2017 Cybersecurity Roadmap

May you live in interesting times.

This expression can be seen as a blessing or a curse. Either way, it certainly seems to apply to the world in which we live today.

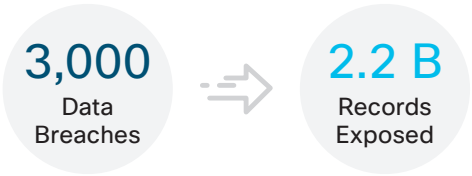
The hardware and software powering communications networks, connected devices and modern applications are incredibly powerful and productive. Yet they put organizations at risk in entirely new ways. That risk continues to mount as systems and devices become more connected, and bad actors become more sophisticated in using new technologies and techniques to penetrate networks and systems, steal our data, impinge on our privacy, and remotely take control of our assets.

This heightened risk environment means organizations and governments need to become more sophisticated in their approach to protect these valuable resources. They must also be ready to respond when attacks and breaches do occur.

These new needs create challenges for organizations. They also provide new opportunities for individuals who have the right skill sets to help those organizations address their cybersecurity challenges.

The Big Picture

Last year, approximately 2.2 billion records were exposed by about 3,000 publicly disclosed data breaches. Such incidents have proven to be costly for U.S. businesses, even those in tech-savvy industries that would seem to have an edge in this kind of thing.



A popular online search and media company last year disclosed two major data breaches that resulted in the exposure of personal information of some 1.5 billion user accounts. That not only hurt the company's reputation and required it to spend time and resources addressing the hack rather than its core business interests, but it also caused the organization that was planning to buy the company to lower its acquisition price by $350 million.

That is just one of many tech and media businesses that have experienced high-profile hacks in the last couple of years. One 2014 breach of an online auction site involved the theft of customers' names, addresses, and dates of birth, leading the company to ask 145 million of its users to change their passwords.

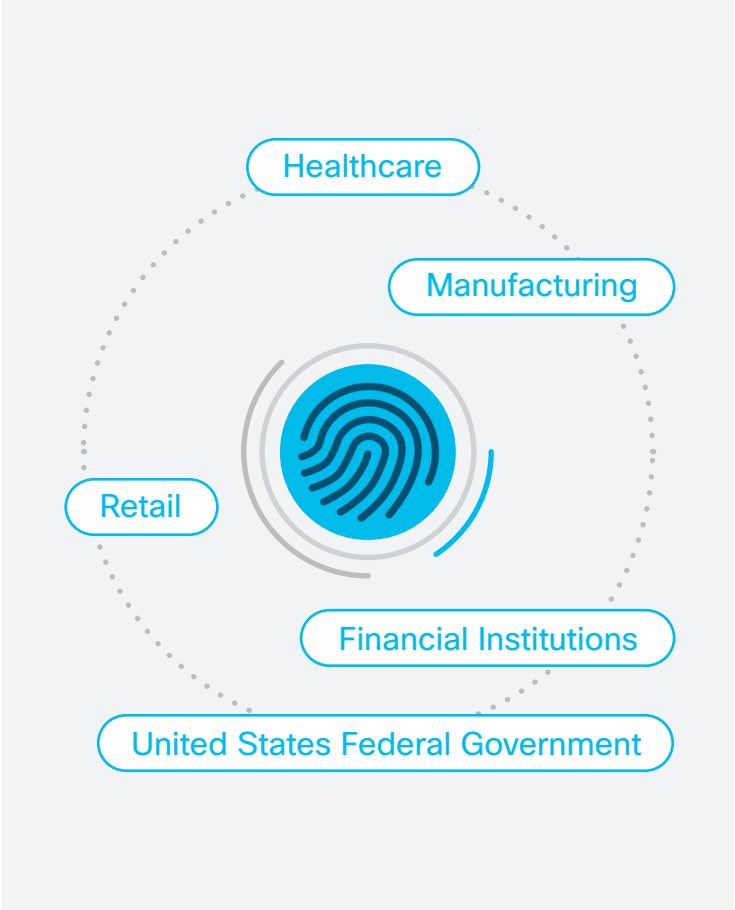
Another thing to consider: your organization's business transactions rely on reputation, and your brand. If you think that value can't be quantified, check out how much the top 100 brands are worth. Just the top 10 brands combined are worth over $700 Billion Dollars. That's more than the GDP of all but 18 countries.

If you had an easily damaged asset that was worth that much, and was helping you generate that much income, you would spend significant time strategizing how to protect it.

It's easy to succumb to breach fatigue. Yet all businesses are at risk from similar threats. As an industry, we need to figure out what to do about that.

Let's take a look at the cybersecurity challenges facing some major industries in the coming year, including regulatory shifts that organizations need to be aware of.

An Industry-Specific Assessment



Healthcare

Healthcare organizations need to be extra vigilant. According to Experian, their business vertical will be the No. 1 target of hackers in 2017.

Data breaches in this industry have tallied up around $6.2 billion in losses. The average cost of a cyberattack in the healthcare space is a whopping $2.2 million.

The healthcare space is a favorite target given the valuable nature of patient records. These files include names, addresses, phone numbers, and other contact information. They contain details about the most personal and private aspects of our bodies and minds. They also include such financial information as credit

card numbers, government ID numbers, insurance account numbers, and payment histories.

Unsecured patient records are a big part of the problem. The 2009 Health Information Technology for Economic and Clinical Health Act required healthcare organizations to adopt electronic health records. But it didn't require them to secure these records.

Keeping patient records in electronic form is good because it can lower the potential for confusion due to duplicate records. It also eliminates mistakes caused by poor handwriting. But digitizing this information and putting it on connected computers makes it ripe for the picking—especially when few have made a sufficient effort to secure it.

Hackers have now gone to work harvesting that information. They are enjoying a rich payday. These records fetch around $15 each on the black market. Hacks of hundreds of thousands or millions of patient records yield big returns for thieves.

Regulatory changes are coming to help raise the bar in the defense against these evolving threats.

The Health Insurance Portability and Accountability Act (HIPAA) rules that are already in place aim to protect the privacy of patients. The Office of Civil Rights (OCR), the body that enforces HIPAA, this year is expected to identify additional entities for audit, and address privacy related to big data, cybersecurity risks, and the Internet of Things (IoT). That is according to a paper published late last year (just as the new president was coming into office) by the Department of Health and Human Services, and related media reports.

In its paper, the OCR indicates that upcoming efforts are likely to include providing cybersecurity guidance to healthcare institutions via the incorporation of the National Institute of Standards and Technology Framework. OCR says it also aims to create "a more robust system for the collection, use and sharing of the personal health information and other data necessary" to fuel research reliant on healthcare industry big data, and talks about how IoT will play a growing role in medical records as well as research and other aspects of healthcare, and that today's HIPAA regulations "may not extend" to all those information types.

> "Since the issuance of the HIPAA rules, there have been significant advances and innovations in health information technology, health delivery systems, and health research."
>
> "This initiative will focus efforts to modernize the health information privacy and security protections paradigm, while enabling further advances in healthcare, research, and technology that will improve health outcomes and improve ability to detect and prevent cyberattacks. This initiative also encompasses efforts to streamline HIPAA requirements to make them less burdensome while at the same time ensuring robust enforcement as well as to evaluate new areas where HIPAA does not currently apply."
>
> —OCR Paper

Manufacturing

After healthcare, manufacturing businesses are the second most frequent targets of hackers, according to Experian. That's up from its third-place finish last year—and not in a good way.

Automotive manufacturers are most at risk. Nearly a third of manufacturing attacks in 2015 were executed on companies in this category. Chemical manufacturers were next in line.

Intellectual property is a key reason hackers attack manufacturing companies. Estimates indicate that 21 percent of manufacturers have suffered a loss of intellectual property due to security vulnerabilities.

Part of the reason manufacturing is a key target may have to do with the fact that it is behind the curve in terms of security. That's because unlike other industry verticals, like financial services and healthcare, manufacturing companies in the United States don't have compliance rules like Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), and HIPAA that they need to conform to. As a result, the manufacturing space as a whole is considered to be more lax than other leading verticals.

Manufacturing is also inviting to hackers because the industrial controllers that operate in every industrial environment lack basic security controls like strong authentication, access, and encryption controls. That means most attacks are connected to manufacturing environments do not need to exploit complex software vulnerabilities. They just need to get basic access to the controllers, from which they can change configuration, logic, and state.

Financial Institutions

Financial institutions are also favorite hacker targets. In the first quarter of 2016 alone there was an average of more than 4,000 ransomware attacks per day, according to Deloitte. That was a 300 percent increase from the 1,000 ransomware attacks per day the prior year.

Ransomware is one of the top cybersecurity threats to the financial industry. Fifty-five percent of the financial services firms surveyed by SANS recently said they consider ransomware the biggest threat to their business. And, more than 32 percent of financial firms said ransomware attacks have resulted in losses between $100,000 and $500,000.

Financial regulators are also looking to address cybersecurity as it relates to their areas. Virtually all banks and financial institutions have compliance departments to ensure that they comply with applicable laws, regulations, and rules in order to preserve the integrity and reputation of the bank. As cybersecurity requirements begin to be integrated into regulations, financial institutions are being tasked with more cybersecurity responsibilities as well.

The Sarbanes-Oxley Act (SOX) is one of the big regulatory concerns in this environment. It's most commonly described as a way to prevent Wall Street from misleading investors, although over the past few years there has also been a lot of discussion about extending it to address cybersecurity. Bills to add a cybersecurity component to SOX have been introduced, but did not pass. However, SOX may see some significant changes going forward. Some observers are questioning whether the new U.S. administration will eliminate SOX just as it did recently with the Dodd-Frank Act.

Retail

While healthcare, finance and manufacturing are top targets for hackers, retail has been hard hit as well. Although the number and cost of hacks on retailers have been far fewer than those incurred by these other industries, they've still been costly in terms of dollars, time, and reputation.

In the United States, outdated payment technology is partly to blame for retail's vulnerability. The good news is that the credit card industry is encouraging retailers to install chip card readers at their locations. But while many U.S. retailers are implementing point-of-sale systems based on the new chip technology, many others are dragging their feet.

That's at least in part because of the cost of such upgrades. Estimates indicate that upgrading to the new chip readers costs retailers an average of $2,000, or $35 billion nationwide.

Of course, point-of-sale systems are just one area of vulnerability for retailers. On-site Wi-Fi networks, which sometimes support both business processes and guest connectivity, can also be an easy in for hackers. The fact that more in-store devices – like digital signs, sensors that can track people and products as they move around stores, and surveillance cameras – are now connected only increases the attack surface.

Aside from payment card devices, point-of-sale systems are also targets as they are now connected to online inventory management and online logistics systems. Building energy-management systems, with ties to lighting, HVAC, and refrigeration, might also be on the network.

Businesses and organizations in other industry verticals are likewise at risk for a wide variety of cyberattacks targeting their connected devices, electronic data, and their personal privacy and safety. Consider how hackers can remotely exploit and control anything, from a website, to a back-end business system, to a connected car, to a power grid, to a country's weapons arsenal.

United States Federal Government

In the United States, the Federal Information Security Management Act (FISMA) is legislation that provides a framework to protect government data and resources against risks from both natural and man-made threats. Governments in other jurisdictions are also setting up their own guidelines and regulations. Whether and how FISMA might be impacted by the new administration remains to be seen.

Cybersecurity Regulations and Standards

United States Federal Government

The laws and regulations mentioned previously represent just a sampling of the way politicians, regulators, and other bodies have moved – and are moving – to address cybersecurity.

The previous presidential administration was active in the area of cybersecurity. In February of 2013, it issued an executive order entitled Improving Critical Infrastructure Cybersecurity.

Additionally, the previous presidential administration also passed the Cybersecurity Act of 2015. It aimed to create a framework for the voluntary sharing of cyberthreat information between private entities and the federal government, as well as within agencies of the federal government. It followed up in 2016 by releasing the "Report on Securing and Growing the Digital Economy," which identifies key cybersecurity gaps and how to address them.

In May 2017, the current White House administration signed the long-anticipated Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

The order commissions nine reports, covering cybersecurity issues across the areas of national cybersecurity, critical infrastructure cybersecurity, and federal network cybersecurity.

National Cybersecurity

In the national cybersecurity space, reports have been commissioned around two areas: Deterrence and protection, and workforce development.

Deterrence and Protection

The White House has asked for a report of strategic options for deterring cyber adversaries, and for greater international cooperation with allies and partners. Key U.S. departments have been asked to define federal international cybersecurity priorities, including investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. They have also been asked to define and document an engagement strategy for international cooperation in cybersecurity.

The Cyber Workforce of the Future

On the workforce front, a report has been commissioned to assess the scope, sufficiency and efforts to educate and train the U.S. cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education. The White House is looking for recommendations on how to support the growth and sustainment of the nation's cybersecurity workforce in both public and private sectors. The goal is to maintain or increase national-security-related cyber capabilities, along with calling out any recommendations for improvements.

In the interest of best practices identification, it has also asked for a study of foreign workforce development practices likely to affect long-term US cybersecurity competitiveness.

Critical Infrastructure Cybersecurity

Three reports have been commissioned in the area of critical infrastructure cybersecurity. What's critical infrastructure? Critical infrastructure is defined as, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

By November 2017, a report will be published by relevant authorities and agencies with input from critical infrastructure (CI) owners and operators, identifying the CI at greatest risk. The goal will be to set up an annual assessment and recommendations, review and to promote market transparency of cybersecurity risk management best practices. The executive branch is also looking to improve the resilience of the internet, and encourage collaboration to reduce threats from botnets and automated, distributed attacks.

The other reports in the CI area include assessing the impact of prolonged power outages on the U.S. power grid, and to cybersecurity risks to the defense industrial base, including supply chain, U.S. military platforms, systems, networks and capabilities, along with recommendations for mitigation.

Federal Network Cybersecurity

At the federal level, the presidential Executive Order 13800 directly holds the heads of departments or agencies accountable for managing their cybersecurity risk. The message is clear: No longer can cybersecurity breaches be blamed on IT. Cybersecurity is a management issue of the highest level.

Federal agencies have been directed to use the NIST Cybersecurity Framework. They have been asked to leverage shared IT services, such as cloud, email, and cybersecurity, or justify why they can't.

Agencies have been asked to document their cybersecurity risk and mitigation strategy, including pointing out obsolete systems, IT budget, and operational issues affecting cybersecurity risk.

Agencies have been asked to "regularly" assess their cybersecurity risk, and to improve policies, standards, and guidelines in order to align with the NIST Cybersecurity Framework.

U.S. States

Some U.S. states are tackling cybersecurity as well. In fact, cybersecurity legislation was introduced or considered in at least 28 U.S. states last year. Moreover, 15 states enacted such laws in 2016, according to the National Conference of State Legislatures.

Most of these laws and bills address national infrastructure and governmental agencies. But some of them specifically target the interests of businesses.

For instance, New York has established regulations that require banks, insurance companies, and other financial services institutions to establish and maintain cybersecurity programs. Those rules went into effect on March 1, 2017.

Legislators on the West Coast have addressed cybersecurity as well. One of the three cybersecurity bills signed into law in California last year makes it a crime for a person to knowingly introduce ransomware into any computer, computer system, or computer network.

Colorado, Utah, and Washington are among the other U.S. states that have put cybersecurity laws in place. A new Colorado law calls for the creation of a state cybersecurity council to provide policy guidance to the governor. That council will also coordinate with the general assembly and the judicial branch regarding cybersecurity. Utah has enacted civil penalties for hackers. In addition, Washington State has established the State Cybercrime Act.

Global

Other countries and regions in the world also have cybersecurity on their radar. At least a few of them have already put laws and other rules in place to address it.

For example, the European Union (EU) last summer approved the General Data Protection Regulation (GDPR), cybersecurity rules that force businesses to strengthen their defenses. Specifically, the GDPR requires banking, energy, and major tech companies to report attacks. The new rules unify the EU's approach to issuing and enforcing cybersecurity regulations and strengthen privacy protections for its citizens.

In October, the informal bloc of industrialized nations referred to as the "Group of Seven" (Canada, France, Germany, Italy, Japan, United Kingdom, and United States) published a paper that calls for entities in the financial sector to establish cybersecurity strategies. That should include establishing processes that monitor and detect cyber incidents and that periodically evaluate their effectiveness, according to the document, which was distributed by the U.S. Department of the Treasury and the Board of Governors of the Federal Reserve System.

Meanwhile, Australia has developed a national strategy through which government and the private sector collaborate on cybersecurity. The effort has yielded a white paper identifying major risks and how to address them. Australia has established the Australian Cyber Security Centre, which aims to make the country's networks more difficult to compromise.

Indeed, the areas of cybersecurity, privacy, and technology are the fastest emerging areas of law and regulation worldwide. Governments of all regions have needed to rapidly educate themselves on the potential ramifications of cybersecurity issues, and are busy crafting new regulations and adapting older regulations to address new issues created by this rapidly evolving environment. On the law enforcement side, governments are struggling to train traditional officials on digital forensics, how to collect and handle digital evidence, and how to handle technology-assisted crime.

Industry

Industry organizations are working to encourage governmental action in cybersecurity as well. For example, in the United States, the National Association of Manufacturers (NAM) has been calling for a public-private partnership to encourage investment beyond ordinary levels of commercial cybersecurity spending. NAM is also pushing for the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), and the research arm of the Department of Homeland Security to prioritize funding for IoT security research. There have also been major efforts to secure critical national infrastructure, such as the power grid or energy sector security.

Best Practices

The commentary above illustrates just a few of many vulnerabilities that need to be addressed to secure things at the data, device, and network levels.

As already mentioned, endpoints like computers, smartphones, and the diverse and growing array of IoT devices should be secured. Some key best practices on this front include: changing device passwords; having intrusion detection, secure remote update capability and security management as standard features; activity logging and monitoring of suspicious activity; turning on security as a default; reviewing device configurations; and subscribing to security advisories from your device and network infrastructure suppliers.

Key Best Practices

- Changing device passwords
- Having intrusion detection, secure remote update capability and security management as standard features
- Activity logging and monitoring of suspicious activity
- Turning on security as a default
- Reviewing device configurations
- Subscribing to security advisories from your device and network infrastructure suppliers

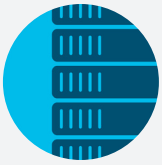
To guard against such threats, it's important to take the following actions:

Actions to Take

Give people access
only to the methods of access and network equipment ports that they require (least privilege)

Establish authentication and authorization practices
(strong identity management)

Log and account for all access
should you need to do an audit later on (activity monitoring)



Protect locally stored data
from viewing and copying (protecting data at rest)

Manage passwords
by maintaining and controlling them via a centralized authentication, authorization, and accounting (AAA) server

Inform users of policies
via legal notice developed in conjunction with company legal counsel for interactive sessions.

Properly configuring firewalls and other controls, leveraging monitoring controls and employing encryption are some ways to protect the network and data.

Cybersecurity obviously impacts networks as well. Networks are under siege by botnets, denial of service (DoS) attacks, intrusions, Layer 2 attacks, man-in-the-middle attacks, privilege escalation efforts, routing protocol attacks, session hijacking, spanning tree attacks, and unauthorized access, among other threats.

The Need to Develop Talent

Investment in and cooperation around hard-to-solve problems is usually a good idea. But organizations cannot afford to take anything for granted, and must prepare to do a lot of the work of securing their organization internally and with partners.

Solving this problem won't be easy. Addressing cybersecurity is not only about solving a particular problem. It is also about putting in place the people, processes, and technologies so we can protect against the latest risks and respond to them when needed.

Cybersecurity is clearly an entirely new kind of challenge. It's complex. It's ever-changing. And it's going to require people with specific kinds of knowledge and skillsets.

That in itself is a problem, because there's a shortage of tech experts out there, particularly those with cybersecurity skills. Multiple sources indicate that there will be an unmet need for between one and two million cybersecurity professionals by 2019.

That means that the industry needs to create and update the workforce for this new world in which cybersecurity is an important new discipline.

In this marketplace cybersecurity jobs are growing three times faster than are IT jobs. They're increasing at a rate 12 times that of the overall job market. More than one-third of employers ask cybersecurity job candidates for industry certifications.

When it comes to cybersecurity, there are four main job types:

- Chief information security officers (CISOs), who set policies, priorities, and budgets around cybersecurity. They understand their organization's risk profile, regulatory, and legal responsibilities, and business priorities, including how they interrelate with cybersecurity and risk.
- Security architects and security engineers are tasked with designing and securing cybersecurity architecture, controls, procedures, frameworks, and initiatives in order to support the policies set by the CISO.
- Network security infrastructure engineers, technicians, and administrators are required to build and maintain secure solutions.
- The security operations team is composed of a diverse group of personnel involved with 24x7 detection of and response to cybersecurity events. This team may include security analysts, first responders, digital forensics investigators, and a security operations center (SOC), as well as internal and external auditing resources.

Cisco offers training that is useful to all of these roles, and certifications for growing your cybersecurity career as it evolves.

The Cisco CCNA Security, CCNP Security, and CCIE Security certification programs offer practical, relevant, and job-ready certification curricula closely aligned with the specific tasks needed by cybersecurity professionals. The CCNA Security certification lays the foundation for such job roles as network security technician, administrator, or support engineer.

The CCNP Security certification offers employers proof of job-ready training and skills from experienced, Professional-level network security engineers. The CCIE Security certification recognizes individuals who have the knowledge and skills to implement, and support extensive Cisco network security solutions using the latest industry best practices and technologies.

CCNA Cyber Ops is the most recent Cisco cybersecurity certification, focusing on the role of the security analyst working in a Security Operations Center. It introduces IT personnel to valuable skills, enabling them to monitor IT security systems, detect cyberattacks, gather and analyze evidence, correlate information and coordinate responses to cyber incidents.

The role of the Security Operations Center Analyst is to determine through various types of event monitoring whether an intrusion or security-related event has occurred or is currently occurring. The telemetry data analyzed by these individuals is commonly obtained through various "feeds" that are presented chronologically to the analyst as they occur.

These feeds are also commonly warehoused in tools such as logging databases and security information and event management (SIEM) appliances. This allows the analyst to historically review the feed data as well as to obtain dashboard-style access to the data, associated metrics, and correlation of additional feeds in order to simplify the starting point for any potential investigation.

For Students

People who work in cybersecurity should have experience with, and skills and abilities related to, operating systems, coding, networking, and basic security principles, according to Tom Gilheany, Cisco's product manager for security training and certifications.

They should know how applications, subsystems, and users reside in an operating system and how they are controlled and interact with each other. That will be useful if they need to clean up after a system has been compromised.

It's also helpful to know how to code in at least one programming or scripting language, since software represents a large part of the attack surface, says Gilheany. C, Python, and Perl are all good choices, he adds.

Additionally, according to Gilheany, individuals who work in cybersecurity need at least a fundamental understanding of networking. Professionals in this role should know both about cybersecurity and physical security.

But how do individuals who are considering expanding their knowledge in the area of cybersecurity decide what kind of jobs they want to pursue and what they'll need to do to be considered for those positions? When choosing a cybersecurity career, it is important to first think about who you are, and how you like to work. There are many types of cybersecurity roles available, and it is important to select one or more that match up with your interests, and how you enjoy working.

More Information

If you're interested in getting more information about cybersecurity opportunities, training, and certification, here's where to go next:

- This Cisco Learning Network online resource is a good starting point to help you better understand how you can advance your cybersecurity career and cybersecurity business readiness.
- The CCNA Cyber Ops Study Group site is a Cisco Learning Network community in which you can ask questions, connect with others as they prepare for certification exams, and share ideas.
- Read Tom Gilheany's blog, "Getting Started in a Cybersecurity Career."

Looking ahead

The digitized economy is only going to get more complex. 2017 saw a new wave of regulations, standards and shifting expectations across all industries. Regardless of where an organization is on its journey to digitization, it's going to need cybersecurity professionals to help it safely guide the course.

Good luck. And have a safe journey.