the knock-on benefit users get from our unrivaled investment in compliance with

laws, regulations, and standards for data protection. As we will describe in later chapters on privacy and compliance, we have hundreds of engineers working full time on meeting the requirements of Europe's General Data Protection Regulation. We have hundreds more working to ensure our compliance with a wide range of other regulations from every region of the world. We also have the largest portfolio of international standards certifications of any cloud provider.[17] Of course, we're not doing this compliance work just for ourselves, but also for our customers who use our software and cloud services.

Digital transformation does not consist in simply shutting down your data center and moving your IT operations to the cloud. Of course, such a migration will save costs and make it easier to launch strategic new applications quickly. For the majority of business organizations today, the cloud is likely the right course to take. But the cloud by itself will not transform your business. What transforms your business is leveraging the externalization of activities that are not part of your core value creation process to concentrate on those that are. If you do not use the opportunity afforded by cloud migration to improve your primary value creation activities, you are missing the essence of digital transformation.

Digital transformation requires the relentless unbundling of value-creating activities from value-consuming activities. But activities that consume value in one organizational and market context can create it in another. One firm's cost center can be another firm's core competence. In these circumstances, firms that retain their IT cost centers must make them competitive with the best that the market can offer—or risk losing ground to more focused competitors.

Digital transformation sometimes leads to the opposite of unbundling. Dropbox, another digital disrupter founded around the same time as Airbnb, spent the first eight years of its life as an all-cloud company, running its pioneering data storage service entirely on Amazon Web Services.[18] But with 500 million users, Dropbox ultimately decided it had the scale to match the cloud giants and by 2016 had migrated nearly all its data from Amazon to its own cloud data centers. Nevertheless, such examples are rare.

"Cloud-first strategies are the foundation for staying relevant in a fast-paced world."

—Ed Anderson, Research VP at Gartner

Today, when companies contemplate their internal IT infrastructure, they must ask themselves: Do we really want to compete with Amazon, Microsoft, and Google? Can we be as efficient in the use of capital as they are? Can we match their depth of human expertise? Can we be as secure and compliant as they are? Can we match the scale not only of their physical infrastructure, but of the data they accumulate and the broader insight it gives them into what new innovations are worth exploring?

The answers to these questions will help you chart the course of your digital transformation.

Cloud delegation and a new framework for trust

Around the year 1300, the Northern Italian city of Florence was one of the largest in Europe. Its population of something over 100,000 surpassed both London and Paris. It was also very likely the richest city on the continent. Its economy was built on two great industries: fine woolen cloth and merchant banking. Of the two, the latter was largely a Florentine invention developed by trial and error over the course of the previous century.

Both industries involved long-distance trading networks where the outcomes of transactions were uncertain. Both industries, but especially banking, required the emergence of a new institutional framework of laws, accounting methods, and mechanisms for enforcing contracts. They also required a new kind of trust between business partners who were no longer always united by blood ties.

Long-distance trade had been a cornerstone of the ancient world, but the networks that crisscrossed Europe and tied its scattered regions to each other and to the opposite shores of the Mediterranean disintegrated with the fall of Rome. It took nearly a thousand years for them to revive.

Although largely an extension of commerce, Florentine merchant banking was—in contrast to trade—an innovation that represented a radical departure from the ways of the ancient world.[19] Starting from closely held family firms, banks in Florence and other Northern Italian cities evolved into more elaborate associations of partners who drew up written agreements among themselves. A host of innovations in contract law arose to accompany the new firms, and the same thing happened in accounting. Double-entry bookkeeping, which spread rapidly through the region around the turn of the 14th century, was an early example of the power

of standardization, a precursor to much more complex modern conventions such as the Generally Accepted Accounting Principles (GAAP).

To supervise the application of these new tools of commerce, entire populations of specialists sprang up. Florence's neighbor and banking rival Bologna, celebrated for its law school, counted no fewer than 2,000 professional notaries among its 50,000 inhabitants.[20] These specialists were precursors to the modern community of legal and compliance experts that guide enterprises through the thickets of today's sprawling regulatory regimes.

Throughout history, new forms of trade and new kinds of business partnership have required new laws and new standards. Today's cloud revolution is no different in this respect than the merchant banking revolution of medieval Italy.

When an enterprise delegates critical activities that were once part of its core to partners, trust is essential. When the form or manner of the delegation is different than those previously known, a new kind of trust may be called for. We believe this is the case with cloud computing.

An enterprise that migrates all or a substantial portion of its IT infrastructure to the cloud is making what could be a make-or-break decision. What would happen if the software that runs all of a firm's operations and financials were wiped out in an hour? What would happen if a firm lost its entire customer database and the personal information of millions of consumers to cyberattackers? What would happen if thousands of patient records held by a hospital chain were leaked? What if all the account balances of a global bank were posted on a rogue website? Could any of these organizations survive such catastrophes?

Cities have business models too

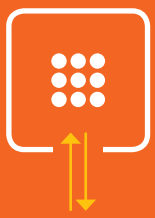
Technology determines an organization's shape and mode of value creation

Medieval town of Dubrovnik, Croatia

Originally a marketplace protected by walls

Usually situated on a river, port or crossroads for transportation of goods and raw materials

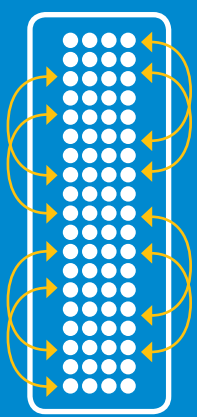
At first transacts mainly with its hinterland, but may gradually specialize its production and develop far-flung trading networks



20th century Manhattan skyscrapers

Skyscrapers made possible by new technology (steel, electricity, high-speed elevators) permit firms to build large governing bureaucracies that supervise transactions on a national scale

Densely packed buildings in a tight urban perimeter permit high bandwidth interactions between these corporations and their peers, partners and suppliers



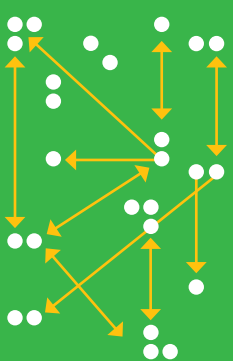
21st century Silicon Valley

Large firms disperse into sprawling suburban campuses linked by road networks

Loosely packed regions specialize, with many similar peers competing and interacting

Information exchange is largely electronic and virtual

Trading networks and supply chains are global



Disasters on this scale are fortunately rare, but they are not impossible. **However, there is no evidence to suggest that such disasters are more likely to happen in the cloud than elsewhere.** In fact, we firmly believe the opposite is true: your data and your applications are likely to be safer in the cloud than in your own data center. But we know you can't take our word for it. Indeed, you should not. Proofs of many kinds are required.

The new delegation model of cloud computing requires a new framework of trust to govern relations between cloud users and cloud providers. The functions provided by the cloud provider are critical to the survival of the enterprise. Even short-term disruptions or minor breaches can have serious consequences. A massive breach or a long-term disruption could cause an enterprise to go under. Yet the same is true of other vital services provided by outside suppliers, for example, energy, banking, transportation, and telecommunications. The difference is that cloud services are embedded in much deeper and more intricate ways in the enterprise's own business processes.

In the 21st century we are witnessing the gradual emergence of a global, or at least multinational, legal framework to regulate transactions and trust on the Internet. The European Union's major new privacy law known as the General Data Protection Regulation (GDPR—which we discuss at length in Chapter Three) is the first but certainly not the last example.[21] Trust is central to Microsoft's mission to empower every person and every organization on the planet to achieve more. We take a principled approach to building trust, with strong commitments to privacy, security, and compliance. In the rest of this book we discuss these three pillars of the new framework of trust called for by the cloud revolution.

A cloud safe for business

The three pillars of the new framework of trust required by the cloud revolution are security, privacy, and compliance. But these pillars do not exist in isolation. You cannot have a cloud that protects privacy without a cloud that is secure. You cannot have a lawful cloud without compliance—and without the rule of law there can be neither privacy nor security.

Enterprises, nations, and individuals have become profoundly dependent on computers and computer networks. We live in a globally connected world where nearly every economic transaction and an ever-growing share of social interactions depend on the electronic processing of information. Threats to the security, privacy, or legality of our information processing systems are also threats to our economic prosperity, our national security, and our personal safety.

"Almost every form of bad human behavior in real life ultimately makes its way into cyberspace. The good news is there are solutions. Technology is getting better. Business processes are getting better."

—Brad Smith, President and
Chief Legal Officer of Microsoft

At a time when our IT dependency grows deeper by the day, the networks and IT systems of enterprises and governments are under relentless, unprecedented assault from hostile actors. In most cases, these actors no longer fit the outdated stereotype of rebel-without-a-cause teenage thrill-seekers. Over the past decade, they have morphed into ruthless criminal syndicates and rogue nation-states whose aim is to steal or even destroy their victims' vital information assets.

At the same time, the value that our IT systems and the global Internet deliver to society has never been greater and will continue to grow for the foreseeable future. Abandoning or artificially restricting the use of these marvelous tools of human fulfillment and freedom from want is out of the question. We must do everything in our power to make them safer. That is what the following chapters are about.

Jumping from kerosene to solar power with the cloud

When we hear the phrase "digital transformation," we may think most readily of giant corporations or sophisticated startups building new business models with advanced technology. But the most profound kind of digital transformation is one that utterly transforms the lives of people who until now have lived in a pre-digital world. Indeed, a striking characteristic of digital technology is that it allows less developed societies to leapfrog older technology and catch up with richer societies in far less time than it took those societies themselves to reach their present level.

According to the World Bank, about three quarters of the people in Sub-Saharan Africa still lack electricity in their homes. Yet roughly half of these people have mobile phones and that share is growing rapidly. Therein lies a problem—and an opportunity. M-KOPA Solar, a remarkable startup based in Nairobi, is bringing solar power to 2.5 million East Africans with a business model built entirely on the cloud.

Operating out of 100 regional agencies, M-KOPA's sales force of 1,500 agents trawls the countryside in Kenya, Uganda, Tanzania, and Ghana selling compact solar kits to individual households. For a deposit of $35 and a daily fee of 50 cents (roughly what many already spend on kerosene lighting), buyers acquire the means not only to charge mobile phones and other small devices, but to light their homes with electricity for the first time. Instead of using cash, M-KOPA customers pay their bills with electronic payment apps from local telecom companies.

"We are a mix of a micro-finance, technology, and energy company wrapped up in one."

—Jesse Moore, Co-founder of M-KOPA

Also remarkable is the IT infrastructure that allows this startup to manage a large number of employees, customers, and physical devices scattered over a vast swath of East Africa. Virtually all of the firm's finance, supply chain, and field sales operations and even regulatory compliance reporting run in the cloud with Microsoft Dynamics 365.

Chapter 2

A secure cloud

Understand the true nature of the threat

What you should know

Cybersecurity is a greater challenge than ever for enterprises and their leaders. Evidence for this proposition is all around us. It is found most obviously in the seemingly unending series of breaches and hacks that some of the world's most prominent companies and government agencies have fallen prey to in recent years: Equifax, Sony, the U.S. Office of Personnel Management, South Korea's Defense Data Center, the U.S. National Security Agency, Yahoo, Maersk, and many others, doubtless including more than a few organizations whose names have been withheld from the public.

But the challenge is also reflected in the bewildering proliferation of new technologies designed to protect against cyberattacks. Which is more important—intrusion detection or data loss prevention? What is the difference between threat analytics and threat protection? What does a Security Intelligence and Event Management system actually do? Are firewalls obsolete?

The answers to these questions are not as clear as they should be. The speed of innovation in security technology, like a flood of uncorrelated alarm signals arriving in a network control center, can cause information fatigue in leaders charged with charting a safe course through the cyber-jungle.

Cybersecurity threats come from four main types of actors. The four types are very different, and the mix is evolving rapidly.

We are all familiar with the first type from tabloid news and Hollywood movies: the rebellious teenager who conducts cyberwarfare from his parents' basement, until the day the FBI shows up on the doorstep. Such hackers still exist and no doubt will always exist,[22] but they represent a small and declining share of the most dangerous attacks.

The next type of cyberattacker is the professional criminal or—more commonly—the organized criminal syndicate. These hackers are in it for the money, and while they can strike anywhere, they tend to be concentrated in regions of the world where the rule of law is weakest.

The third kind of attacker—and at present the most dangerous—is the rogue nation-state. North Korea's highly destructive attack on Sony Pictures is a textbook example of this phenomenon.[23]

The fourth kind of attacker is one that has fortunately not often yet struck in cyberspace, but has the potential to wreak havoc—we mean terrorist groups like ISIS or Al Qaeda.

> **"90% of all cybersecurity intrusions begin with a phishing email."**
>
> —Brad Smith, President and Chief Legal Officer of Microsoft

This grim menagerie of cyberattackers may give the impression that effective cyberdefense is hopeless. But this is not so. The most important fact about cybersecurity that enterprise leaders should know is that it is, to a much larger extent than they may realize, within their power to ward off even the most dangerous cyberattacks.

The key is to recognize that **nearly all successful attacks start from avoidable human errors** made by well-intentioned employees (or those of partners or suppliers). Here are some examples of such "cyberattack gateway" errors:

- A user clicks on a link in a phishing email or on a malicious website
- An executive uses a USB thumb drive handed out at a conference, unaware that it has been preloaded with malware that infects his machine
- An IT administrator forgets to set a password on a critical piece of software or hardware, or fails to restrict access rights to a sensitive database
- An employee fails to encrypt a spreadsheet full of passwords stored on a shared server
- A laptop with personal information about employees or customers is stolen from a car
- A call center operator is persuaded by a caller's "sob story" to reset an account password despite the caller's lack of adequate credentials
- An IT organization fails to patch known security vulnerabilities in the software it uses, or grants expansive system administrator privileges to more individuals than the strict minimum necessary

These examples show that security is first and foremost about enterprise culture. To reduce both the risk and the consequences of a successful cyberattack, you must gain control over the elements in your culture that make you vulnerable. You must train, cajole, and warn employees to recognize and avoid actions that can open the

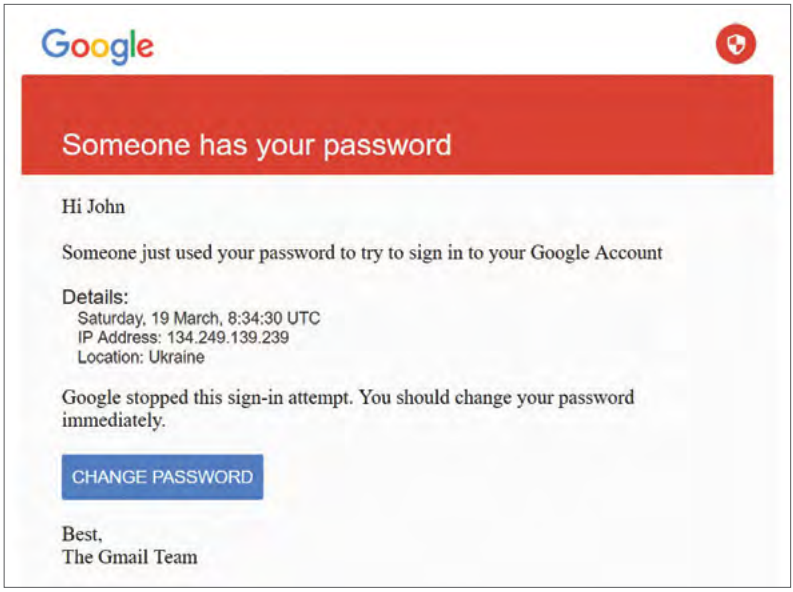
door to a cyberattack. This is not a simple task that can be accomplished overnight. But it is doable.

What is "phishing"?

A "phishing" attack is the use of a fraudulent email to trick the recipient into doing something that helps the hacker, such as disclosing his or her logon credentials (user ID and password) to the hacker or downloading malware that the hacker will later use to steal data. Phishing emails are crafted—often very carefully—to look like they come from a legitimate sender making a legitimate request.

Some phishing attacks are known as "spear phishing" and are designed to target a specific individual using information the hacker has gathered about that individual. Other phishing attacks are more generic and are sent in identical form to thousands of targets at the same time.

A nearby example shows a screen capture of a phishing email similar to one sent to John Podesta of the Democratic National Committee in March 2016. Note that although this message pretends to be from Google and bears Google's logo, it in fact emanated from unknown hackers who had nothing to do with Google. The email states that the victim's Gmail password has been compromised. It then urges the victim to click on a "change password" link that leads to a fraudulent website designed to look like an authentic Google site. Once the victim's credentials have been harvested on this site, they can be used to access the victim's account and intercept or download emails.



Example of an actual phishing email[24]

What you should do

Companies should adopt the following policies and actions to build a cybersafe culture in their organizations:

Require a unified security strategy that is applied by—and applies to—all. Encourage innovation and learning, but don't let business units or individuals improvise security policies in isolation.

While startups may embrace an all-cloud approach from the start, most large existing organizations—even if they adopt a cloud-first policy—will continue to have non-cloud legacy applications and data for some time to come. On-premises, cloud, and mobile IT are

typically used for different applications and managed by different teams. For large enterprises that are not digital natives, it is usually unrealistic to abolish legacy IT overnight and move everything to the cloud immediately (although that remains a desirable long-term goal in most cases).

Given this heterogeneity of IT assets, large organizations will have many people working on data security issues and these various teams will naturally develop different perspectives. But this multiplicity can be a source of risk if proper coordination is not established.

IT and security staff across your organization must have a unified approach to data security, whether the data resides in your own data center, in the cloud, on mobile devices, or on your customers' premises. Security issues must not fall between the cracks due to inadequate communication between different parts of your organization.

User authentication is a key area to focus on, as we discuss further below. If your web applications, legacy systems, and mobile devices all require different logon procedures, you may be creating gaps that attackers can exploit or inefficiencies that will incent employees to develop faster but less secure work-arounds.

Rationalize your portfolio of security tools. Good information is the foundation of good decision-making. But in cybersecurity as in life, receiving too much information at once, or not receiving it in the right context, can cause danger signals to be missed. Limit the fragmentation of your security tools and insist that they be able to exchange data easily. All tools in your portfolio should

feed seamlessly into an integrated big picture. This goal is not easy to achieve, but is worth the effort.

Today's attackers use many attack methods: stealing credentials, installing malware that erases itself to avoid detection, modifying internal processes and rerouting network traffic, tricking users with social engineering scams, and targeting both corporate and personal mobile devices.[25] Against this constantly evolving threat landscape, enterprises are deploying more and more security tools, many designed to address narrowly specific issues.

Too often, these solutions don't play well together. Their lack of integration can make it difficult for security professionals to see the total picture of what's happening and to prioritize threats quickly. This is even more difficult when multiple teams manage cloud, on-premises, and mobile IT in different ways.

A common approach has been to use Security Information and Event Management (SIEM) solutions to correlate the flood of alarm signals arriving from various far-flung spots in the enterprise network. However, these tools aren't perfect and detection still depends on human experts poring over logs and data, prioritizing incidents, and carrying out investigations. Data gathering and reconciliation are difficult, and the lack of a unified view makes both response and management cumbersome.

Leaders should insist that their security teams focus on gaining a holistic view across the entire enterprise network. This means building a constantly updated security picture of what's happening in on-premises IT, cloud services, corporate, and personal mobile devices, and ultimately even Internet of Things devices controlled

Who is responsible for what?

Division of responsibilities between cloud provider and enterprise

Security component
An organizational culture that encourages each individual to take responsibility for cybersecurity
Compliance with laws, regulations, and standards
Regular sweeps of network and permanent hunt for signs of intrusion or anomalous behavior
Active protection measures against malware threats
User Identity and Access Management properly configured and managed
Data and files properly encrypted
Applications patched and properly configured
Databases patched and properly configured
Middleware patched and properly configured
Network properly configured and managed
Server operating systems patched and properly configured
A physically secure data center

	Software as a service	**Platform** as a service	**Infrastructure** as a service	**On premises**

by customers. A best practice is to create an ecosystem of security products and platforms designed to integrate with each other and that can provide insights across all platforms.

Delegate activities that are not part of your core value creation. Leverage the security experience of your cloud providers. Keep what you do better than anyone else—or that which you must do yourself—in-house. But hand off activities that are not part of your core value-creation process to providers who can do a measurably better job.

The fundamental security advantage of the cloud providers—particularly the global leaders like Microsoft, Amazon, or Google—is that because of their vast scale they see far more "bad things" than their customers do. Microsoft is the world's largest provider of enterprise cloud email; it scans 400 billion emails per month for malware and phishing attacks. Google is the world's largest search engine. Amazon provides more cloud infrastructure services than anyone else.

In the era of software intelligence, data rules. The ability of machine learning algorithms to detect threats and anomalies improves exponentially as the quantity of data they are exposed to increases. Seeing enough data is often the dividing line between problems that can be solved in milliseconds and problems that cannot be solved at all.

But scale brings more advantages than just data. The large cloud providers can afford to employ more of the world's top computer scientists and data security experts. They can afford large "red teams" devoted full time to probing their own defenses for weaknesses. They keep their hardware and software fully updated and patched at all times. They have unmatched R&D budgets that

fund a continual stream of new ideas and methods for delivering cloud services securely. They can innovate faster and more fruitfully than any individual customer organization can on its own.

In short, you should continually benchmark your security against that of the cloud providers. If you can do a better job, keep it in-house. If not, delegate.

Never forget that your enterprise retains ultimate responsibility for its own security. As the cloud matures and users deploy more sophisticated applications to it, the most important piece of the security puzzle remains in your hands: namely, the conduct and actions of your employees. That is something you cannot delegate.

> **"Every company has at least one person who will click on anything."**
>
> —Anonymous executive at a Fortune 50 firm

Errors by well-meaning employees remain the greatest source of risk. To mitigate that risk, you must build a culture of attentiveness and responsibility. Consider this analogy: Your bank may be the most trustworthy and secure bank in the world. But if you allow your employees to access accounts at your bank without proper access controls or audit trails, you are asking for trouble.

No organization can guarantee that all of its employees (let alone those of its partners and suppliers) will do the right thing all of the time. But the most secure enterprise is the one whose leaders understand that security always starts at home.

The UK trusts its national security to the cloud

Providing security on any front requires a willingness to adopt leading-edge technologies. But highly regulated government entities must find the right balance between enabling employees with data access anytime and anywhere, and ensuring security.

Britain's Ministry of Defence has assumed a leadership role in this effort with the decision to adopt the Microsoft Cloud as well as Office 365 Advanced Threat Protection and Customer Lockbox from a Microsoft U.K. data center. More than 95,000 Ministry of Defence mailboxes will be protected with Office 365 Advanced Threat Protection.

"The MOD chose Microsoft cloud technologies to support our transition to a more cost-effective, modern and agile organisation. Microsoft offers the security, privacy, control, and transparency that meets our stringent criteria for cloud services—all available from data centres in the U.K."

—Mike Stone, Chief Digital and Information Officer, MOD

Aligning its vision for digital transformation with the Microsoft Cloud, the MOD gets the best of both worlds—productivity-enhancing agility in a highly secure online environment.

360-degree security

What you should know

For most of recorded history, cities of any significance were surrounded by walls. For thousands of years, empires and city-states waxed and waned as countless battles were fought before high ramparts of stone or wood. Rulers expended vast sums on fortifications. Attackers developed ingenious tactics to defeat them. Cities whose walls withstood the battering rams, scaling ladders, and buried mines (or the occasional Trojan horse) were able to live on. Cities whose walls were breached fell prey to fearful pillaging and were often reduced to rubble.

For most of the modern IT era, cybersecurity has been built on the same idea of a fortified perimeter surrounding the vulnerable enterprise and its precious data. Enterprises deployed firewalls and sought to lock down every access to their networks.

Walls of Paris during the Prussian Siege 1870–1871[26]

But today, walled cities are obsolete. And the same is true of the walled enterprise. Staking everything on a single fortified perimeter is no longer a safe or prudent way to defend against cyberattackers. Walls are no longer enough, because threats are everywhere. In fact, today's enterprise leaders must base their cybersecurity strategies on the uncomfortable but realistic premise that attackers are already within the walls.

"Security never stops. It's like going to the gym every day. You have to exercise your operational security posture on a continuous basis."

—Satya Nadella, CEO of Microsoft

Why is a fortified perimeter no longer enough to guarantee safety? The reasons have to do both with new technologies that circumvent old defenses and new ways of doing business that depend on the free flow of information.

Static access controls like firewalls and intrusion prevention systems at network entry and exit points are readily evaded by attackers, because communications paths in and out of networks are too complex and dynamic. Widespread use of personal devices inside corporate networks has dissolved what was once a hardened network boundary. We no longer conduct business within a perimeter of highly regulated, corporate-issued devices that access the network only under the strictest of controls. Instead, the modern enterprise encourages dynamic communities of employees, contractors, business partners, and customers to connect through an agile digital fabric designed for sharing and collaboration.[27]

Of course, we are not saying you need no longer bother to protect your enterprise's network perimeter. You should also not neglect the physical security of your data center. At Microsoft, we treat our own data centers like literal fortresses, equipping them with fences, man-traps, video surveillance, and 24-hour on-site human security, as well as requiring multi-factor authentication of all personnel before entry. We even physically shred hard drives when we take them out of service.

But with the increasing scale and sophistication of cyberthreats, no matter how strong your defenses are, fortifications alone are not enough. **Effective cybersecurity now requires a 360-degree approach that not only defends the wall itself, but deploys active defense measures both outside and inside the perimeter.**

Today the "outside" of your corporate network is no longer defined by your firewall, but by the credentials your employees, suppliers, and customers use to log onto your network from remote locations that may be anywhere in the world. We discuss this in the section below titled "Identity is the new firewall." Likewise, the "inside" of your network can no longer be treated as a secure enclave. Instead, it must be constantly scanned for signs of a breach, with the intent of deploying damage control measures at the earliest possible moment if one is detected. We discuss this in the recommendation below titled "assume breach."

What you should do

Enterprise leaders and their legal and compliance advisors should adopt the following policies to implement a 360-degree approach to cybersecurity:

Update your software and hardware. If technology never changed, it wouldn't be necessary to update it. But if technology didn't change, we would still be living in the Stone Age. Over the past half century, wave after wave of new computing technologies have transformed society, business, and daily life. To continue reaping the benefits of this seemingly unending stream of technological innovation, we must accept the cost of constantly swapping out the old for the new.

Although the earliest modern computers date from the 1940s, the true takeoff of the enterprise IT era began with the launch of the IBM 360 mainframe in April 1964.[28] In that month annual GDP per capita in the United States was about $19,000. In 2017, after the successive mainframe, PC, Internet, and mobile revolutions—and on the eve of new revolutions in Artificial Intelligence and the Internet of Things—U.S. GDP per capita exceeds $52,000.[29] If this growth rate continues for another 53 years, we will reach $143,000 per capita by 2070. The benefits of innovation are real and large. (All amounts in this paragraph are in 2009 constant dollars.)

But technology does not stand still. No one still uses IBM 360s. Despite the billions of dollars once spent on them, they have all long since been junked. Today, the lowliest iPhone provides orders of magnitude more compute power and memory for a tiny fraction of the cost.

Similarly, there comes a time when yesterday's software is no longer adequate for any purpose. No enterprise should permit its users or IT staff to continue running an obsolete operating system like Windows XP on the pretext that some critical legacy application requires it. Replacing the old application may not be easy, but it is the safe and right choice.

Faster chips and smarter algorithms are not the only advantages of newer technologies. They are also far more secure, because they can leverage their improved capabilities to detect and defend against threats that the designers of the IBM 360 or Windows XP[30] never imagined.

Don't allow outdated technology with compromised security to linger in your organizations. Yes, requiring your IT staff to install the latest versions of operating systems and other software will cost more in both money and operational complexity, as will replacing older, less capable hardware (where security vulnerabilities often lurk in outdated firmware). But enterprise leaders must not shirk from these common-sense safety measures. Instead of trying to cut costs by deferring essential upgrades, it is better to manage costs by leveraging the pay-as-you-go flexibility of the cloud to purchase only the amount of IT resources you actually need at any given moment.

Patch your software. Nothing in modern civilization is more complex than software, and this complexity can become a source of vulnerability when enterprises underestimate it. To paraphrase a saying attributed to Albert Einstein, the goal of good software design can only be to make software as simple as possible, but not simpler. No piece of modern software can ever be completely free of programming errors or design flaws that unintentionally expose it to the probing of cyber attackers. Your security policies must reflect this fact.

Software vendors understandably do not seek to broadcast the extreme complexity of their products, preferring instead to wrap it in reassuring brand and feature names. But enterprise leaders should not be lulled into thinking that, because their IT staff has

installed the latest version of an operating system, the enterprise is therefore fully up to date. There is a crucial difference between updating to a major new software release and making sure that the new release is itself continually updated with the smaller updates known in the industry as "patches." Updating from Windows 7 to Windows 10, for example, does not absolve you from the imperative of continuing to apply new security patches to Windows 10 as soon as they become available.

For a chilling example of why patching is not the same as updating and why both are necessary, see the nearby text box describing the notorious WannaCry ransomware attack.

WannaCry: Why patching is essential

The WannaCry ransomware attack began in May 2017. Based on techniques believed to have been first discovered by the U.S. National Security Agency and later obtained by hackers, this destructive virus exploited a vulnerability in older versions of the Windows operating system to encrypt user data and demand a ransom in exchange for the decryption key. Systems running Windows 10 were immune to the virus, because it no longer has the old vulnerability. Users running Windows 8 were protected if their systems were fully up to date with patches. Some users running unsupported versions of the obsolete Windows XP were susceptible to the virus at the time of its first appearance in May 2017, although Microsoft quickly provided a patch that protected them.

The vast majority of WannaCry victims (98% by some estimates) were actually running Windows 7. This older operating system is still widely used and will be supported by Microsoft until 2020, but—like any operating system still in service—it must be continually patched as new threats are discovered. Ironically, Microsoft had already issued a patch for Windows 7 in March 2017 that fixed the WannaCry vulnerability, two months before the attack began. Users who patched their Windows 7 devices promptly were protected. But those who failed to apply the patch—including several hospitals in Britain's National Health Service—fell prey to the virus.[31]

In short, updating is not enough—continual patching is also essential. Ensure that your enterprise policy not only requires patches to be applied, but requires them to be applied promptly. And don't forget that more than half of all known vulnerabilities affect software other than operating systems: you must ensure that your IT team patches all of your software.

Use the new security features in modern operating systems to harden your endpoints. We have seen that the walled enterprise is no longer safe from attack. Walls must now be supplemented by other forms of defense that operate both outside and inside your wall, as we shall discuss further below. But the examples of upgrades and patching should serve as a reminder that if walls are not enough, they are nevertheless still essential. The basic building block of your enterprise's cybersecurity wall is the device that connects each individual user to your network. These "endpoints," as they are known, are the first target of attackers. Consequently, you should take all available measures to harden them.

The first step in hardening endpoints is to make sure your enterprise is actually using the security features these devices and their operating systems come with. Modern operating systems such as Windows 10 and recent enterprise-grade versions of Linux are introducing deep architectural modifications that dramatically improve their defensive capabilities compared to older software.

The guiding principle behind these changes is that any piece of software running on a user device should be severely restricted in the resources it can access and the actions it can take. The idea is to isolate applications from their environment and from each other. This is achieved by surrounding them with barriers built into the lowest levels of the operating system and enforced by the underlying hardware itself.

Security is an arms race. The attackers are not standing still. You should insist that your Chief Information Officer (CIO) and Chief Information Security Officer (CISO) investigate the latest operating system security features and deploy them as soon as they judge feasible. The technology behind these features is complex and rapidly evolving. Understanding their capabilities and carrying out their deployment will require skill and specialized knowledge on the part of your security teams. Below, we provide a high-level summary of some of the key concepts implemented in these new operating system architectures.

Endpoint hardening: Security features in modern operating systems	
Biometric logon	Allows or requires user to log on with unique biometric feature such as fingerprint, face scan or iris scan. *Example: Windows Hello, Apple Face ID*
Anti-malware	Scans incoming files and code for known threats using continually updated database, blocks execution of detected threats. *Examples: Windows Defender, McAfee, Symantec, and many competing products*
Application whitelisting	Instead of blocking known threats (blacklist), only allows programs to execute if they are on enterprise-approved whitelist. *Examples: Windows Device Guard, AppLocker*
Hardware isolation of user logon secrets	Uses hardware cryptographic chip to store user logon secrets, which are thus protected even if malware infects the operating system. *Example: Windows Credential Guard*

Endpoint hardening: Security features in modern operating systems	
Drive encryption	Encrypts all data on device storage, prevents access if device is lost or stolen. *Example: BitLocker*
Restricted information use/access	Protects enterprise-owned data from unauthorized use. Prevents data from leaking outside the enterprise. *Example: Windows Information Protection*
Restricted administrator rights	Administrators can only perform specified tasks in a specified timeframe. If admin password is compromised, the scope of damage is limited. *Examples: Microsoft Just Enough Administration, Just in Time Administration, Role-based Access Control*

Always assume breach. Hardened endpoints are necessary, but not sufficient. You must also prepare your post-breach defenses, because the reality in today's threat environment is that you will be breached at some point. Your ultimate goal should not be to stop something that is likely unstoppable, but to contain the damage as much as possible.

In the industry this proactive defensive stance has come to be known as "assume breach." Just as our immune system has evolved to detect the infections it cannot prevent and limit the harm they cause, enterprise leaders should implement standing procedures to detect breaches and mitigate their consequences. **Breaches may be inevitable, but catastrophic consequences from a breach are not**—the goal of the well-defended enterprise is to minimize damage and recover swiftly.

"Assume breach" boils down to three essential measures:

1. Implement a standing and professionally staffed program of scanning that combines sensor data, analytics and intelligence from all available sources to sweep continually for signs of a breach inside your network perimeter.

2. In addition to building a strong outer wall, make sure that your IT systems are compartmentalized by internal walls that will block attackers from spreading laterally throughout your organization.

3. Develop a thorough breach response plan and train a team to carry it out. The plan must include technical measures to end the breach, tactics to recover or repair affected data, and measures to deal with any legal and compliance issues that arise, as well as reputational matters. The response team should not be limited to technologists, but should include enterprise leaders, legal and compliance experts (possibly including outside counsel), marketing and public relations experts, and other relevant business stakeholders.

"There are two kinds of big companies, those who have already been hacked, and those who don't know they've been hacked."

—Former FBI Director James Comey

A continuous breach monitoring program should be designed to minimize the noise of low-level alerts and highlight the issues that truly matter. Assume breach means that your operations teams must shift from reactive alert management to proactive hunting. Identifying abnormalities with managed sweeps is a new critical operational process. The operations teams should also run regular red team/blue team drills to refine their skills and identify weak spots. Enterprises that adopt these tactics will be in a much stronger position both on the day a breach is detected and in the days that follow.[32]

Protect your information assets with encryption. An immediate implication of an "assume breach" stance is that you must adopt a layered defense. If breach is a given (or very likely), then you must fortify not only your outer wall, but also important information assets inside the wall. Two key components of such a layered defense are encryption and an approach called "information protection."

Modern encryption methods are based on complex mathematical formulas, but the basic idea is simple: only users who have the right key can access encrypted documents. Encryption can be applied at many different levels in both on-premises and cloud systems. It can apply at the level of a single file, an entire hard disk, or an entire cloud application. Information assets that are encrypted cannot be stolen, even if hackers trick a user into giving up their credentials, breach your outer defenses and run wild on your corporate network. Encryption of sensitive data is one of the cornerstones of a cyberdefense in depth.

The most important thing to remember about encryption is that it must be turned on to work. Many enterprises have paid the price for overlooking this elementary precaution. Enterprise leaders must not only establish high-level guidelines for the use of encryption, they must also see to it that these guidelines are put into practice and rigorously enforced.

Some cloud providers offer an additional service called "information protection," which extends encryption. Your administrators will set up tools provided by the cloud service to classify and label any sensitive files or emails you designate, and then selectively encrypt them so they can only be accessed by authorized users. The cloud service itself never sees your protected information and cannot decrypt it.

A further extension of this idea is "data loss prevention." Here, a cloud email service such as Office 365 can be taught to recognize certain sensitive information types such as Social Security numbers, patient health records, financial account numbers, and the like. The cloud then tracks where messages containing these types of information are sent, and blocks them if someone tries to send them to an unauthorized user or destination.

Anatomy of a breach[33]

STAGE 1

Attacker gets initial foothold

The tiniest opening can allow an attacker to gain a foothold in your organization. Whether through a compromised PC, an unpatched Internet-facing server, or a badly configured network device, an attacker can use anything available to breach a company's perimeter and gain access into its network. Once inside, the hacker can perform reconnaissance to identify and target valuable information or resources.

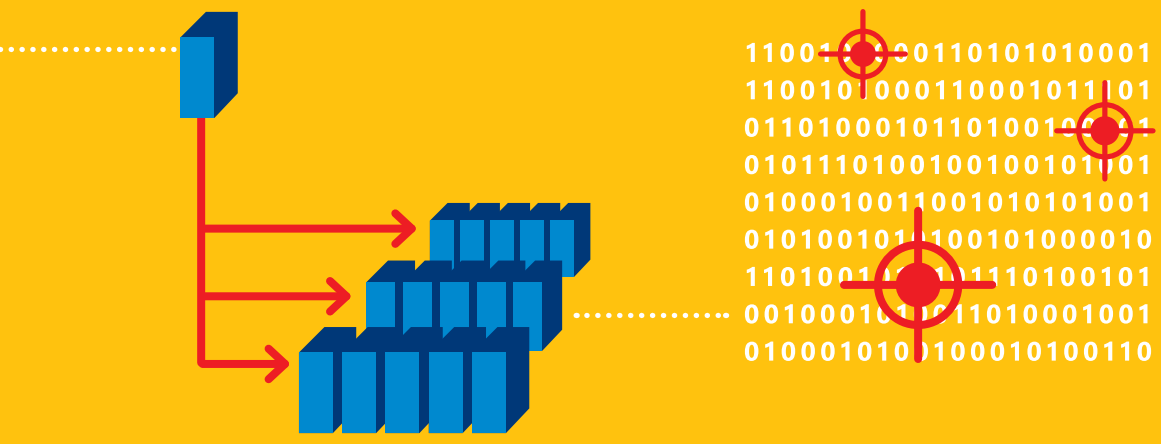
"Breaching the wall is only the first step"

STAGE 2

Attacker gains elevated control

Once an attacker has infiltrated an organization, the next step is to expand its foothold into a broader front. Attackers first try to consolidate their control of the local system (where the initial breach occurred), or look for another system that offers a better chance to gain administrative privileges or access to valuable data.

The attacker's goal is to find user accounts that are responsible for managing other systems, gain control of those accounts, and then exploit their ability to access and control other resources on the network. Typically, these actions require administrator account privileges and cannot be accomplished as a normal user.



STAGE 3

Attacker expands inside your network

In stage three, the attacker gains widespread access to your network by spreading out from an individual workstation or server into as many systems as possible. The attacker may then install a permanent backdoor or alternate mechanism for long-term access to the systems.

The attacker may use built-in or downloaded tools. Some of these might be malware (known as implants). Other techniques can appear more legitimate, such as creating fake accounts and gaining remote access so that the attacker can not only get back into the network, but can hide in the environment while accessing various resources.

STAGE 4

Attacker settles in for long-term persistence

In stage four, the attacker settles in for the long haul, deploying processes to conceal their presence and exploit it to accomplish their mission. They may install malware to exfiltrate large amounts of sensitive data over prolonged periods of time (many months in some cases), or even deliberately destroy data and sabotage vital systems in the target organization. At this stage the attack has become what is known as an Advanced Persistent Threat (APT). If they suspect they've been detected, they can slip away and reenter later, or inflict a final wave of catastrophic damage.


TT126
TT116
S4
S3

For banks, data security is everything

DBS is a major financial services group in Asia, with more than 280 branches across 18 markets. Headquartered in Singapore, it strives to be the bank of choice for the ever-expanding Asia economic region.

As part of that mission, DBS is implementing a digital vision. Explains David Gledhill, CIO of DBS, "We're digitizing all the way to the core of our banking activities, then guiding our customers to embrace digital practices, and transforming the relationship between employees and technology to create a more productive workplace."

"We believe the Microsoft cloud is more secure than anything a traditional bank could implement. DBS gains consistent vigilance, technology experts that no bank could likely retain, and constant security reinvestment."

—David Gledhill, CIO of DBS

As a heavily regulated financial services company, DBS has strict security and privacy standards. A move from on-premises solutions to the cloud would have been unthinkable without absolute confidence in the safety of bank information. The DBS IT team thoroughly examined Microsoft cloud security measures as they apply to financial services. The comprehensive information in the Service Trust Portal, the positive response from Microsoft to address Singapore banking guidelines, and access to the Microsoft Financial Services Compliance Program all gave DBS confidence in its evaluation.

DBS is promoting a change in corporate culture to further its digital agenda. The bank wants to use technology to help individual employees and teams provide better service to customers. Says Gledhill, "We see technology itself as a competitive advantage."

Identity is the new firewall

What you should know

As we have already noted, the vast majority of enterprise data breaches begin with the compromise of a single user's credentials. The most common scenario is a "phishing" attack, where an email carefully crafted to look legitimate lures the victim into typing their credentials into an attacker's phony web page. But other scenarios are possible, such as guessing a weak password or outright theft of credentials.

We live in a world where it is no longer possible to insist that business be conducted exclusively within a controlled perimeter of corporate-issued devices. Employees now expect to work anywhere, on any device, whether approved by IT or not. And employees are not the only users who connect to your systems—customers, suppliers, and other outside partners must do so as well. As a result, the firewall no longer marks the true perimeter of your enterprise network.

Because the enterprise can no longer isolate itself from the world behind a wall and a moat, identity becomes the new firewall. In such a world, the electronic credentials that identify who has the right to access your network become strategic assets that must be protected from compromise at all costs.

Identity transcends devices and locations. It enables companies to apply rigorous and granular controls based on the user's organizational role, authorized privileges, and verified needs, regardless of how or where the user connects. By focusing on authenticating and managing user access rights, organizations can protect data regardless of where it is stored or how it is accessed.

The industry uses the phrase "Identity and Access Management" (abbreviated IAM) for solutions that manage user access to enterprise applications and data. IAM can eliminate the need for multiple credentials by giving employees a single identity to access cloud, mobile, and on-premises resources. Cloud-based IAM can also leverage threat intelligence from the cloud provider to detect abnormal logon behavior and respond appropriately.

Multi-factor authentication (MFA), which we discuss further below, offers another layer of protection, requiring users to prove their identity with something they know (a password or PIN), something they have (a specific device), and possibly even something they are (a biometric).

"Effective Identity and Access Management is 70% people, process, and politics, and only 30% technology."

—Forrester Research

An even more advanced IAM tactic is conditional access, where every logon attempt is assessed in real time for user risk, device risk, application risk, and even location risk. Is it reasonable for a senior member of your finance team to request access to the corporate budget application using a company-issued laptop from the IP address of a New York hotel? Possibly or even likely, if the user's online credential and secondary authentication factor are valid. Is it reasonable for an office assistant in the same department who rarely uses the budget application to request access on an unknown Android mobile device at 1 A.M. local time from an IP address in Moscow? Conceivably, but further verification may be indicated. Could the same user validly request access on a different device from Tokyo 10 minutes later? Definitely not.

By assessing the context of a logon attempt in real time, the IAM system can, applying policies your security staff defines, choose to grant or block it outright, require further proof such as an additional MFA factor, or even kick the issue upstairs for a human to decide.

In short, protecting your data begins with protecting the credentials that grant access to it.

What you should do

Require single identity. In any modern organization, even one that is not particularly large, users inevitably need access to multiple applications that live on various systems (either on-premises or in the cloud), and they use multiple devices to do it. If not proactively managed, this diversity of IT assets almost always leads to an unmanaged sprawl where users have different user names and passwords for different systems. This multiplicity then creates an obvious and profitable target for attackers.

While delegating technical details to your CIO or CISO, enterprise leaders should aim for a single identity policy for all users and all applications, no matter who owns them. The ideal scenario is to manage identity and authentication for all users, applications, and devices that access your information assets in a unified way, while enforcing specific policies that your security team establishes such as conditional access and multi-factor authentication. In practice, this ideal can be difficult to achieve for large organizations that have many legacy applications, which may require ad hoc solutions. But modern cloud-based IAM systems such as Microsoft's Azure Active Directory and comparable solutions from other providers are the first step on the road to unified identity management. They should be regarded as the default best practice for controlling identity sprawl and the security risks that come with it.

Mandate multi-factor authentication. The basic idea of multi-factor authentication or MFA (sometimes also known in the variant form of two-factor authentication, or 2FA) is not new. Typically, it requires a user to type a password and also present a second factor, which can be something as simple as a code in a text message sent to the user's phone, or something more complicated like a special USB key or smart card. More recent versions of MFA can make the second factor a biometric trait of the user, such as a fingerprint, facial or iris scan, or even a voiceprint.

The fundamental advantage of MFA is that it means stealing a username and password through a phishing attack is no longer enough for a hacker to break into your network. To gain access the hacker must also steal something else that is usually more difficult to steal: a specific authorized device that the user physically possesses–a phone, PC, USB key, or other device.

> **"Multi-factor authentication is one of the best practical things an enterprise can do to protect its security."**
>
> —Brad Smith, President and Chief Legal Officer of Microsoft

The technology of MFA is evolving quickly and the choice of the right scheme for your enterprise is best left to your security team. To be sure, MFA is not 100% bullet-proof—nothing is. MFA—at least in its non-biometric forms—also requires extra steps during login that some users will find inconvenient. But the improvement in security it brings is more than sufficient to justify enterprise leaders in overruling objections and making it mandatory.

While it is possible to require MFA in granular fashion only for certain groups or individuals, it is safer to apply the mandate to everyone. Enterprise leaders should query their CIO or CISO closely to understand who has the authority to grant exemptions to an enterprise MFA policy. Ideally the answer should be "nobody." But we have seen cases among customers where the board was assured that MFA had been implemented, only to discover after a data breach that, in fact, hundreds of users had received exemptions for this or that reason. At Microsoft not even the CEO can override the requirement for MFA. We recommend MFA as the default best practice.

Consider getting rid of passwords. Passwords are the single greatest chink in the cyberdefense armor of the modern enterprise. Following now outdated advice of the U.S. National Institute of Standards (NIST), many organizations have inflicted onerous password rules on their users, forcing impossible-to-remember mixtures of upper- and lower-case letters, numbers, and non-alphanumeric characters, and further requiring that passwords change every few months.

Remarkably, after conducting extensive field research on what actually works and doesn't work, NIST has recently offered a sweeping revision of its guidance that replaces many of the old rules.[34] Instead of odd and likely too-short mixtures of characters, NIST now recommends long, memorable passphrases based on private user secrets.

Such passphrases, which NIST suggests do not need to change unless lost or compromised, can reduce the risky shortcuts that many users resort to under the old rules, such as taping their passwords to the screen or using the same easy-to-guess password everywhere. They also reduce the frequency

of resets due to forgotten passwords, which are a known source of vulnerability when clever hackers persuade human administrators over the phone to override standard procedures.

But an unexpected benefit of modern MFA schemes is that they make it feasible to replace passwords altogether with methods based on public key encryption. Such schemes combine an easy-to-use local authentication factor such as a PIN or biometric scan entered on the user's pre-registered access device (for example, a specific PC or smartphone) with a cryptographic secret stored in a secure chip on the same device.

"Getting rid of passwords isn't just a good idea, it's increasingly possible."

—Julia White, Corporate VP
Cloud Platform, Microsoft

When users want to log onto an application they are authorized to use, they must prove their identity to the device by means of the PIN or a biometric scan. This purely local factor never travels over the network and is of no value without the user's authorized device. The device then uses its cryptographic secret to prove to the distant application (which may reside anywhere on the enterprise network or the Internet) that the user has been authenticated and that the device itself is one this user has previously registered.

One such multi-factor cryptographic logon scheme has been standardized by the FIDO Alliance, with the support of Microsoft, Google, the major credit card companies, and many other firms.[35] Enterprise leaders should instruct their security teams to evaluate FIDO and similar schemes and plan for migration away from passwords to more secure cryptographic logon methods.

Use mobile device management and data segregation. The use of mobile devices personally owned by employees has become widespread in large organizations. Although some may try to ban the practice and may even succeed, doing so likely hurts productivity and may encourage users to explore dangerous work-arounds. A better alternative is to use a mobility management system to control enterprise data and access on personal mobile devices.

Such software, typically cloud-based, allows the enterprise to enforce separation between its own data and personal data on a user's device. It can impose encryption policies, prevent forwarding to unauthorized accounts, and even perform a remote wipe of enterprise data and access rights if the user's device is lost or stolen, or if the user leaves the organization.

Monitor and restrict privileged access. The most dangerous kind of user—the one who will be the prime target of attackers—is the employee whose job requires him or her to have expansive access privileges on your enterprise network. System administrators with privileged access rights are of course indispensable for managing an effective enterprise network and securing the valuable information assets that reside on the network. But their activities must be rigorously and continuously monitored for anything unauthorized or unusual. Such monitoring is known as Privileged Identity Management, or PIM, and requires dedicated policies and software tools.

Two key principles of PIM are just-in-time (JIT) administration and just-enough administration (JEA). Both are based on the idea of least privilege. With JIT, a system administrator must request elevated privileges, approved by another person, before gaining access to sensitive data. With JEA, the administrator

only receives the minimum permission necessary to do what needs to be done, and then only for a limited amount of time.

In a notorious example where these principles were not applied, a system administrator at the National Security Agency named Edward Snowden, whose job required him to apply security patches to a file sharing server, was also mistakenly granted access to the actual data on the server. The rest of the story is likely already known to the reader.

At Microsoft, the most sensitive data is data that belongs to our customers. Access to this data by our employees requires multiple interlocking approvals. Not even our CEO can override these mechanisms. PIM is an essential security discipline that all enterprises should practice.

A state offers citizens a unified online identity

To support local entrepreneurs, the state of Indiana decided to create a one-stop web portal for business formalities called INBiz. The state wanted to provide secure online access to services such as registering a business, paying taxes, and other services. A key requirement for INBiz was single sign-on for all of these services, which were provided by multiple back-end applications.

The idea was that any citizen of Indiana could use the web portal with a single digital identity, instead of logging on to different systems, each with a different password.

The state's IT team decided to centralize identity management with Microsoft's cloud identity management service, Azure Active Directory B2C. Highly secure, available, and scalable, this pay-as-you-go cloud service can extend to millions of users. It also provides for easy multi-factor authentication. Today more than 100,000 Indiana business owners use INBiz, and the number is expected to triple in the near future. The INBiz portal is hosted by Azure App Service on Azure Government, a physically isolated instance of Microsoft Azure, built exclusively for U.S. government customers and their solution providers.

Ultimately, Indiana looks forward to expanding a single identity management solution to all state agencies. A citizen of Indiana will then have a single electronic ID to get a driver's license, file taxes, apply for medical benefits, or start a business. As Indiana is demonstrating, the future of government is e-government.

Machine intelligence and big data

What you should know

Machine Learning is driving a quiet but remarkable revolution in cybersecurity. Let's take a brief step back in history to explain the context of this development, which has profound and positive implications for enterprise cloud users.

The branch of academic computer science called Artificial Intelligence was founded in the mid-1950s. Although it attracted some of the most brilliant minds at our greatest universities and vast amounts of government funding, for half a century and more AI's achievements were largely unimpressive. Certainly it produced nothing resembling human—let alone superhuman—intelligence. Perhaps traditional AI's greatest achievement was to demonstrate that genuine intelligence cannot be usefully modeled by systems consisting solely of logical axioms and deduction, no matter how sophisticated.

But in the past few years, a specialized sub-branch of AI, one that replaces pure logic with subtle mathematical techniques of pattern recognition, has begun to show unexpected progress. This branch, known as Machine Learning, and especially its even more specialized offshoot known as Deep Learning (or Neural Networks),[36] has produced a series of genuine breakthroughs in the fields of image recognition, speech recognition, and machine translation.[37] Indeed, these results are so remarkable that they have revolutionized almost overnight the quality of popular cloud-based consumer services that we are all familiar with. Promising work in many other areas, such as self-driving cars and medical diagnosis, is also advancing rapidly.

Today the world's leading tech companies—in particular Google, Microsoft, Facebook, Amazon, Apple, and Salesforce—have large Machine Learning research teams that compete with each other

to recruit the top Ph.D.s in the field and publish pioneering research on a regular basis.

Machine Learning is also making less publicized but equally dramatic progress in cybersecurity. Here, just as in the more visible consumer services, the key to Machine Learning success is the availability of immense quantities of data used to train learning algorithms and measure their progress.

To learn to recognize the early warning signs of a cyberattack and classify it correctly, Machine Learning algorithms must be exposed to vast numbers of threat examples, preferably hundreds of thousands or even millions. Only a handful of the very largest cloud providers possess such data. Microsoft, to take the example we know best, scans more than 400 billion email messages every month for malware and signs of phishing attacks. We also receive telemetry data from a billion Windows devices that alerts us to new cyberattacks in their earliest stages.

We analyze this data on an unparalleled array of cloud-based compute resources that represent billions of dollars in capital investment. But most important, recognizing that human intelligence is still irreplaceable, we also employ a large number of the world's best and brightest specialists—hundreds of machine learning researchers and 3,500 cybersecurity experts in all.

The top global cloud providers have far more data about cyber-risks than even the largest enterprises, and they also have deeper human expertise. In the cloud, cybersecurity is all about scale.

What you should do

Leverage the cloud provider's big data and machine learning advantages. We've already seen that more data means more insight. We've also learned that prudent enterprises adopt an "assume breach" defensive stance to cope with the permanent menace of cyberattackers. But enterprise leaders should understand that the cloud now makes possible new forms of cyberdefense that combine these two core concepts to connect pre-breach and post-breach defenses.

Conventional anti-malware software—such as Microsoft's Windows Defender built into Windows 10 and similar products from other providers—attempts to block malware by regularly scanning user devices for known malware "signatures" (specific sequences of bits), relying on a database that is regularly updated by the anti-malware provider. But this conventional approach, while still essential, is static. It is not good at detecting threats it has never seen before and, especially, it can be fooled by advanced forms of malware that use cloaking techniques to conceal their presence. Further, it is not much help in investigating breaches that have already happened and learning how to halt them.

The next stage of anti-malware (such as our own Windows Defender Advanced Threat Protection)[38] does not rely on static signatures, but looks at the actual behavior of a suspected threat over its entire lifecycle. It asks: What is this piece of software doing, and why?

This lifecycle begins from the moment our security experts first become aware of a particular threat's existence in the wild, extends to the instant it first attempts to launch harmful code on one of your devices (perhaps after a user has inadvertently downloaded

an infected file), and then continues to track the malware's post-breach activity inside your network, all while delivering real-time advice to your security team about how to shut it down.

This form of intelligent cyberdefense stores everything it learns in a private cloud repository specific to your enterprise and your devices. It observes and records real and suspected malware events that occur on all your enrolled devices, providing an indispensable historical database of evidence for post-breach investigation and cleanup. This private repository is further enriched with threat intelligence that Microsoft gathers from millions of other customers and from partners in industry and government.

We call our continuously updated global threat database the Microsoft Intelligent Security Graph. It contains many billions of items of information that flow in constantly from all the sources available to us. We apply always-evolving machine learning and deep learning algorithms to the graph to track known threats and identify new ones. By connecting the insights we gain from this global graph with the data we gather about threats on your specific network, we create a two-way street of improvement driven by machine learning and big data. If a snippet of code or its behavior on your network resembles malware we have already observed elsewhere, we can detect that. If your network comes under attack from a kind of malware never before seen, we can use this observation to warn others while we develop countermeasures. In this way, without jeopardizing anonymity, security learnings from any one customer can benefit all of our customers.

Use automation and "nudges" from the cloud to help your employees avoid mistakes. At Microsoft, our internal cloud operations are highly automated to reduce the possibility of human error. Our ideal is touchless operation, where rigorously designed

and managed software code operates our services, not people. We want people to make decisions, not trouble.

> **"We're working to use technology to protect people from themselves, because the truth is we all could use some help protecting us from ourselves."**
>
> —Brad Smith, President and Chief Legal Officer of Microsoft

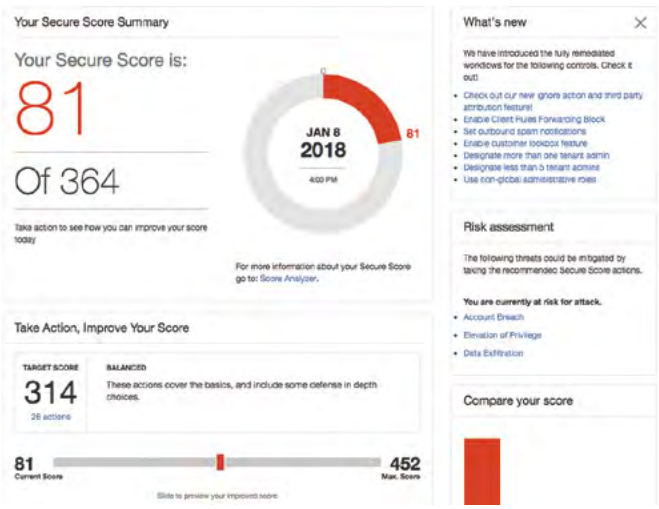
Enterprises should leverage the big data experience embedded in cloud services to "nudge" their employees away from mistakes and toward correct, safe behaviors. Well-designed cloud services warn both users and system administrators about risky actions. Here are some examples:

- Cloud-based enterprise email systems can be set up to block users from opening messages containing known or suspected phishing links.
- Suspicious emails can be evaluated in virtual "detonation chambers" in the cloud. If no malicious activity is detected, the message is passed through to the user.
- Cloud applications can warn designated administrators in real time when unusual or forbidden user actions are observed: for example, if a large file is suddenly sent to an unfamiliar address outside the enterprise network, if an email contains certain kinds of known sensitive data (Social Security numbers, credit card numbers, patient

IDs), or if a user tries to log onto the network from geographically separate locations within a short span of time.

- The cloud can also warn an enterprise security team when administrator accounts attempt unauthorized actions, or even when the enterprise has more administrators with elevated access privileges than strictly necessary.

- Some cloud applications (like our Office 365 collaboration suite) can automatically review the security settings your administrators have chosen across hundreds of indicators and give you a consolidated "security score" along with advice on how to improve it.[39] A major insurance company is already using this score to set cybersecurity insurance rates.



Office 365 Secure Score automatically evaluates all security settings in your enterprise's installation of Office 365, calculates an overall score, shows how you stand compared to peer enterprises, and tells you how to improve your score.

Prepare for cyber-risks of the Internet of Things. Until now we have considered only the cybersecurity issues raised by such "conventional" networked devices as servers, PCs, and mobile phones. But the world is already engaged in the next wave of dramatic growth in connected devices that will see billions of ordinary "things"—household appliances, cars, factory machinery, elevators, and countless less consequential devices such as light bulbs—connected to the cloud and enterprise networks. A conservative estimate is that this "Internet of Things" or IoT, will consist of 50 billion or more devices by 2020, and a far greater number within another decade.

Universal Internet connectivity of people, devices, and now things will permit entirely new and more intelligent behaviors by the devices that populate our daily lives and the invisible technical infrastructure of modern life. It will be a tremendous gain for the global economy and human welfare. Yet, given the experience we already have with cyberattackers on today's Internet, it is all too easy to anticipate that the IoT will bring a host of new dangers. With this in mind, enterprise leaders must build their IoT cybersecurity strategy at the same time they build their IoT business strategy.

A critical weakness in current incarnations of the IoT is that most IoT devices do not have security built in. Often this is because their manufacturers do not believe it is technically feasible or profitable to put enough processing power on board these devices to implement security in addition to their primary functions. Most IoT manufacturers also have little or no experience in developing enterprise-grade security software.

But these reasons should not be an excuse for deferring action. When billions of ordinary objects such as refrigerators and light bulbs can connect to the Internet, they will have the power—if

commandeered by malicious actors—to launch overwhelmingly destructive attacks on vital public services and infrastructure. A few early incidents of this kind have already occurred, although fortunately none yet with truly devastating consequences.[40]

The issue of IoT data integrity is especially important. While the computer security industry has spent decades obsessing over data confidentiality and availability, in a world where machines make life-altering decisions based upon data, it will be critical to ensure that the data has not been improperly or maliciously altered—consider medical devices and self-driving cars.

If a serious IoT crisis erupts, public opinion and government authorities may be tempted to blame enterprises that have deployed IoT networks, even if the attacks have been carried out by malicious actors entirely unknown to these enterprises. Consequently, enterprises with IoT plans should join us in advocating for appropriate regulations and standards that support IoT cybersecurity.

Today there is no global standard for IoT security, but several efforts are underway. As a leading cloud provider, Microsoft is participating in IoT security efforts in the world's major standards bodies. This is a fast-moving and very technical area. Here, we briefly summarize some key concepts that should be included in an IoT security standard. We believe every IoT device should be required to have the following elements:

- A hardware identifier, so networks can recognize the device
- Signed data, so the network knows that data from the device has not been altered

- The ability to receive software updates and patches, so that security vulnerabilities can be fixed when they are discovered

While waiting for formal IoT security standards to emerge, enterprise leaders should be aware that a body of best practices is already being developed based on a layered security-in-depth approach. Enterprise leaders should instruct their security and IoT teams to build these best practices into their IoT deployments from the ground up. Too much is at stake to leave IoT security as an afterthought.[41]

In short: What to do about cybersecurity

Understand the true nature of the threat

Require a unified security strategy that is applied by—and applies to—all.

Encourage innovation and learning, but don't let business units or individuals improvise security policies in isolation.

Rationalize your portfolio of security tools.

Limit the fragmentation of your security tools and insist that they be able to exchange data easily.

Delegate activities that are not part of your core value-creation.

Keep what you do better than anyone else or must do yourself in-house. Hand off activities that are not part of your core value-creation process to providers who can do a measurably better job.

Never forget that your enterprise retains ultimate responsibility for its own security.

As the cloud matures, the most important piece of the security puzzle remains in your hands: the conduct and actions of your employees.

360-degree security

Update your software and hardware.

To continue reaping the benefits of technological innovation, we must accept the cost of constantly swapping out the old for the new.

Patch your software.

No piece of software can ever be completely free of the programming errors or design flaws that unintentionally expose it to the probing of cyberattackers.

Use the new security features in modern operating systems to harden your endpoints.

The basic building block of your enterprise's cybersecurity wall is the device that connects each individual user to your network. You should take all available measures to harden these devices.

Always assume breach.

The reality in today's threat environment is that you will be breached at some point. Your ultimate goal should not be to stop something that is likely unstoppable, but to contain the damage as much as possible.

Protect your information assets with encryption.

If breach is a given (or very likely), then you must fortify not only your outer wall, but also important information assets inside the wall.

Identity is the new firewall

Require single identity.

The ideal scenario is to manage identity and authentication for all users, applications, and devices that access your information assets in a unified way, while enforcing specific policies that your security team establishes such as conditional access and multi-factor authentication.

Mandate multi-factor authentication.

The fundamental advantage of MFA is that it means stealing a username and password through a phishing attack is no longer enough for a hacker to break into your network.

Plan to move beyond the password.

Passwords are the single greatest chink in the cyberdefense armor of the modern enterprise.

Use mobile device management and data segregation.

Mobility management systems can control enterprise data and access on personal mobile devices.

Monitor and restrict privileged access.

The user who will be the prime target of attackers is the employee whose job requires him or her to have expansive access privileges on your enterprise network.

Machine intelligence and big data

Leverage the cloud provider's big data and machine learning advantages.

More data means more insight and makes possible new forms of cyberdefense.

Use automation and "nudges" from the cloud to help your employees avoid mistakes.

People should make decisions, not trouble.

Prepare to cope with the cyber-risks of the Internet of Things.

If a serious IoT crisis erupts, public opinion and government authorities will hold enterprises that have deployed IoT networks responsible.

Chapter 3

A cloud that respects privacy


125.150
71.870 TO ℄ CROSS MEMBER AND SPRING HANGER
℄ OF FRONT SUPPORT HOLES
℄ OF RADIATOR BRACKET
℄ OF REAR SUPPORT HOLES
℄ OF FRAME
BODY MTG. HOLES LOCATED ON THIS LINE MUST BE WITHIN .062 TO EACH OTHER FORE AND AFT.
1/2 DIA. PILOT HOLE (REF.)
℄ OF REAR AXLE
℄ OF FRONT WHEELS
114.000 WHEELBASE
178.050 OVERALL
60 BODY HOLE (PICK-UP)
78.130 BODY HOLE (PANEL)
511 AT ℄ FRONT ENGINE MOUNT
2.511 AT ℄ REAR ENGINE MOUNT
℄ OF ENGINE CYLINDER
℄ OF CRANKSHAFT
FRONT OF DASH
MODELS 2100
TRUCK INSTRUCTION MANUAL

A brief history of privacy

What you should know

The concept of privacy—or at least the narrower but related idea of secrecy—is not new. It was known even in the ancient world, where Julius Caesar famously used an alphabet shift cipher to encrypt military messages.[42] But the idea of a fundamental right to privacy enjoyed by all is much more recent, and its embodiment in actual legislation is more recent still.

In the United States, this idea can be traced back to the Fourth Amendment to the Constitution, which puts strong limits on the right of government to search and seize evidence from citizens. The Fourth Amendment remains to this day the foundation for American privacy law.

In Europe, most observers trace the emergence of the idea of a legally codified right to privacy to the aftermath of WWII.[43] Article 8 of the 1950 European Convention on Human Rights (ECHR) affirms that:

> "Everyone has the right to respect for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests."[44]

In the 1970s, concern over the rise of automated data processing applied to large volumes of records held by governments and corporations prompted Europeans to take a further step toward a modern law of privacy. The Council of Europe's Convention 108 of 1981 (also known as the Strasbourg Data Protection Convention)

was ratified by all EU member states and introduced the idea of "personal data," which was defined as "any information relating to an identified or identifiable individual."[45]

With this definition of personal data we have now almost reached the language of the EU's 1995 Data Protection Directive. The Directive codified the rights of European data subjects in great detail. In doing so, it introduced many important new ideas, such as the distinction between data controllers (who make decisions about how personal data is processed) and data processors (who carry out processing instructions from controllers).

The 1995 Directive has had a profound impact on the concept and practice of data privacy not only in Europe, but all over the world. In particular, it led to the Safe Harbor agreement between the U.S. and Europe in 2000, which created a framework that allowed firms processing personal data of Europeans in the U.S. to remain in compliance with the Directive.[46]

2000 saw another major step in Europe with the proclamation of the Charter of Fundamental Rights of the European Union, which serves as a constitutional document for the EU and was ratified by the 2009 Treaty of Lisbon. Notably, the Charter provides for both a right to privacy (like the ECHR) and a right to data protection (like Convention 108).[47]

Today of course the 1995 Directive is giving way to the EU's General Data Protection Regulation, which updates the Directive to account for the vast expansion in the power of automated processing of personal data that has occurred since 1995. We discuss the GDPR in detail in the following sections.

Privacy law in the United States in recent decades has followed a different course than in Europe. American legislators, like their European counterparts, have expanded the notion of privacy from protection against government intrusion to a much broader field that considers the privacy of personal data held by all sorts of non-governmental institutions, in particular for-profit entities such as corporations and nonprofit organizations such as schools and hospitals.

But a major difference between European and U.S. privacy law lies in the latter's focus on data privacy in specific economic sectors rather than privacy in general. Two prominent examples of this vertical industry focus in U.S. legislation are the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which establish rules for the protection of student educational records and patient health records.

Modern privacy legislation in the U.S. and Europe has become extraordinarily complex, and poses many difficult compliance challenges for organizations with computer applications that handle large amounts of personal data. This compliance burden has now spread to most other regions of the world as well, where the example of EU data protection law has been highly influential. Dozens of nations in Asia, Latin America, the Middle East and Africa have adopted laws in recent years that are consciously modeled, at least in part, on the EU's 1995 Directive.

At Microsoft we have spent years investing in privacy law compliance. We have hundreds of lawyers and other specialists dedicated to this task. They work closely with our engineers to

make sure our software and cloud services comply with the ever-expanding body of global privacy laws, both those that are general (like the GDPR) and those that are specific to certain sectors (like HIPAA). And we work just as hard to help you make sure that the business applications you build with our products also comply with the law. In this chapter and the next we provide an overview of these efforts and offer some practical advice on how you can ensure that your organization not only achieves compliance, but maintains it.

Privacy milestones: Milestones in history of modern privacy law	
1950	European Convention on Human Rights
1974	U.S. Family Educational Rights and Privacy Act of 1974 (FERPA)
1981	Council of Europe Convention 108
1996	U.S. Health Insurance Portability and Accountability Act (HIPAA)
1995	EU Data Protection Directive 95/46/EC
2000	Charter of Fundamental Rights of the EU
2000	EU-U.S. Safe Harbor
2016	EU-U.S. Privacy Shield
2018	EU General Data Protection Regulation (GDPR)

Machine learning in the cloud delivers healthcare while protecting patient privacy

As the U.S. struggles to control healthcare costs, a new model for medical payments is gaining popularity. Instead of traditional "fee for service" where healthcare providers are paid for procedures regardless of outcome, insurers and government programs such as Medicare are shifting to "value-based care." In this model, providers are paid for successful health outcomes.

Startup KenSci has developed a cloud-based health risk prediction application with machine learning. Caregivers need to identify high-risk individuals before they get sick. KenSci builds mathematical models that incorporate hundreds of variables ranging from genetics, demographics, income, and psychosocial factors to living situation, childhood illnesses, and even the patient's postal code.

Medical privacy was a key factor in KenSci's choice of Azure. HIPAA (Health Insurance Portability and Accountability Act) is a U.S. law that sets strict rules for the safeguarding of patient health information. Microsoft has worked diligently to extend HIPAA compliance across its portfolio of cloud services.

"HIPAA compliant Azure ML will lower the complexity of analyzing large health datasets leading to rapid deployment of our state-of-the-art ML models for the patient care continuum."

—Professor Ankur Teredesair, Co-founder of KenSci

Making lifesaving predictions is a perfect illustration of how Machine Learning and cloud-scale computing can deliver lifesaving breakthroughs in patient care.

Understanding the GDPR

What you should know

What is the GDPR? Simply put, the GDPR is the European Union's sweeping new data protection law, also known by its full name of "General Data Protection Regulation." Fundamentally, the GDPR is about personal privacy rights, or more specifically about the rights of individuals to control what happens to data that is about them.[48]

Although the GDPR preserves many of the principles of previous EU privacy law, it is much more ambitious. Among its most notable changes, it gives individuals much more direct control over their personal data and imposes many new obligations on organizations that collect, handle, or analyze such data. The GDPR also gives national regulators new powers to impose large fines on organizations that violate the law.

The GDPR will take effect on May 25, 2018. This is the date that actual enforcement begins by EU data protection authorities. The law was passed in April 2016, but the EU recognized that a lengthy transition period was necessary to help organizations make the many changes the law mandates.

You should not assume that all regulators will allow a grace period beyond May 25, 2018. Some EU member-state regulators have already said there will be no enforcement holiday for organizations that fail to comply. You should also be aware that the application of GDPR is highly specific to the facts and circumstances of your company. Moreover, notwithstanding the enforcement deadline, many details of the GDPR remain unsettled. More detailed guidance will come through the establishment of industry codes of conduct and likely also through litigation.

The GDPR is not just about privacy rights in Europe. It will impact all those doing business with Europe, no matter what their location. And because legislators, regulators, and concerned citizens in other parts of the world often view the EU as a role model on privacy issues, we expect to see key concepts from the GDPR adopted in privacy laws and data protection regulations in many other regions in the coming years. Thus, GDPR will impact privacy rights in the rest of the world as well, setting a new global bar for privacy, security, and compliance. At Microsoft, we believe privacy is a fundamental human right and that the GDPR is a major step forward in enhancing and securing the privacy rights of individuals.

> **"GDPR means enhanced privacy rights for people and that's a good thing."**
>
> —Brad Smith, President and Chief Legal Officer of Microsoft

What you should do

Determine if the GDPR applies to your organization. No matter where your organization's activities may be located, if it has any kind of relationship at all with EU residents—whether they be customers, non-paying website visitors, employees, or business partners—then there is a good chance the GDPR almost certainly applies to it.

The GDPR applies more broadly than you might think at first glance. Unlike privacy laws in some other jurisdictions, the GDPR applies to organizations of all sizes and all industries. Specifically, the GDPR applies to:

- Processing of anyone's personal data, if the processing is done by an organization established in the EU (regardless of where the processing itself takes place)

- Processing of personal data of individuals who reside in the EU by an organization established outside the EU, where that processing relates to the offering of goods or services to those individuals or to the monitoring of their behavior

Understand the broad principles driving GDPR compliance. The GDPR is a dense and complex legal text that contains 173 recitals and 99 articles and over 50,000 words in its English language version.[49] It imposes a wide range of requirements on organizations that collect or process personal data. While nothing can replace a systematic review of the text by your legal and compliance team to determine the exact requirements you face, it is useful to think of GDPR compliance in terms of six principles for processing personal data:

1. **Lawfulness, fairness, and transparency.** You will need to be fully transparent with individuals—which includes your own employees—about how you use their personal data. You must always have a lawful basis for processing that data, such as consent, as part of a contract with the data subject, or other lawful means described in the GDPR's Article 6. Where consent is the basis, it will need to be consent that is "freely given, specific, informed, and unambiguous," not merely the passive consent of a user who does not opt out.

2. **Purpose limitation.** You must restrict the processing of personal data to specified, explicit, and legitimate purposes.

You will not be able to reuse or disclose personal data for purposes that are not "compatible" with the purpose for which it was originally collected.

3. **Data minimization.** You must restrict the collection and storage of personal data to the minimum that is adequate and relevant for the intended purpose.

4. **Accuracy.** You must ensure that the personal data you hold is accurate and permit users to request that it to be erased or rectified.

5. **Storage limitation.** You will need to ensure that you retain data in a personally identifiable form only for as long as necessary to achieve the purposes for which it was collected.

6. **Data integrity and confidentiality.** You must take steps to ensure the security, integrity, and confidentiality of personal data. Your organization must implement appropriate technical and organizational security measures.

Recognize that the GDPR defines "personal data" very broadly. The GDPR regulates the collection, storage, processing, and sharing of "personal data." Personal data is defined under the GDPR as *any information that relates to an identified or identifiable natural person*. This can include data such as online identifiers (for example, IP addresses), employee information, sales databases, customer feedback forms, location, biometric data, CCTV footage, loyalty scheme records, health records, financial information, and much more.

The GDPR's definition of personal data is so broad that it can even include information that does not appear to be personal at all—for

example, a photo of a landscape without people—if that information is linked by an account number or unique code to an identifiable individual. And even personal data that has been pseudonymized can still count as personal data if the pseudonym can be linked to a particular individual.

You should also be aware that the processing of certain "special" categories of personal data–such as personal data that reveals a person's racial or ethnic origin, or concerns their health or sexual orientation–is subject to more stringent rules than the processing of "ordinary" personal data.

Identify any data you transfer out of Europe. Many organizations serving EU residents routinely transfer personal data concerning those residents for processing or storage in countries outside the EU. For example, you may operate a U.S. or Asia-based web portal that EU residents can access. Your human resources system may store personal data about your EU employees in a system housed elsewhere—perhaps in the data center of a non-EU cloud provider. Or your CRM system may contain a central data warehouse that rolls up data about your customers from every region of the world.[50]

Nothing in the GDPR forbids these transfers outside of the EU, so long as organizations that move the data have a lawful basis to do so and use "appropriate safeguards." The EU has defined a number of such safeguards for the transfer of personal data, including:

- Model Clauses—a standard EU-defined contract that is entered into between service providers and their customers

- EU-U.S. Privacy Shield—an agreement between the EU and the U.S. creating a process for companies to self-certify to key protections for data

- Binding Corporate Rules (BCRs)—a complex process that involves entering into an agreement with relevant data protection authorities in the EU

- A determination by EU authorities that the receiving country has equivalent data protections to those in the EU[51]

Know that GDPR imposes stringent new breach notification requirements. The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." If a personal data breach occurs, the GDPR requires data controllers to notify their supervisory authority within 72 hours of detecting the breach, unless the breach is not likely to lead to a risk to the rights and freedoms of individuals. Controllers may also need to notify affected individuals if there is a significant risk of harm due to the breach. Processors are required to provide notice to controllers without undue delay.

For many firms, the breach notification requirement may be the biggest practical consequence of GDPR. The new rules will significantly increase the stakes for organizations that suffer a breach resulting in the disclosure of personal data. As discussed in the sub-chapter on cybersecurity, organizations must guard access rights rigorously by protecting credentials. It is also important to

carefully limit the scope of access even for users such as system administrators whose job roles require higher than normal access privileges. And it is highly advisable (though not legally required) to encrypt personal data, not only while it is in transit over a network, but also when it is at rest (that is, stored on a server). The majority of recent breaches of customer data have involved compromised access credentials or unencrypted data, or both.

Embrace the GDPR—it's the law and it's here to stay. For the past several decades, European privacy laws have generally not included significant fines for violations. That will change dramatically under the GDPR. The maximum fine for serious infringements will be the greater of €20 million or four percent of an organization's annual global revenue. In addition, the GDPR empowers consumers (and organizations acting on their behalf) to bring civil litigation against organizations that fail to comply with the GDPR. In short, for any well-run organization focused on serving the interests of its stakeholders, not complying with the GDPR is simply not an option.

Building out full GDPR compliance in your organization will be a long journey. In a very real sense, it will be a journey that never ends, because compliance is an ongoing requirement that must be continually adjusted and monitored as new personal data flows into your organization and as new business processes or data processing methods—including artificial intelligence—are deployed.

At the end of the day, embracing the GDPR is the best and only strategy. It is the right thing to do for personal privacy, and it will be legally mandatory for any organization in the world that processes personal data of EU residents.

Complying with the GDPR

What you should know

Complying with the GDPR requires board leadership. As we have seen in the chapter on Digital Transformation above, the value-creation process in modern enterprises is increasingly dependent on the interaction between vast amounts of information and software-based intelligence. The information that drives your business and flows through its component business processes will inevitably contain large quantities of personal data. Thus your core value-creation strategies will be directly impacted by the GDPR.[52]

Moreover, the board has a fiduciary responsibility to shareholders to protect the interests of the business and to address potentially negative, materially impacting events before they happen. Receiving a large fine or being banned from doing business in the EU would have a material impact on any firm.

Especially for large organizations, compliance will be a business-wide effort that will take time, tools, expertise, and investment. In all likelihood it will require considerable changes to your privacy and data management practices.

Given the scale and scope of the GDPR challenge, its strategic importance, and the consequences for non-compliance, it is essential that your organization's board of directors and CEO take the lead in establishing a GDPR strategy and verifying that it is implemented correctly.

Compliance with GDPR requires an empowered Legal and Compliance team. The many complex technical details of GDPR implementation are vitally important and are properly delegated to your IT, privacy, and security leaders. Because virtually all personal data processed by organizations is stored in electronic form,

technology will inevitably play a central role in your march toward compliance. Nevertheless, compliance is still fundamentally about business process and culture. Consequently, the board and the CEO should work closely with your Legal and Compliance team, led by your General Counsel or Chief Legal Officer, to build the requisite culture of compliance. This team may also include a Data Protection Officer, a position which is defined by the GDPR and will be mandatory for any organization significantly involved in the processing of personal data (as defined by Article 37 of the GDPR).[53]

Compliance with GDPR requires a holistic approach. Your organization or its partners may use many different systems to handle personal data. These systems likely include servers on your premises and in the cloud, PCs, tablets, smartphones, and—last but not least—devices in your factories or on your customers' premises. With the rise of the Internet of Things, even something as ordinary as a consumer household appliance will be impacted by GDPR. In short, nearly any system or device, no matter how simple, that processes or stores personal data and sends it back to a controller can fall within the scope of the GDPR. Consequently, your approach to GDPR must look holistically at your entire technology landscape, both inside and outside the walls of your organization.

Your journey to GDPR compliance will go more smoothly if you have a well-architected enterprise data model and an effective data governance program in place. In particular, the more of your IT assets that are cloud-native or have migrated to modern cloud platforms, the straighter the path to achieving and maintaining compliance will be. Finding and cataloguing the different kinds of personal data an organization possesses is generally much easier in the cloud. Also, modern cloud services are built using the principles of Privacy by Design[54] and are designed to enable compliance with the GDPR and other new legal requirements.

For instance, many of the technical and organizational measures to prevent, detect, or respond to vulnerabilities and data breaches required by the GDPR are similar to the controls expected by other data protection standards, such as the ISO 27018 cloud privacy standard. Rather than track the controls required by individual standards or regulations on a case-by-case basis, a best practice is to identify an overall set of controls and a set of capabilities to meet these requirements.

What you should do

Understand the four steps in the compliance process. Although the process of achieving and maintaining GDPR compliance is complex, at a high level it can be broken down into four fundamental steps, which we review here: Discover, Manage, Protect, Report.

1. **Discover: Identify what personal data you have and where it resides.** The GDPR regulates the collection, storage, use, and sharing of "personal data." Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person.

To understand whether the GDPR applies to your organization and, if it does, what obligations it imposes, your IT and Legal and Compliance teams will have to undertake a systematic inventory of your organization's data. This will help you to understand what personal data you are currently processing. It will also identify the systems where that data is collected and stored, and understand why it was collected, how it is processed and shared, and how long it is retained.

Keep in mind that the GDPR also applies through you to third parties you work with. These include cloud service providers, IT and business process outsourcers, payment processors, advertising companies, shipping companies, and other business partners who may have access to personal data on your behalf. You must seek appropriate legal assurances from these third parties that they "implement appropriate technical and organizational measures" to meet GDPR requirements and to protect the rights of data subjects.

2. **Manage: Govern how personal data is used and accessed.** The GDPR provides data subjects—individuals to whom data relates—the right to more control of how their personal data is captured and used. Data subjects can, for example, request that your organization delete data that relates to them, transfer their data to other services, correct mistakes in their data, or restrict certain data from further processing in certain cases. In some cases, these requests must be addressed within fixed time periods.

To satisfy your obligations to data subjects, you will need to understand what types of personal data your organization processes, how, and for what purposes. The data inventory mentioned above is a first step toward this understanding. Once that inventory is complete, you must also develop and implement a data governance plan. This plan can help you define policies, roles, and responsibilities for the access, management, and use of personal data, and will allow you to verify that your data handling practices comply with the GDPR. Among other things, a good data governance plan can give your organization confidence that it effectively respects data subject demands to delete or transfer data.

3. **Protect: Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.**

Organizations increasingly understand the importance of information security, but the GDPR raises the bar. It requires that organizations take appropriate technical and organizational measures to protect personal data from security breaches leading to loss or unauthorized access or disclosure.

Data security is a complex area. There are many types of risk to identify and consider—ranging from physical intrusion to rogue employees to accidental loss or hackers. Building risk management plans and taking risk mitigation steps, such as password protection, audit logs, employee training, and encryption, can help you ensure compliance. We review these and other data security issues at greater length in the previous chapter, "A Secure Cloud."

4. **Report: Execute on data requests, report data breaches, and keep required documentation.** The GDPR sets new standards in transparency, accountability, and record-keeping. You will need to be more transparent about not only how you handle personal data, but also how you actively maintain documentation defining your processes and use of personal data.

Organizations with more than 250 employees that collect personal data will need to keep records about the purposes of processing; the categories of personal data processed; proof of the lawful basis for this processing by data subjects; the identity of third parties with whom data is shared; whether (and which) third countries receive personal data, and the legal basis of such transfers; organizational and technical security measures; and data retention times applicable to various datasets. Audit tools that track and record processing of data—whether it be collection, use, sharing, or otherwise—can help with some of these requirements.

In certain cases, the GDPR requires that when a controller becomes aware of a data breach, it needs to rapidly notify regulators. In some cases, organizations will also need to notify the affected data subjects. To meet this requirement, organizations will benefit from being able to monitor for and detect system intrusions.

Know how to respond to a breach. The GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." Once you have detected a potential breach, we recommend (and use for our own incident response program) a four-step process:

- Assess the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to a cybersecurity/data protection response team.

- Conduct a technical or forensic investigation, and identify containment, mitigation, and workaround strategies. Once the cybersecurity/data protection team becomes aware that personal data may have been subject to a breach, a notification process begins in parallel as called for in the GDPR.

- Create a recovery plan to mitigate the issue. Crisis containment steps such as quarantining affected systems should occur immediately and in parallel with diagnosis. Longer-term mitigations may be planned to occur after the immediate risk has passed.

- Create a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a recurrence of the event.

Respect the rights of data subjects. Among the most significant elements of the GDPR are the rights of the "data subject." These rights will bring substantial new obligations both for you and your cloud providers.

What are these rights? Among others, they include each individual user's right to:

- Access readily available information in plain language about how their personal data is used, how long it will be retained, and other details
- Access their personal data
- Have personal data rectified and/or erased in certain circumstances (the latter case is sometimes referred to as the "right to be forgotten")
- Restrict or object to processing of personal data, or withdraw previously granted consent for such processing
- Receive a copy of their personal data
- Object to processing of data for specific uses, such as marketing or profiling

Ensuring that all your new and existing IT applications respect these data subject rights will not be a trivial undertaking. In particular, the GDPR requirement that you allow users to see data you have about them and control its use may require significant modifications to legacy applications. You should consider carefully whether it is worthwhile to make these changes, or whether it would be better to migrate to more modern cloud-based applications that already have these features designed in from the ground up.

Last but not least, understand the shared responsibility between you and your cloud providers for GDPR compliance. The GDPR is a complex piece of legislation, but its fundamental intent is simple: to give individuals more control over their data. However, providing them with that control is a task that requires some revision of current information processing practices. Corporate business processes and the information systems that support them are themselves quite complex. A seemingly simple action such as recording a customer's purchase transaction and payment information might involve multiple computers owned by multiple organizations operating in multiple locations—possibly on multiple continents. The difficulty of course lies in determining just who is responsible for each piece of this chain of processing of data, as well as the related storage of data, which is also covered by the GDPR.

In broad terms, the GDPR distinguishes between two fundamental roles that an organization can play in processing personal information. A **data controller** is defined by the GDPR as:

- "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

A **data processor** is:

- "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[55]

Consider the case where your enterprise subscribes to a cloud service such as our Office 365 email and collaboration suite. Here, you are the controller, because you determine how and why your users' personal data is processed by the cloud service. Microsoft, as the processor, carries out your instructions to process that data—and, as the GDPR stipulates, must take care to perform no other processing than that which you, the controller, have specifically authorized. That means that we are not allowed, for example, to "data mine" your users' email messages unilaterally for our own purposes, such as targeting online advertising at them. In the future, as artificial intelligence advances, customers will no doubt expect cloud services to do many things to personal data to make it more useful, but this can only happen with proper authorization.

Under previous EU data protection law, almost all the compliance burden fell on the controller. For instance, it was and remains the controller's obligation to obtain proper consent for processing from individuals or establish another legally acceptable justification for processing their data. Few if any specific responsibilities fell on the processor.

But under the GDPR things will be different. Processors will be subject to tighter constraints in how they carry out processing activities on behalf of a controller. In particular, they will be required to comply strictly with controller instructions, keep records of that activity, cooperate with data protection authorities,

take appropriate security measures, and comply with restrictions on the transfer of data outside the EU. Failure to meet these obligations will subject processors to the same fines that controllers risk—set by GDPR as up to 4 percent of annual turnover or €20 million, whichever is greater.

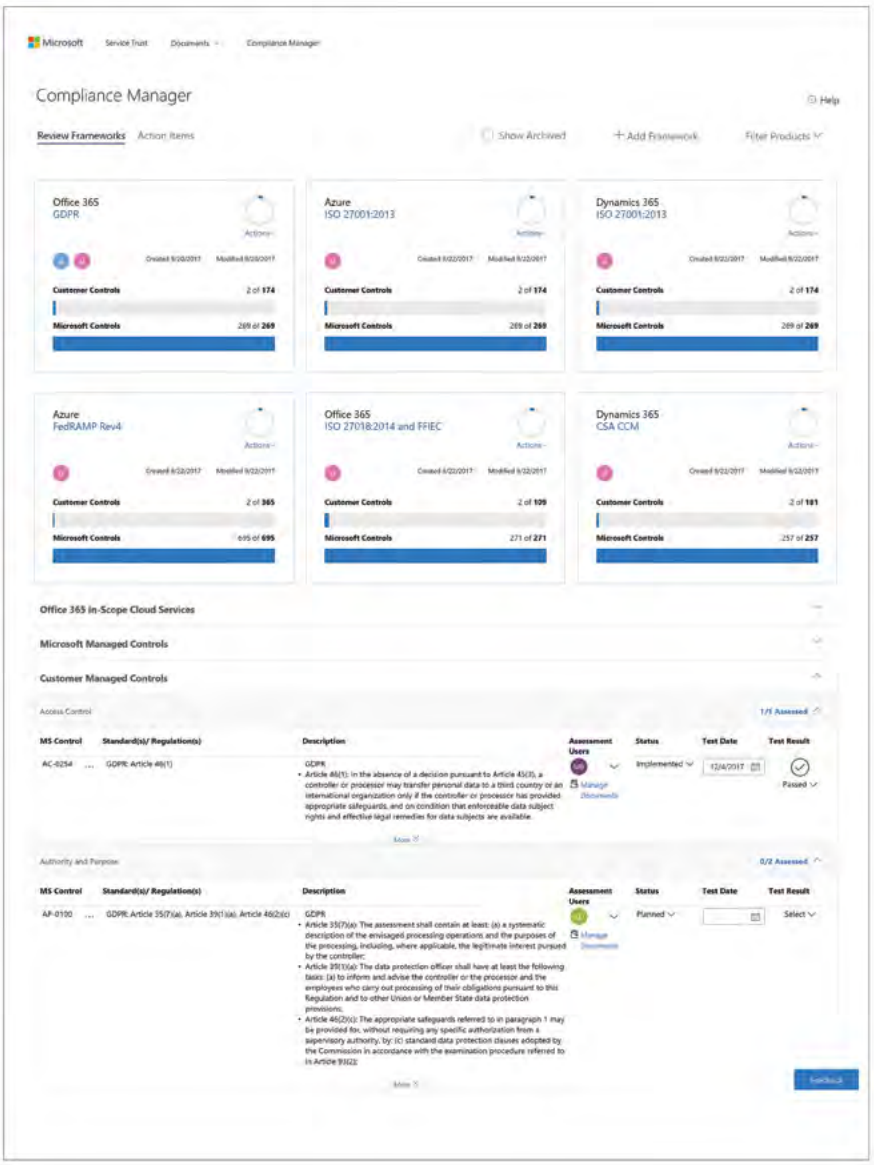
The frontier between controller and processor will not always be easy to establish. In some cases your cloud provider may be both. For example, a controller for the administrative data of your enterprise account with the service, but a processor for the user data that the provider processes on your behalf. You will need to consult closely with your legal and compliance team to determine exactly where the boundary lies given the specific circumstances of your enterprise.

As you can see, achieving compliance with the GDPR will require close collaboration between your organization and your cloud providers on both legal and technical matters. We offer many tools and resources that can help you, including an extensive library of GDPR white papers,[56] detailed self-assessment tools,[57] and contracts. These resources have been thoroughly updated to provide you with critical assurances of Microsoft's support for your GDPR compliance efforts.[58] Recognizing that achieving compliance requires more than just words, we also have hundreds of engineers working on an end-to-end re-engineering of our software and services to create a single data privacy architecture for all Microsoft products and to support GDPR compliance.

Microsoft's commitment to you and to all of our enterprise customers is that we will do everything in our power to comply with the GDPR's rules on our end, and we will provide you with the best tools we can create to help you do the same on your end.

"We're the one company that has been prepared to put our contracts behind our words and commit to you and others around the world that you can count on us to ensure that our services are GDPR compliant."

—Brad Smith, President and Chief Legal Officer of Microsoft


Microsoft
Service Trust
Documents
Compliance Manager
Compliance Manager
Help
Review Frameworks
Action Items
Show Archived
+ Add Framework
Filter Products
Office 365
GDPR
Azure
ISO 27001:2013
Dynamics 365
ISO 27001:2013
Customer Controls
2 of 174
Microsoft Controls
269 of 269
Azure
FedRAMP Rev4
Customer Controls
2 of 365
Microsoft Controls
695 of 695
Office 365
ISO 27018:2014 and FFIEC
Customer Controls
2 of 109
Microsoft Controls
271 of 271
Dynamics 365
CSA CCM
Customer Controls
2 of 181
Microsoft Controls
257 of 257
Office 365 in-Scope Cloud Services
Microsoft Managed Controls
Customer Managed Controls
Access Control
1/1 Assessed
MS Control
Standard(s)/ Regulation(s)
Description
Assessment Users
Status
Test Date
Test Result
AC-8254
GDPR: Article 46(1)
GDPR
Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
Implemented
12/4/2017
Passed
Authority and Purpose
0/2 Assessed
MS Control
Standard(s)/ Regulation(s)
Description
Assessment Users
Status
Test Date
Test Result
AP-0100
GDPR: Article 35(7)(a), Article 39(1)(a), Article 46(2)(c)
GDPR
Article 35(7)(a): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
Article 39(1)(a): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
Article 46(2)(c): The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorization from a supervisory authority, by: (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
Planned
Select

Manage regulatory compliance with one tool

Complying with legislation such as the GDPR can be a significant burden for organizations that handle large amounts of personal data. Determining exactly what the rules mean for your organization is already challenging. Then the effort to meet them can demand a great deal of costly and time-consuming manual labor by your staff and outside advisors. Two-thirds of firms rank "design and implementation of internal processes" the biggest GDPR hurdle. In short, documenting your compliance actions and verifying that they have been completed properly needs sustained attention. And consider that GDPR is certainly not the only regulation you must comply with.

750 regulatory bodies in the world issue some 200 updates per day to their rules. To cope with these challenges, Microsoft is developing a new compliance management tool to help organizations meet their data protection and regulatory standards more easily when using our cloud services. Compliance Manager supports three key aspects of the process:

Real-time risk assessment: Compliance Manager provides a summarized dashboard showing your compliance posture against specific data protection regulatory requirements when using Microsoft cloud services. Each assessment framework provides a compliance score that reflects your real-time compliance posture and helps assess your risk.

Actionable insights: For Microsoft-managed controls, you can see the control implementation and testing details, test date and results. For customer-managed controls, you receive recommended actions with step-by-step guidance for implementation and testing.

Simplified compliance workflow: Compliance Manager includes a tool to assign tasks and collaborate across teams. You can generate audit-ready reports with evidence, reducing the need to collect information manually. This tool helps compliance teams and risk assessors perform proactive assessment and prepare for audits.

Managing privacy risk

What you should know

Concern among enterprise leaders about the damage a major data breach could cause to their organization is understandably high. Recent years have witnessed a wave of cyberattack horror stories. The recounting of these stories in the media has been as humiliating for the corporate victims as it has been frightening for the rest of us—who still hope never to become victims ourselves.

It is sobering to think that a careless action by one of your employees or a bug in a piece of software could cause your enterprise to disclose sensitive private information about thousands or even millions of your customers. Yet we see these events happening all around us.

> **"There is no privacy without security."**
>
> —Brad Smith, President and
> Chief Legal Officer of Microsoft

Managing risk is a fundamental part of protecting privacy. But the harsh reality is that risk is everywhere. It will never be possible to eliminate it. The only solution is to manage it. Enterprise leaders must adopt a risk management approach that identifies and compares the different kinds of risk. This means prioritizing risks in terms of both the cost of the possible damage incurred and the likelihood of occurrence.

Should your enterprise be planning for the possibility of an asteroid strike? Probably not. But we should all hope that NASA is. Should enterprises plan for the possibility that inadvertent or malicious breaches will lead to the disclosure of sensitive personal information about their customers? Absolutely. The most

devastating possible breach will be incomparably less costly than an asteroid strike, but also incomparably more likely in statistical terms.

Privacy risk management begins with a thorough and realistic ranking of the threats your enterprise faces. You might give a composite score to each risk that balances its likelihood with its potential cost. Then, each risk must be matched with feasible mitigating actions that reduce both the chances of it actually occurring (pre-breach defenses) and the consequences if it does occur (post-breach defenses).

An effective ranking of privacy risks may cause you to revise previous beliefs about what is important.

Consider the possibility that a court order compels your cloud provider to turn over sensitive information about one of your customers or employees. Such things happen. At Microsoft, in recent years we have found it necessary to sue our own government on several occasions when we believed it was acting beyond the bounds of its lawful authority. For example, we have resisted U.S. government orders to turn over customer data stored in our European data centers when we believe it would violate EU laws. We have also sought the right to tell our customers when the government seeks to access their data. As a result of a Microsoft lawsuit, the U.S. Department of Justice recently issued a new policy limiting the use and duration of orders compelling cloud providers to keep instances of government surveillance secret from customers.[59]

You might be tempted to say: "We want to be 100% certain that no government can access data in our enterprise cloud without us being notified." But under current laws in the United States and many other nations, this is not possible. As a law-abiding

corporation, we cannot refuse to comply with what appear to be lawful government orders, even if we do challenge them in court when their legality is not clear. But we can't guarantee that we will always win these cases.

Moreover, you have no certain protection against government action even when the data is stored on your own premises. Law enforcement authorities with a valid warrant can show up without warning at your data center and impound servers or disk drives containing data they seek.

Instead of focusing on the possibility of government access to data stored in the cloud, enterprise leaders should ask: "What is the risk of hacker access to our data compared with the risk of government access?"

As a cloud provider, Microsoft's strongly held view is that governments should address data requests to the enterprises that own the data, not to us. And indeed, the reality is that governments rarely ask for data belonging to our enterprise customers. In the rare instances that they do, it is not for the purpose of stealing intellectual property or putting confidential information up for sale on the black market.

But in fact, it is much more common for governments to issue warrants or subpoenas for cloud data belonging to individual consumers, for example in the course of criminal investigations. For an enterprise, both the likelihood and the costs of a successful hacker attack on your data are far greater than that of government surveillance.

In short, when assessing the privacy risk of storing sensitive data in a cloud service operated by a third party, you must compare it with

the risk of storing the data on your own premises. In many cases, you will find that the risk to data privacy on premises is as great or greater than to data in the cloud. By prioritizing risks, you improve your chances of protecting the things that matter most.

At the same time, you cannot assume that cyberattackers will target the information assets on your network that you consider most valuable. Rather, they will look for the assets they think are most valuable.

The lesson is clear: when prioritizing the cyber-risks your organization faces, you must look at your information assets from both points of view—your own and that of your potential attackers.

What you should do

Because sound cybersecurity is the prerequisite for preserving data privacy, you should benchmark your cybersecurity against your peers and your cloud providers. It's hard to plan for cybersecurity if you don't know where you stand. It's difficult to measure improvement if you don't know what others are doing better than you. Cybersecurity benchmarking is therefore essential.

As we mentioned in a previous chapter, some cloud applications can automatically evaluate the security settings your administrators have chosen and compare them to your peers. But in general, there is no straightforward formal methodology for benchmarking the cybersecurity status of an entire enterprise. The task has too many variables to capture in a single formula.

The best approach is to assign the task to a small team of experts with a mix of skills and organizational roles. The team might include some outside experts, but should be led by a senior member

of your own staff. The team's work can be divided into the five stages described in the following table.

Protect data privacy by benchmarking your cybersecurity in 5 stages	
Prioritize risks	Identify and prioritize your organization's greatest information risks (intellectual property theft? GDPR non-compliance? financial fraud? consumer data leak?), considered in terms of overall impact and likelihood rather than specific attack methods.
Assess defenses	Assess your technical cyberdefenses against these prioritized risks, relying on your own technical experts and selected outsiders. Use a red team approach to ensure that negative findings are not overlooked. When a major breach occurs elsewhere, start with the default assumption that you face the same vulnerability and work to eliminate that possibility.
Learn from peers	Pursue an informal but structured and regular exchange of information about risk priorities and cyberdefense techniques with your industry peers at multiple levels (board, CEO, General Counsel, CISO, CIO, line-of-business, technical expert).
Learn from cloud leaders	Compare your assessed cybersecurity status against that of leading global cloud providers (as best-in-class benchmarks), and ask them to assess yours as well.
Adjust policies	Adjust your cyberdefense policies as indicated by these assessments, exchanges, and comparisons.

Cyberdefense assessment should be seen as a continuing process of steering and course correction rather than a one-time event. In the long run, we believe you are likely to find that most of your information assets are best entrusted to commercial cloud services managed by global leaders in cybersecurity.

When the cloud is not an option, consider a hybrid architecture. What about information assets that simply cannot be entrusted to the cloud, either because of legal mandates (for example, certain types of patient medical records) or because of extreme sensitivity (for example, national security secrets)? Does this mean you must give up the flexibility and security of the cloud, retreating to legacy on-premises IT as the only option?

Not necessarily. When it is not possible to bring your information to the cloud, you can bring the cloud to your information. Thanks to what the industry calls "hybrid cloud," it is now technically feasible to install in your own data center the same cloud management software used by global cloud providers in theirs.[60] Based on policies and priorities you set, the hybrid software will ensure that certain kinds of data never leave your premises, while others are seamlessly passed to the cloud. Although your IT staff will know the difference and will retain direct physical control over your most sensitive information assets, from the point of view of your users and business units, launching an application will look the same whether it happens in a distant cloud or on your own premises.

Build a robust post-breach plan, then staff and train for it. "Assume breach" does not mean that a breach with catastrophic consequences is inevitable. It means there is a high probability that some breaches will occur, and that you must plan ahead to contain and minimize the damage they do (while still striving to keep their chances of happening low).

A detailed plan for post-breach action is essential. Your leaders must know what they will say to customers, employees, regulators, and the media. Your legal and compliance team must understand your disclosure obligations under data protection laws such as the GDPR and be prepared to meet their deadlines. Your IT team must have a plan for restoring any compromised information assets, applications, or IT infrastructure. Your cybersecurity team must be equipped to find and remove any malware that still lurks in your network, while conducting a forensic investigation to determine how the incident occurred and reduce the chance of it happening again.

Experience demonstrates that enterprises which suffer a major breach can recover quickly if they address the situation forthrightly and effectively. But enterprises that commit additional cybersecurity, public relations, or regulatory blunders after the initial breach often suffer a prolonged crisis. Enterprise leaders who bury their heads in the sand usually pay a high personal price. Dismissive statements in the early hours after a breach becomes public can be particularly damaging.

It is unpleasant to contemplate the aftermath of a disaster that, likely as not, may have begun with a small error by one of your own employees. But it is much better to contemplate the possibilities now than to thrash and grope in the throes of crisis.

Finally, while practicing disciplined risk management, you should not entirely neglect the possibility of a "black swan" or "asteroid strike" event—that is, a highly unlikely but utterly destructive event. While not investing disproportionate resources to cope with such an event, you should at least determine what your options would be if one occurred. In the crisis of 2008, the difference between financial institutions that survived and those that did not was most often a matter of building resilience before the shock wave hit.[61]

Calculating risk at truly global scale

Willis Towers Watson's specialty is developing complex mathematical models that help insurance companies price their policies. Insurance is all about evaluating risk. Will these patients get sick? Will this driver have an accident? Will a hurricane strike this city? But making predictions is difficult, especially about the future.

Risk Agility FM is the firm's platform for modeling the financial risk of insurance pricing decisions. Insurers use it to understand the financial reserves they need to maintain to cover their policies for decades to come. When insurers were smaller, risks lower, and regulations fewer, those models ran on a workstation. Today, things are far more complex, and it's common for insurers to run the software on scores or even hundreds of compute nodes.

To test the scalability of its software on Microsoft's Azure Batch cloud service, the firm decided to try an experiment. But it needed to ask its model for the answer to a very big question. The question it chose was this: How much capital would be needed to underwrite a $100,000 life insurance policy for every child, woman, and man on earth—the more than 7 billion inhabitants of our planet?

Willis Towers Watson estimated that to run this model on a computer with only a single core would take about 19 years. With Microsoft's help, it tested the model on 100,000 cores on Azure. The result? Only two hours of compute time were needed, 100,000 times faster than on a single core. And how much would it cost to underwrite life insurance for the entire world? About $189 trillion.

In short: What to do about privacy

Understand the history of privacy law

Milestones

1950 European Convention on Human Rights

1974 U.S. Family Educational Rights and Privacy Act of 1974 (FERPA)

1981 Council of Europe Convention 108

1995 EU Data Protection Directive 95/46/EC

1996 U.S. Health Insurance Portability and Accountability Act (HIPAA)

2000 Charter of Fundamental Rights of the EU

2000 EU-U.S. Safe Harbor

2016 EU-U.S. Privacy Shield

2018 EU General Data Protection Regulation (GDPR)

Understand the GDPR

Determine if the GDPR applies to your organization.

The short answer is that the GDPR almost certainly applies to you.

Understand the broad principles driving GDPR compliance.

Review the 6 key principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Data integrity and confidentiality

(continued)

Recognize that the GDPR defines "personal data" very broadly.

Personal data is defined under the GDPR as any information that relates to an identified or identifiable natural person.

Identify any data you transfer out of Europe.

The GDPR strictly regulates transfers of personal data tied to European residents to locations outside the European Economic Area.

Know that GDPR imposes stringent new breach notification requirements.

In the event of a personal data breach, the GDPR requires you to notify regulators within 72 hours of detecting the breach.

Embrace the GDPR—it's the law and it's here to stay.

For any well-run organization focused on serving the interests of its stakeholders, not complying with the GDPR is simply not an option.

Comply with the GDPR

Understand the four steps in the compliance process.

Discover: Identify what personal data you have and where it resides.

Manage: Govern how personal data is used and accessed.

Protect: Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.

Report: Execute on data requests, report data breaches, and keep required documentation.

(continued)

Respect the rights of data subjects.

These rights will bring substantial new obligations both for you and your cloud providers.

Last but not least, understand the shared responsibility between you and your cloud providers for GDPR compliance.

The difficulty lies in determining just who is responsible for each piece in the chain of processing of data.

Manage privacy risk

Benchmark your cybersecurity against your peers and your cloud providers.

It's hard to plan for cybersecurity if you don't know where you stand.

When the cloud is not an option, consider a hybrid architecture.

When it is not possible to bring your information to the cloud, you can bring the cloud to your information.

Build a robust post-breach plan, then staff and train for it.

A detailed plan for post-breach action is essential.

Chapter 4

A compliant cloud


HITRUST
ITAR
ISO 9001
CJIS
EN 301 549
China DJCP
EU-US Privacy Shield
WCAG 2.0
BIR 2012
SOC 1
DoD
NIST CSF
CSA Star Certification
CDSA
ITAR
HIPAA/HITECH
UK G-Cloud
ENISA IAF
SOC 3
SOC 2
Section 508
MPAA
PCI DSS
FISC
GxP
Spain ENS
ISO 27018
ISO 22301
DFARS

Building a culture of compliance

What you should know

Privacy and security compliance is a foundational requirement for the cloud-first enterprise. It is also a vast and very technical subject, where the trees can easily block the view of the forest. Enterprise leaders should approach compliance firmly focused on essential general principles, while delegating critical execution tasks to their legal and compliance advisors.

When we say "compliance," the natural question to ask is: "Compliance with what?" There are two basic kinds of compliance:

- Mandatory—Usually this means compliance with data protection laws and privacy regulations enforced by governments

- Voluntary—For example, compliance with international, national, and industry standards for security, consumer protection, and data governance

Of course, data protection laws and government regulations may offer enterprises considerable choice on their path to compliance. This is the case, for example, with the many ways that enterprises can obtain the right under the GDPR (discussed in previous sections) to process the personal information of website users.

At the same time, not all "voluntary" standards are actually voluntary. Compliance with the International Organization for Standardization's 27000 family of information security management standards,[62] although not a legal mandate, is a default baseline for any enterprise that is serious about security. In particular, no cloud provider that hopes to earn the trust of its customers can forgo ISO 27000.

Compliance with data protection laws, privacy regulations, and security standards is not primarily about technology. Certainly, having the right technology can help. Enterprises will find it easier to comply with the GDPR if they use modern cloud services that automatically build a unified catalogue of sensitive data types, rather than on-premises legacy IT systems that bury information in multiple database silos.

The cloud-first enterprise must be built on an institutional culture of compliance. You must establish business processes that can reliably achieve and maintain compliance across your entire portfolio of IT applications. Such processes should be designed and operated by legal and compliance experts who know your business well and understand both the letter and the spirit of the law.

What you should do

Build a legal and compliance team with the right skills and empower it to do the right thing. Modern data protection legislation such as America's HIPAA (Health Insurance Portability and Accountability Act) or Europe's GDPR (General Data Protection Regulation) is dauntingly complex. Simply determining what the law requires is an arduous process that requires specialist knowledge, particularly when—as in the case of the GDPR—a sweeping new law has just been introduced that may engender years of litigation before its real contours are clear. Putting that determination into practice in your organization is even more challenging—it requires people with a rare combination of technical mastery and management ability.

Enterprise leaders should build a legal and compliance team that has the skills to cope with new data protection laws as well as the established industry regulations you operate under. This team will

naturally include your General Counsel and perhaps a Chief Privacy Officer, as well as your CIO and CISO. The GDPR also mandates a specialized Data Protection Officer with a specific skillset and scope of authority, who logically belongs to the legal and compliance team. However, the GDPR states that the DPO must have "significant independence" and a direct reporting line to "the highest level of management" of the company.[63] The exact interpretation of this requirement is one of many GDPR issues that will only be settled by practical experience after the GDPR takes effect.

Your legal and compliance team must be adequately resourced and empowered to do its job. That means that it must have the authority to bring reluctant business units into line when compliance obligations require possibly inconvenient changes to existing ways of doing business and managing IT assets.

A good example we have already mentioned (see "Identity is the New Firewall") is the use of multi-factor authentication. MFA is a powerful and ultimately very simple way to prevent your employees from having their all-important login credentials stolen in phishing attacks. But to be effective, MFA must be used by everyone. Your legal and compliance team should have the authority to say no when departments or individuals seek exemptions from the enterprise MFA policy.

Leverage the compliance investments and expertise of your technology providers. We know that compliance cannot be achieved by technology alone. But it is equally true that, as a practical matter, it is not feasible to comply with such complex regulatory regimes as HIPAA or GDPR without extensive help from technology.

Building the technology foundation for your enterprise compliance programs is not a matter of choosing just the "right" technology product or service that will function as a magic bullet. There is of course no such thing. For any given technical problem—for example, identifying and cataloguing all the forms of personal information retained by your organization that are subject to GDPR requirements—there will be more than one good solution from more than one good technology provider.

The key to using technology to solve compliance challenges is to leverage the intellectual capital that your providers have built into their products and services. Global cloud providers have little choice but to design their services from the ground up with compliance in mind.

At Microsoft, we currently have hundreds of software engineers working on a new unified end-to-end privacy architecture for all of our services. To meet the multitude of complex and constantly evolving compliance requirements our software and cloud services face, we have also built a large internal organization whose sole job is to ensure we meet these requirements and can prove it to customers and regulators.[64] As a result of the work of this group and others, we have built what we believe is the largest catalogue of standards certifications of any technology provider.[65]

We know our reputation and our very business depend on delivering solutions that ensure our customers will be able to comply with HIPAA, GDPR, and many other regulatory regimes around the world. Accordingly, we invest in the business processes, the software, the data centers and—above all—the people who will help us help you achieve compliance.

Don't let compliance stifle innovation. Enterprise leaders must insist on compliance from all parts of the organization, because the consequences of a major data breach or destructive hacker attack can be extreme. At the same time, leaders must not shut down the exploration of new ideas and new tools that naturally bubble up from employees seeking solutions to genuine business problems.

The reality is that the profusion of inexpensive, convenient, and immediately useful cloud services has placed a cornucopia of new software solutions within easy reach of your employees. This has led to a phenomenon known as Shadow IT, where individuals or business units subscribe to an unsanctioned cloud service without asking corporate IT or the compliance team. Few companies today know the true extent of cloud services deployed by their employees. Going rogue in this way creates obvious risks, because these services might become avenues for attackers to enter your network and seize control of its assets, which could lead to a damaging leak of sensitive or highly regulated data. Gartner estimates that within five years as much as a third of successful enterprise cyberattacks will involve this type of Shadow IT.[66]

Clearly you need to get control of your Shadow IT. But blocking it completely, although (perhaps) possible in principle, is not the right solution. In any large organization, real business problems will frequently arise that are locally obvious, but invisible to the center. Preventing employees from finding solutions to these problems will hurt your bottom line and damage morale. Moreover, there is no guarantee that the suppression of Shadow IT by the center will be effective. Innovative employees will find ways around restrictions.

The alternative to repression is monitoring behavior to identify risk and managing it before incidents happen. The cloud services that employees embrace in Shadow IT can be detected and brought under control with a special type of cloud service known as a cloud access control broker.[67] Such a service inspects the logs of your network, looks for the signatures of thousands of known and catalogued cloud services, and tells your security and compliance teams which ones are creating risk. You can then take action to limit their use or impose guard rails.

The reality is that Shadow IT is the new normal in dynamic modern enterprises. Allowing end users and teams to use the cloud applications that are best suited for their work solves business problems and boosts morale. Gaining control and managing the risk of these shadow cloud apps instead of applying a blanket interdiction will smooth your enterprise's path to digital transformation.

Banking in the cloud must satisfy exacting regulations

Bank of America—or BofA as it is familiarly known—is one of the world's leading financial institutions. It operates in all 50 U.S. states and 35 other countries, and counts 47 million consumers and small businesses as its customers, as well as many large corporations. Information is the lifeblood of any organization of this size, and all the more so when the organization is a bank.

BofA will soon begin rolling out the Microsoft Office 365 cloud productivity suite to some of its 200,000 employees, and will also begin to deploy applications on Azure cloud infrastructure. The bank's goal is to deliver 80% of its business applications in the cloud within the next several years.

In a highly regulated industry like banking, digital transformation is not possible without compliance because of the exacting requirements of banking regulators in many countries. A key factor in BofA's decision to embrace the cloud was the breadth and depth of Microsoft's investments in security, transparency, and regulatory compliance.

Microsoft's Financial Services Compliance program allows firms and regulators to deeply examine Microsoft cloud systems, services, and processes.

The Financial Services Compliance program lets banks verify that Microsoft has taken the proper steps to secure data and mitigate risk. In addition, Microsoft's industry-leading compliance portfolio helps financial institutions move to the cloud while meeting current compliance requirements and planning for the EU's GDPR.

Standards as a framework for trust

What you should know

When mandatory regulatory regimes defined by modern data protection laws such as the GDPR have become so all-encompassing, one might well wonder why voluntary privacy and security standards are still necessary. Two key reasons are flexibility and granularity.

Huge pieces of legislation are cumbersome affairs crafted by government officials over months or years of intricate negotiations. They reflect various political compromises and seek to cover as many cases as possible, even though their authors are rarely domain experts. Once passed, they are very difficult to change. They may remain in force for decades, becoming divorced from changing realities in the later phases of their life.

Modern data privacy and security standards—notably those developed by the International Organization for Standardization (ISO)—are written by experts. Their impetus comes from leading technology providers and large technology users, who work with national standards organizations such as the American National Standards Institute (ANSI) and similar organizations from dozens of countries around the world. These truly international standards are not set in stone. They can and do evolve, albeit slowly. Although often broad in coverage, they are always tailored to a specific set of concerns and do not aim for the universality of a law like the GDPR.

The most important global security standard is ISO's 27000 family of information security management standards (briefly mentioned in the security chapter). Its earliest versions were developed in the pre-cloud 1990s by the British Standards Institution (BSI). They were a response to the growing realization among large IT users and providers that a structured approach to enterprise information

security had become an urgent necessity.[68] Constantly evolving, the most recent version was released in 2013,[69] but it is still a general information security standard, not one designed specifically for cloud computing.

Enterprise leaders should understand the fundamental difference between a security management standard like ISO 27000 and low-level technical protocols that spell out how networks and IT systems handle security. The latter are important, but they are all about bits and frequencies and coding schemes. Security management standards, in contrast, are not about technology. Instead, they spell out ways of thinking about organizational problems. They are tools enterprise leaders and their legal and compliance teams use to build robust institutional cultures that are able to withstand numerous and inevitable security challenges.

There are of course many other standards that apply to cloud computing besides those established by ISO. Most of them are established by national legislation and typically apply to industries that handle particularly sensitive kinds of information, such as financial services and healthcare. These vertical standards are too numerous and too specific to discuss here, but we provide some pointers to further information later in this chapter.

What you should do

Use the emerging body of new ISO cloud standards to guide your cloud migration. When enterprises and governments entrust more and more of their strategic information assets to the safekeeping of cloud providers, trust is essential. Yet given the complexity of assets and the intricate technologies that weave the enterprise and its cloud providers together in a single digital fabric, such trust cannot be purely informal or ad hoc. It must be formalized and based on recognized standards.

We have already mentioned the ISO 27000 family, which is not a true cloud standard, but nevertheless remains foundational. Almost every executive concerned with enterprise security will be aware of ISO 27000's best known components, ISO 27001 (the base standard) and 27002 (associated best practices). But in the past few years ISO has begun to publish a whole new family of privacy and security standards specifically focused on cloud computing.

These new cloud standards are an important step forward, because the cloud raises security and privacy issues not anticipated by the original 27000 series. For examples of the new standards, see the table below.

Selected ISO standards for cloud computing	
ISO 27017 Code of Practice for Information Security Controls[70]	For cloud providers, who may be certified to this standard. Expands the security best practices defined in ISO 27002 to cover cloud computing services.
ISO 27018 Code of Practice for Protecting Personal Data in the Cloud[71]	For cloud providers, who may be certified to this standard. Extends ISO 27001 to address issues of data privacy and protection of personal information in the cloud.
ISO 19086 Cloud Service Level Agreement Framework[72]	For cloud providers and cloud customers both. Establishes a flexible framework for cloud service level agreements (SLAs).
ISO 38505 Governance of Data[73]	For cloud customers. New standard that specifies principles for managing data as a strategic enterprise asset, wherever it resides.

Enterprise leaders should ask their legal and compliance team, as well as their CIO and CISO, to study the new ISO cloud standards and incorporate them into their baseline work on cloud compliance. The ISO family of cloud standards is evolving rapidly and is likely to become as important for enterprise cloud computing in the next decade as ISO 27000 has been for enterprise information security in the past.

Make sure your legal and compliance team has a thorough mastery of the specific standards that apply to your industry. Legislators and regulators all over the world have long recognized that certain kinds of information are especially sensitive and require dedicated regulatory regimes. Prime examples include financial and patient health records as well as personal information about students and citizens.

As noted above, these industry standards are too numerous and too specific to their respective national markets to discuss here. However, at Microsoft we have made a sustained effort to meet the requirements of these important vertical and national standards, with a particular focus on highly regulated sectors such as financial services, healthcare, and government. We have a permanent staff of hundreds of lawyers, engineers, and policy experts working full-time on building compliance into all our services and software. We have built a specialized central organization to manage the numerous audits of our facilities and procedures that outside standards bodies conduct every year, and we provide detailed evidence of the outcomes of these audits to our customers.

All in all, we believe we have the largest portfolio of such standards of any cloud provider in the world. Extensive documentation of these standards compliance efforts is published on our website.[74] For illustrative purposes, we list a number of examples of national and vertical industry standards or regulations that our cloud services such as Office 365 and Azure comply with.

Selected Office 365 national and vertical standards	
Data processing terms	We provide customers with additional contractual assurances through our data processing terms regarding Microsoft handling and safeguarding of customer data. By agreeing to these terms, we commit to more than 40 specific security commitments collected from regulations worldwide. The robust commitments in our data processing terms are available to customers by default.
European Union model clauses[75]	The EU model clauses are recognized as a preferred method for legitimizing the transfer of personal data outside the EU for cloud computing environments. Offering the EU model clauses involves investing and building the operational controls and processes required to meet the exacting requirements of the EU clauses.
Family Educational Rights and Privacy Act (FERPA)	FERPA imposes requirements on U.S. educational organizations regarding the use or disclosure of student education records, including email and attachments. Microsoft agrees to use and disclosure restrictions imposed by FERPA that limit our use of student education records, including agreeing to not scan emails or documents for advertising purposes.
Federal Information Security Management Act (FISMA)[76]	FISMA requires U.S. federal agencies to develop, document, and implement controls to secure their information and information systems. Federal Risk and Authorization Program (FedRAMP) is a federal risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

Selected Office 365 national and vertical standards	
Gramm-Leach-Bliley Act (GLBA)	GLBA requires financial institutions to put processes in place to protect their clients' nonpublic personal information. GLBA enforces policies to protect information from foreseeable threats in security and data integrity. Customers subject to GLBA can use Office 365 and comply with GLBA requirements.
Health Information Trust Alliance (HITRUST)	Viewed as an important standard by U.S. healthcare organizations, HITRUST has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store, or exchange personal health and financial information.
Health Insurance Portability and Accountability Act (HIPAA)[77]	For certain customers, HIPAA imposes security, privacy, and reporting requirements regarding the processing of electronic protected health information. Microsoft developed Office 365 to provide physical, administrative, and technical safeguards to help our customers comply with HIPAA. We offer a HIPAA Business Associate Agreement (BAA) to any customer.
Statement on Standards for Attestation Engagements No. 16 (SSAE 16)	Office 365 has been audited by independent third parties and can provide SSAE16 SOC 1 Type I and Type II and SOC 2 Type II reports on how the service implements controls.

Standards are about trust

Today, new technologies like cloud computing, artificial intelligence, robotics, virtual reality, and a host of others are transforming our world. But if we're going to use these technologies to solve society's greatest challenges and share these solutions equitably around the world, then we must be sure we can trust them.

If we look carefully at the devices, materials, systems, and physical and business processes that make up the modern world, we see that they are embedded in a dense mesh of standards. The mesh is made up of national and international standards, government certifications, engineering best practices, industry codes, and innumerable rules mandated by legislation.

In our daily lives we interact with countless people and things that we trust to do us no harm. Household appliances, cars and their drivers, our food and the people who prepare it, useful chemicals such as drugs, public transportation systems, airplanes, buildings, electrical grids—all fall within an extended web of trust that surrounds us at all times. Standards help develop trust through clear definitions, clearly articulated best practices, transparency into mechanisms, and proof (such as certifications). The modern IT industry is no exception. From the very start it has been dependent to an extraordinary degree on standards.

Most early IT standards concerned rules specifying how hardware devices plug into each other or communicate over networks. But the most important IT standards today deal with more intangible things, such as risk management, the protection of personal information, business processes, and procedures that organizations should follow to ensure information security.

Today cloud computing is at the epicenter of the development of new IT standards. We won't attempt to review the technical content of the new cloud standards. But we do want to convey some of the benefits they offer. Here are the most important:

Definitions of key terms used in cloud computing. Standards offer precise definitions of the different kinds of data that customers entrust to the cloud and the actions that cloud services can take on these data. The same will be true for AI and machine learning. **Example:** ISO/IEC 17788 provides definitions of common cloud computing terms, including those for cloud service categories such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It also specifies the terminology for cloud deployment models such as "public" and "private" cloud.

Transparency into cloud processing based on common baselines and explicit best practices. Processing performed by cloud services may take place far from users, in inaccessible data centers located in other countries or even on other continents. Standards give users, providers, and regulators a shared understanding of the processing actions performed by a given cloud service and the protections the service offers. **Example:** ISO/IEC 27018 is a code of practice for the protection of personally identifiable information (PII) in public clouds acting as PII processors. It is particularly relevant to organizations concerned with GDPR compliance.

Guidance for organizations engaged in digital transformation. New cloud standards spell out recommended procedures for data governance and service level agreements with cloud service providers. **Example:** ISO/IEC 19086-1 provides a formal checklist for defining and evaluating cloud SLAs.

Assurance and certification that cloud providers are doing what they are supposed to be doing. Trust is reinforced through proof points—certifications, audits, attestations, and the like. These help customers and regulators gain assurance about the practices, procedures and technologies that process customer information in the cloud. Microsoft provides a large collection of certificates and attestations including ISO/IEC 27001/27018 certificates to demonstrate its management, implementation, and continuous improvement of its Information Security Management System.

What happens if you are sued over a patent used in your cloud application?

The technology industry is built on constant innovation. Unfortunately the race to bring innovations to market also sometimes leads to disputes about intellectual property. As a cloud provider, we want to make sure that our customers are protected from such disputes while using our cloud services. That's why we decided to use our vast patent portfolio to help protect our cloud customers.

The risk is real. According to a study by IPlytics, cloud-based IP lawsuits have risen 700% over the past four years in the U.S. And non-practicing entities (NPEs) have increased their acquisition of cloud-related patents by 130% over the same period.

To address this challenge, our Azure IP Advantage program offers the following benefits:

1. We provide intellectual property protection with uncapped indemnification coverage, including open source software powering Azure services.

2. We make 10,000 Microsoft patents available to Azure customers for the purpose of defending against patent lawsuits over applications that run on Azure. These patents are broadly representative of Microsoft's overall patent portfolio and are the result of years of cutting-edge innovation by our best engineers around the world.

3. We pledge to Azure customers that if Microsoft transfers patents in the future to non-practicing entities, they can never be asserted against them. We do not have a practice of making such transfers, but we have learned that this is an extra protection that many customers value.

In short: What to do about compliance

Building a culture of compliance

Build a legal and compliance team with the right skills and empower it to do the right thing.

Your legal and compliance team must be adequately resourced and have the authority to bring reluctant business units into line.

Leverage the compliance investments and expertise of your technology providers.

Your providers have built a great deal of compliance intellectual capital into their products and services.

Don't let compliance stifle innovation.

Don't shut down the exploration of new ideas and new tools that naturally bubble up from employees seeking solutions to genuine business problems.

Standards & regulations as a framework for trust

Use the emerging body of new ISO cloud standards to guide your cloud migration.

These new cloud standards are an important step forward.

Make sure your legal and compliance team has a thorough mastery of the specific standards and regulations that apply to your industry.

Prime examples include financial and patient health records as well as personal information about students and citizens.

Chapter 5

A cloud for global good

Advocacy and corporate responsibility

What you should know

We live in an interdependent world. No organization is an island. Every business firm, government agency, and nonprofit entity depends on continual and fruitful interactions with others. From this founding principle, a strong consequence follows: as organizations, we must accept collective responsibility for our security and that of the billions of citizens of planet Earth who depend on us for life and sustenance.

We must embrace and implement the laws and regulations that protect the cybersecurity of organizations and the privacy of individuals. When we disagree with those laws, or find that they have become outdated in the face of rapid technological change, we must seek to change them through the democratic political process.

But those of us who lead organizations must do more than respect the law. We must promote in our organizations a culture of responsibility, a culture that acts not merely out of self-interest, but also always seeks to "do the right thing" for society as a whole.

As a global cloud provider with millions of organizational customers and over a billion individual users, Microsoft works very hard to do the right thing. Here are some of the human values we seek to advance in our work:

- Using technology in ways that protect and sustain the environment

- Enabling access to information technology for all, regardless of ability, disability, gender, religion, age, race, social status, or wealth

- Ensuring that technology provides new and rewarding opportunities for work to those whose traditional tasks are displaced

- Advocating for national and international laws that protect individual privacy and establish reasonable limits to government surveillance

- Supporting a "Digital Geneva Convention" that will prohibit nation-states from conducting cyberattacks on civilian systems

We want our customers to know that they too will benefit from our efforts to further these goals. We invite you to join us in advocating for them.

What you should do

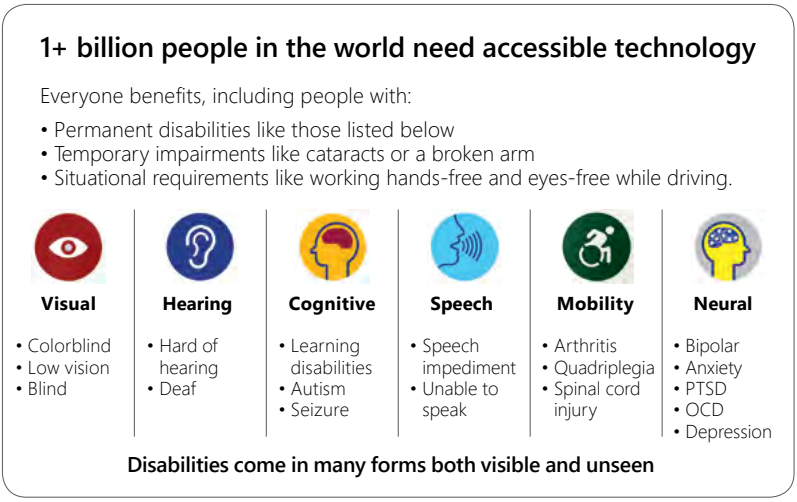
Require that your cloud providers pursue energy efficiency and obtain a greater share of their energy from renewable sources. Because data centers will rank among the world's major consumers of electric power by the middle of the next decade, the development of a global cloud infrastructure provides an important opportunity to accelerate the development of renewable energy, to develop new clean energy technologies, and to drive further improvements in energy efficiency.

At Microsoft our data centers are already 100% carbon neutral. We are approaching 50% of energy obtained from wind, solar, and hydroelectric power. We expect to pass 50% by the end of 2018 and exceed 60% by the early 2020s.[78]

We are also pursuing LEED Gold certification for all the data centers we own. Leadership in Energy and Environmental Design (LEED) is a rating system devised by the United States Green Building Council to evaluate the environmental performance of a building and encourage market transformation toward sustainable design. LEED is the most widely used green building rating system in the world and is used as a framework for all kinds of buildings, not just data centers.[79]

Small changes in data center design can make a big difference in energy consumption. For example, at one of our data centers we recently swapped out an entire area of fixtures to LED lighting. This had big energy impact, resulting in a 28,382 kilowatt-hour annual reduction in energy consumption for the space. But it also created other business benefits, because LEDs are less prone to outages.

Establish procurement policies that mandate accessible technologies based on globally recognized standards for accessibility. Modern computing—both on-premises and in the cloud—offers profound benefits for people of all ages and abilities. Cloud-connected devices in particular offer assistive technologies such as audio captioning, speech recognition, real-time translation of text to Braille, and a constantly improving ability to respond intelligently to spoken or gestural commands. While some of these functions can also be performed locally by desktop or mobile devices, the cloud's instantaneous access to nearly unlimited computing power and memory means that its behavior can be more intelligent, and therefore more accessible to those with disabilities.



The cloud can empower employees with visual, learning, age-related, mobility, hearing, and speech disabilities to be productive and valuable members of your workforce. And because the cloud is a repository for custom settings, people can access information and services formatted to meet their preferences wherever they go, on almost any device.

Global standards for accessibility such as ETSI EN 301 549[80] and ISO/IEC 40500 (W3C Web Content Accessibility Guidelines 2.0)[81] are becoming widely adopted. They encourage the development of a broad range of products and content that can be used by everyone. Your procurement policies should rely on these standards and mandate accessible technology from your suppliers, whether of on-premises IT or cloud services.

You should also ensure that the online services your organization provides to customers or other stakeholders use these same accessible technologies and accessibility standards.

Invest in the future of work by investing in new forms of employee training. We all know that rapid technological change also means rapid change—not all of it welcome—in the kinds and numbers of jobs available in our economy. However, this problem is not new. Past technology revolutions that made traditional occupations obsolete have also created new and ultimately much better jobs for millions. Despite widespread angst over job losses caused by automation and computers, the economy in the early 21st century offers far more rewarding work opportunities to our vast population than the economy of 100 years ago.

Consider the pair of photographs displayed below. Both show New York City's famous Flatiron Building on Broadway. One photo was taken in 1905 and shows streets filled with pedestrians and horse-drawn vehicles. The other, taken at the same spot 20 years later, shows the Manhattan of the Roaring Twenties, where cars fill the streets and not a horse is to be seen.

New York by horse and by car, 1905 and 1925

The automobile revolution of the early 20th century—inspired by innovators such as Henry Ford, whose great River Rouge factory we discussed in Chapter One—destroyed millions of jobs and a centuries-old way of life based on horse transportation. Yet few would deny that it created a better world for all.

Similarly today, technology offers vast new opportunities. One particularly striking change is the revolution in education now being driven by cloud-based learning. Hundreds of millions of people throughout the world are attending university, high school and even grade school level classes via their web browsers. Never before in history has such a universal storehouse of knowledge been made available so cheaply to so many. Dozens of for-profit and nonprofit startups now compete with the world's most famous universities to offer courses on every conceivable subject, including computer programming, science and engineering, mathematics, languages, history, music, art, politics, and economics. And the subjects are not limited to academics—hundreds of online classes offer instruction in more practical subjects such as cooking, accounting, agriculture, and nutrition.

Today the online learning revolution is just beginning. But already it has spread far beyond the U.S. and is sweeping through Africa and Asia. We are confident in predicting that online education will play a central role in helping workers on every continent acquire the skills needed to thrive in the new world of technology-enhanced forms of work.[82]

Enterprises must seize the unprecedented opportunity offered by online education to encourage employees to upgrade their technical, job, and life skills. A more productive workforce will make for a better society.

Help us advocate for new laws that enhance cybersecurity and protect personal privacy in the face of today's technologically advanced threats. At Microsoft we have taken the lead in defending our customers' rights and data. Our pioneering Digital Crimes Unit collaborates with dozens of law enforcement agencies around the world in the fight against cybercrime.[83] At the same time, we have not hesitated to challenge government surveillance activities when we believe they are excessive or unjustified.[84]

To fight crime and protect public safety, governments have a clear and compelling need to access digital data. But balancing that interest against citizens' expectation of due process and the rule of law is essential to maintaining trust in technology. It is therefore critical to craft modern laws that provide law enforcement and intelligence agencies with appropriate mechanisms to access digital information pursuant to lawful process. These laws must protect citizens' fundamental privacy rights, and respect the sovereignty of other nations.

The rapid adoption of cloud services, coupled with the simultaneous rise in transnational criminal activity, raises new challenges for law enforcement. But because many national laws have not kept pace with technology, there is uncertainty about the legal frameworks that govern access to private information stored in the cloud.

Because of the lack of adequate international frameworks for accessing digital evidence, governments may be tempted to take unilateral steps to seize information stored outside their borders. This can create unresolvable jurisdictional conflicts that undermine laws or force companies to violate the laws of one country to comply with the laws of another. Rather than resort to ad hoc measures that create conflict between national laws, governments

should modernize outdated legal rules for accessing digital information. Where necessary, they should create new mechanisms that meet the challenges of policing cybercrime and terrorism while safeguarding time-honored values such as privacy and human rights.

At Microsoft, we have been in the forefront on these issues. In 2014, we sued the U.S. government to prevent a U.S. warrant from compelling us to produce email stored in a Microsoft data center in Dublin. We filed this case because it involves an extraterritorial application of a decades-old U.S. law that does not provide such authority and also because it ignores Irish laws and the rights of those who own the emails. Today this case is before the United States Supreme Court,[85] where we will argue that our obligations to our European customers under European law do not permit us to disclose our customer's personal data to foreign authorities except under conditions defined by European law. Looking beyond this case to the future, when critical principles with important consequences for our customers are at issue, we will not hesitate to return to the courts to uphold basic rights.

At the same time, we are heartened that the U.S. Congress is considering legislation to modernize the aging data protection framework in the U.S. and to provide a clear and fair legal process when governments seek to access emails and other digital information. We strongly support passage of the proposed International Communications Privacy Act.

We invite our customers to join us in advocating for the modernization of laws that authorize government access to private data within justified limits, both inside and across national borders. For more information on this important topic, please consult our publication "A Cloud for Global Good."[86]

Join us in urging the world's governments to endorse a Digital Geneva Convention for cyber arms control. In addition to modernized surveillance and data access legislation, we also believe that new international agreements are essential to limit the dangers posed by cyberattacks conducted by nation-states, especially when they harm civilians.

As technology continues to reshape the world, conflicts between nations are no longer confined to the land, sea, and air, and no longer limited to physical weapons such as guns or missiles. Today a cyber arms race is underway with nations developing and unleashing new kinds of virtual weapons that endanger the critical data and digital-powered infrastructure that we all depend on for our daily lives. The world needs new rules that will prohibit nation-states from hacking into vital civilian systems—whether it be our hospitals or the electrical grid or the voting systems on which our democratic societies rely.

While technology companies like Microsoft and our peers in the industry serve as a first line of defense against such threats, it is a mistake to think the private sector by itself can put an end to cyberattacks by nation-states, any more than it can prevent any other types of military attacks. Nation-state investments in cyberweapons have advanced beyond the point where this is possible.

These are the reasons that led us to propose the concept of a Digital Geneva Convention in February 2017.[87] We acknowledge that such an initiative will require years of effort to reach fruition. We also recognize that this type of agreement could take a variety of different forms and requires more than a single step. We therefore believe it is essential to combine a focus on long-term measures like a Digital Geneva Convention with more immediate steps to build

on existing international law to protect civilians from cyberattacks in the present. We must recognize the current norms that already apply to cyberspace and identify the gaps in them that need to be filled. Governments, civil society, businesses and academia should work together on this effort to prevent the continued harm of civilians by cybercriminals.

Technology has come a long way since the days of rifles and cannons, yet one need is constant: as technology advances, the law must move forward with it.

The cloud makes buildings greener

In 1883, the little-known son of a poor Wisconsin farmer filed a patent for the world's first electrical thermostat. The company that Warren Johnson founded to commercialize his invention, Johnson Controls, is now a global conglomerate.

Johnson's business today is much broader than simple devices like its founder's thermostat. Consider, for example, the large chiller units that control heat and air conditioning in tens of thousands of buildings around the world.

Chillers are complex devices with an unexpected but outsized impact on the global environment. Buildings use 40% of the world's electricity, and chillers account for 50% of the energy used by buildings. Managing that efficiently is very important, and data is the key.

Chillers generate a flood of data that is difficult for building managers to use effectively. Johnson Controls wanted an easier, more automated way to collect data and provide intelligence on systems in any location worldwide. It decided to create a cloud application that could integrate with any building component—from building sensors and thermostats to rooftop air handling and chiller systems. The application was built in the cloud with the Azure Internet of Things Suite, and now collects 14 million records each day.

Managing buildings more efficiently is key to controlling costs for facility operators and improving environmental sustainability for our planet. But more is at stake than energy efficiency—reliable performance is also critical, because lives depend on it. If even one chiller in a hospital or other care facility shuts down, the results can be tragic.

In short: Help build a cloud for global good

Advocacy and corporate responsibility

Require that your cloud providers pursue energy efficiency and a continually increasing share of energy from renewable sources.

Data centers will rank among the world's major consumers of electric power by the middle of the next decade.

Establish procurement standards that mandate accessible technologies based on globally recognized standards for accessibility.

Modern computing—both on-premises and in the cloud—offers profound benefits for people of all levels of ability.

Invest in the future of work by investing in new forms of employee training.

Despite angst over job losses caused by automation, the economy in the early 21st century offers many new rewarding work opportunities to our vast population.

Help us advocate for new laws that enhance cybersecurity and protect personal privacy.

We must balance the legitimate needs of governments to access data with citizens' expectation of due process and the rule of law.

Join us in urging the world's governments to endorse a Digital Geneva Convention for cyber arms control.

New international agreements are essential to limit the dangers posed by cyberattacks conducted by nation-states, especially when they harm civilians.

Conclusion

Digital transformation in the cloud

Digital transformation in the cloud

The payoff of successful digital transformation can be life-changing for enterprises engaged in hyper-competitive global markets. No enterprise can afford to ignore the opportunities that new technology provides for improving their core value-creation activities. Defending and growing your ability to create value in today's environment requires relentless focus on the missions where your performance can be best-in-class. That means handing off other missions to partners who are themselves leaders in those areas. The future of the enterprise in a cloud-based economy is a partnership of equals where each participant is a champion of its own domain.

The promise of digital transformation based on the delegation of your non-core missions to specialized partners is clear. But can you make your data secure and ensure its privacy and your own compliance with the law by handing off these concerns entirely to Microsoft, without a further thought? In an ideal world, the answer would perhaps be yes. But in the real world, the answer is "Definitely not." The question is like asking your friend at the gym: "Can I get fit by watching you work out?" No, regrettably not, at least not yet.

As a cloud provider, we do everything in our power to ensure the security, privacy, and compliance of the data and applications you entrust to us. We can take a lot of the risk and complexity and cost of security off your hands. But certain fundamental tasks you must do yourself. Perhaps the most important of these tasks is to persuade your users—be they employees, partners or customers—to avoid the simple mistakes that are so often at the root of successful cyberattacks.

The more you can automate this process and leverage smart software to protect users from their own mistakes, the better. But automation will not suffice if it does not stand on the solid foundation of a genuine culture of security. Nothing can replace the effort of coaching and educating your users to apply good security practices in everything they do.

Regardless of how much IT infrastructure you keep in-house or move to cloud partners, the final responsibility for keeping your data secure and private rests with you. The more you shift to cloud services at companies like ours, the more we can do the heavy lifting on security, privacy, and legal compliance for you. But when all is said and done, you will still need to go to the gym every day to exercise your security muscles and your privacy reflexes. You are always going to need this workout.

The challenges of cybersecurity and the new data protection regulations are daunting for enterprise leaders and the legal and compliance experts who advise them. But with the right framework of trust between cloud customers and cloud providers, we believe these challenges can and will be met.

Endnotes

1 See Ryan Avent, *The Wealth of Humans: Work, Power, and Status in the Twenty-first Century*, St. Martin's Press, 2016

2 Detroit Institute of Art, https://www.dia.org/

3 For the history and operations of Ford's River Rouge plant, see James M. Rubenstein, *Making and Selling Cars: Innovation and Change in the U.S. Automotive Industry*, Johns Hopkins University Press, 2001

4 For the remarkable story of Ford's Brazil rubber plantations and the industrial town he built in the Amazon jungle, see "Deep in Brazil's Amazon, Exploring the Ruins of Ford's Fantasyland," NY Times, Feb. 20, 2017, here: https://www.nytimes.com/2017/02/20/world/americas/deep-in-brazils-amazon-exploring-the-ruins-of-fords-fantasyland.html

5 See Rubenstein above.

6 Avent, *The Wealth of Humans*

7 See "A Brief Look at the History of Hotel Technology," Intelity, here: http://intelitycorp.com/main/brief-look-history-hotel-technology/

8 See D. Wardell, "Hotel technology and reservation systems," Travel & Tourism Analyst, 1987, here (login required): https://www.cabdirect.org/cabdirect/abstract/19871847447

9 See "Marriott CEO: Technology Is the Biggest Risk in the Starwood Merger," Skift, May 9, 2017, here: https://skift.com/2017/05/09/marriott-ceo-technology-is-the-biggest-risk-in-the-starwood-merger/

10 See "Why Marriott is transforming their legacy systems with NoSQL," Diginomica, Oct. 7, 2015, here: https://diginomica.com/2015/10/07/why-marriott-is-transforming-their-legacy-systems-with-nosql/

11 See "Marriott CEO on Politics, Technology and Loyalty," Skift, June 7, 2017, here: https://skift.com/2017/06/07/interview-marriott-ceo-on-politics-technology-and-loyalty/

12 See "Hyatt's CIO on Cloud Computing," Dec 20, 2010, here: https://hospitalitytech.com/hyatts-cio-cloud-computing

13 See "Equinix Exec: We Spent $17B on Data Centers, but Cloud Giants Spend Much More," Data Center Knowledge, April 6, 2017, here: http://www.datacenterknowledge.com/archives/2017/04/06/equinix-exec-spent-17b-data-centers-cloud-giants-spend-much

14 For full results and methodology, see the research study conducted by Accenture on the energy efficiency of Microsoft data centers, "Cloud Computing and Sustainability," here: https://aka.ms/cloud-computing-and-sustainability

15 For an example of a modern cloud service catalog, see the Microsoft document "What is Azure?" here: https://azure.microsoft.com/en-us/overview/what-is-azure/

16 See the Microsoft document "Security Development Lifecycle?" here: https://aka.ms/security-development-lifecycle

17 See "Keeping trust at the heart of technology
An open letter from Brad Smith, Microsoft President and Chief Legal Officer," here: https://www.microsoft.com/en-us/trustcenter/about/open-letter

18 See "The Epic Story of Dropbox's Exodus from the Amazon Cloud Empire," Wired Magazine, March 14, 2016, here: https://www.wired.com/2016/03/epic-story-dropboxs-exodus-amazon-cloud-empire/

19 See Richard Goldthwaite, *The Economy of Renaissance Florence*, Johns Hopkins University Press, 2011.

20 See Robert D. Putnam et al., Making Democracy Work: *Civic Traditions in Modern Italy*, new edition, Princeton University Press, 1994.

21 See the Microsoft white paper, "Beginning your General Data Protection Regulation (GDPR) Journey: Accelerate GDPR Compliance with the Microsoft Cloud," here: https://aka.ms/Accelerate-GDPR-Compliance

22 See "The 5 Greatest Teen Hackers of All Time," here: https://www.techworm.net/2016/05/5-ultimate-juvenile-hackers-time.html

23 Fortune Magazine, "Sony Pictures: Inside the Hack of the Century," http://fortune.com/sony-hack-part-1/. Note: the web version of this article asks you to download or update Adobe Flash, however this is not necessary to read the article. Ironically, Flash is now regarded as a security risk and is being phased out on most websites.

24 See "He solved the DNC Hack," BuzzFeed, Nov. 8, 2017, here: https://www.buzzfeed.com/jasonleopold/he-solved-the-dnc-hack-now-hes-telling-his-story-for-the

25 Part of the text of this section has been adapted from the Microsoft publication "7 steps to a holistic security strategy." Readers can consult the full document here: https://aka.ms/holistic-security-strategy

26 Paris siege photo source: http://www.alamy.com/stock-photo-french-cannon-and-fortifications-at-montmartre-siege-of-paris-the-53204784.html

27 See Microsoft Secure Blog, "Top Five Security Threats Facing Your Business and How to Respond," here: https://aka.ms/top-5-security-threats

28 For a brief history of the IBM 360, see Wikipedia: https://en.wikipedia.org/wiki/IBM_System/360

29 1964 and 2017 U.S. GDP per capita figures stated in 2009 constant dollars. See: http://www.multpl.com/us-real-gdp-per-capita/table/by-year

30 For the history of Windows XP, see Wikipedia: https://en.wikipedia.org/wiki/Windows_XP

31 See Troy Hunt, "Everything You Need to Know about WannaCry," here: https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/

32 See Microsoft Secure Blog, "Strategies to build your cybersecurity posture," here: https://aka.ms/strategies-security-posture

33 For a longer discussion of the stages of a breach, see the Microsoft document "Anatomy of a Breach," here: https://aka.ms/anatomy-breach

34 The new NIST password guidance is quite technical in nature. For an overview, see Jim Fenton slide presentation, "Toward Better Password Requirements," here: https://www.slideshare.net/jim_fenton/toward-better-password-requirements

35 See the FIDO Alliance website for technical and policy details: https://fidoalliance.org/

36 For a good, short non-technical introduction to these topics, see Michael Copeland, "What's the Difference between Artificial Intelligence, Machine Learning and Deep Learning?" here: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

37 See "What is machine translation?" here: https://www.microsoft.com/en-us/translator/mt.aspx#whatmachine

38 For a case study of how Microsoft's own IT department uses this solution to track and suppress malware on 500,000 PCs at Microsoft, see "Windows Defender ATP helps detect sophisticated threats," here: https://www.microsoft.com/itshowcase/Article/Content/854/Windows-Defender-ATP-helps-detect-sophisticated-threats

39 For a short introduction to Secure Score, see Microsoft document and video "What is Office 365 Secure Score?" here: https://techcommunity.microsoft.com/t5/Office-365/What-is-Office-365-Secure-Score/td-p/61772. For Hartford Financial's use of Secure Score in setting cyberinsurance rates, see Wall Street

Journal, Feb. 10, 2017, "Microsoft to Rate Corporate Cybersecurity: Hartford Financial says it will use the Office 365 Secure Score when setting cyberinsurance rates," here: https://www.wsj.com/articles/microsoft-to-rate-corporate-cybersecurity-1486749600

40 For several recent examples of IoT cyberattacks, see Jack Wallen, "Five nightmarish attacks that show the risks of IoT security," here: http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

41 For a review of IoT security best practices, see the Microsoft document "Internet of Things Security Best Practices," here: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices

42 See Wikipedia, "Caesar cipher," here: https://en.wikipedia.org/wiki/Caesar_cipher

43 See Peter Hustinx, "Ethical Dimensions of Data Protection and Privacy," here: https://edps.europa.eu/sites/edp/files/publication/13-01-09_speech_tallinn_en.pdf

44 Hustinx.

45 Hustinx.

46 See Wikipedia, "International Safe Harbor Privacy Principles," here: https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

47 See "EU Charter of Fundamental Rights," here: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

48 Part of the text of this section has been adapted from the Microsoft publication "An Overview of the General Data Protection Regulation (GDPR)." Readers interested in learning more about GDPR requirements should consult the full document, available here: https://aka.ms/GDPR-overview

49 Final version of the Regulation, released April 6, 2016, here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

50 "Top 10 operational impacts of the GDPR: Part 4 - Cross-border data transfers," available here: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

51 See "Commission decisions on the adequacy of the protection of personal data in third countries," here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

52 Part of the text of this section has been adapted from the Microsoft publication "Beginning Your General Data Protection (GDPR) Journey." Readers interested in learning more about how to implement GDPR compliance should consult the full document, available here: https://aka.ms/Accelerate-GDPR-Compliance

53 "Top 10 operational impacts of the GDPR: Part 2 - The mandatory DPO," available here: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/

54 For a brief introduction, see "Privacy by Design at Microsoft," https://aka.ms/privacy-by-design

55 See Article 4 EU GDPR "Definitions," here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

56 Microsoft offers an extensive collection of resources to help your GDPR compliance efforts, including white papers and self-assessment tools, here: https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/resources

57 See "Are you ready for the EU's General Data Protection Regulation (GDPR)? Our two new tools can help you find out," here: https://aka.ms/GDPR-readiness-tools

58 See Rich Sauer, "Earning your trust with contractual commitments to the General Data Protection Regulation," here: https://aka.ms/GDPR-contractual-commitments

59 For a presentation of our thinking on the issues of government surveillance and lawful access to data, see the testimony of our Chief Legal Officer Brad Smith before the Senate Judiciary Committee, May 10, 2017, transcript here: https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Smith%20Testimony.PDF. For details about the Department of Justice revision to its secrecy order policy in response to the Microsoft lawsuit, see: https://www.nytimes.com/2017/10/24/business/microsoft-justice-department-secrecy.html

60 For hybrid cloud examples, see the Microsoft document "Azure Stack use cases," here: https://azure.microsoft.com/en-us/overview/azure-stack/use-cases/

61 For a careful discussion of differences in bank performance during the 2008 financial crisis, see Beltratti and Stulz 2009, "Why Did Some Banks Perform Better During the Credit Crisis? A Cross-Country Study of the Impact of Governance and Regulation," here: http://www.nber.org/papers/w15180

62 For a brief overview of ISO/IEC 2701, see "ISO/IEC 27001:2013 Information Security Management Standards," here: https://www.microsoft.com/en-us/trustcenter/Compliance/ISO-IEC-27001

63 For an overview of the Data Protection Officer role mandated by the GDPR, see Rita Heimes, "Top 10 operational impacts of the GDPR: Part 2 - The mandatory DPO," here: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/

64 For details on how we build compliance into our products and services, see the detailed white paper "Microsoft's Compliance Framework for Online Services," here: https://aka.ms/online-services-compliance-framework

65 For an up-to-date list of standards that we comply with, see the Compliance section of the online Microsoft Trust Center, here: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

66 See Gartner, "Gartner's Top 10 Security Predictions 2016," June 15, 2016, here: https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

67 For a brief overview of cloud access security brokers, see Hayden Hainsworth, "Why you need a cloud access security broker in addition to your firewall," here: https://aka.ms/cloud-access-security-broker

68 For a short review of ISO 27000 and its history, see Wikipedia, "ISO/IEC 27000-series," here: https://en.wikipedia.org/wiki/ISO/IEC_27000-series

69 See Wikipedia, "ISO/IEC 27001:2013," here: https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

70 For a short overview, see the Microsoft document "ISO/IEC 27017:2015 Code of Practice for Information Security Controls," here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27017

71 For a short overview, see the Microsoft document "ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud," here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018

72 For a short overview, see the Microsoft document "ISO/IEC 19086-1:2016 Cloud Service Level Agreement Framework," here: https://www.microsoft.com/en-us/trustcenter/Compliance/ISO-IEC-19086-1

73 For a short overview, see Geoff Clarke, "How data governance is now a strategic boardroom consideration in a data-driven world," here: https://aka.ms/data-governance-boardroom

74 For an online directory of both ISO and national or industry standards that our cloud services comply with, see "Compliance offerings," here: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

75 See "EU Model Clauses: Frequently Asked Questions," here: https://products.office.com/en-us/business/office-365-trust-center-eu-model-clauses-faq

76 See "FISMA/FedRAMP Frequently Asked Questions," here: https://www.microsoft.com/online/legal/v2/default.aspx?docid=42

77 See "Office 365 & Microsoft Dynamics CRM Online HIPAA/HITECH frequently asked questions," here: https://www.microsoft.com/online/legal/v2/?docid=41

78 See Brad Smith, "Greener data centers for a brighter future: Microsoft's commitment to renewable energy," here: https://aka.ms/greener-data-centers

79 See "Building and Operating Greener Datacenters: Our Commitment to LEED Gold," here: https://blogs.microsoft.com/green/2017/11/08/building-operating-greener-datacenters-commitment-leed-gold/

80 See Standard - EN 301 549 "Accessibility requirements suitable for public procurement of ICT products and services in Europe," here: http://mandate376.standards.eu/standard

81 See "Web Content Accessibility Guidelines (WCAG) Overview," here: https://www.w3.org/WAI/intro/wcag#iso

82 See Carl Benedikt Frey, "The Future of Jobs and Growth: Making the Digital Revolution Work for the Many," here: http://www.g20-insights.org/wp-content/uploads/2017/03/The-Future-of-Jobs-and-Growth.pdf

83 See the short video "Cybercrime: A story of vulnerability, deception, and security," here: https://www.microsoft.com/en-us/trustcenter/security/cybercrime

84 See Brad Smith, "In the Cloud We Trust," here: https://news.microsoft.com/stories/inthecloudwetrust/

85 See John Frank, "Finding Solutions for Law Enforcement Access to Digital Evidence," here: https://blogs.microsoft.com/eupolicy/2017/11/16/finding-solutions-law-enforcement-access-digital-evidence/

86 See Microsoft publication, "A Cloud for Global Good," here: https://news.microsoft.com/cloudforgood/

87 See Brad Smith, "The Need for a Digital Geneva Convention," here: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

DISCLAIMER

This book is a commentary on issues of cybersecurity and measures to protect against cyberattacks, issues of data privacy and measures to protect it, legislation such as the European Union's General Data Protection Regulation (GDPR) and measures that may help organizations comply with it, and other issues regarding compliance with laws, regulations, and standards governing these areas. The comments on these laws and regulations reflect Microsoft's interpretation of them, as of the date of publication. We've spent a lot of time with all of these issues and like to think we've been thoughtful about how to grapple with them. But the application of all such legislation, regulations, and standards is highly dependent on the specific facts of each organization and situation, and not all aspects and interpretations of these laws, regulations, and standards are well-settled.

As a result, this book is provided for informational purposes only and you should not rely on it as providing you specific legal advice or to determine how any law, regulation or standard applies to you and your organization. We encourage you to work with a legally qualified professional to discuss these laws, regulations, and standards, how they apply specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS BOOK. This book is provided "as-is." Information and views expressed in this book, including URL and other Internet website references, may change without notice.

Version 1.0 Published January 2018

microsoft.com/trustcenter