CompTIA

The Computing Technology Industry Association
Docket No.: 160725650-6650-01
National Institute of Standards and Technology
Input to the Commission on Enhancing National Cybersecurity
September 9, 2016

515 2nd St., N.E. Washington, DC 20002

Executive summary

Everyday, technology is becoming more engrained in our everyday life. With this incredible change comes the challenge of security and having the right workforce in place to manage those security threats. To combat increasingly sophisticated cyber attacks, it is necessary that we move beyond hardware and software solutions (e.g. firewalls and intrusion detection) and into up-skilling our workforce. Furthermore, we must ensure that we foster an environment that encourages innovation while enhancing the existing public-private partnership between industry and government.

In our comments, we outline some current security trends, essential skills needed in the workforce today, as well as knowledge required in the short-term (1-3 years) and the long-term (the next ten years). We will also discuss specific examples of public and private sector cooperation that have created a template for success as we work to secure information technology implementations.

We appreciate the opportunity to provide insight to the Commission and look forward to our continued engagement with our government partners.

Current security trends affecting today's IT environments

Security continues to be a top IT priority for companies, as the recent history of new technology models and the reliance on data has brought focus to the need for tight security and privacy. Accordingly, the IT security market is growing, with Gartner projecting overall spending on enterprise security to reach $100.3 billion globally by 2019.[1] However, nearly half of all IT security professionals believe there is some degree of skill gap within their organization. Fifty-three percent of companies with gaps want to be more informed about current threats, followed by desired improvement in current security technology and awareness of the regulatory environment. [2]

That said, issues such as malware, denial of service attacks, and privacy concerns continue to present challenges for the industry. 2016 CompTIA research finds that nearly three in four organizations have experienced a security breach. CompTIA's International Trends in Cybersecurity report notes that security will become a higher priority for more than 8 out of 10 managers. We need to do more to build upon our workforce so that we can address these growing concerns, and we need to do it quickly.

New technology developments

Rapid introduction of new technologies including the Internet of Things (IoT) and cloud storage offer tremendous opportunities for how we function in our daily lives and operate businesses. There are more connected devices in operation than there are people on the planet. Despite security breaches causing devastating effects, one could reasonably argue that given the sheer number of devices and applications in use, the volume of security breaches is actually a low percentage of the total. Nevertheless, there is a responsibility for government and industry to work together to examine some governance approaches and additional best practices. The resulting approaches should foster an environment that will encourage innovation and growth without undue burden from unnecessary regulations. As part of this discussion, we must also focus on programs and policies to ensure we have both the quantity and quality of workers that we need.

Internet of Things and the New Mobility: Cybersecurity implications

IoT has fully entered our lives and continues to grow. According to International Data Corporation (IDC), worldwide revenue from IoT enabled devices will reach $1.7 trillion dollars by 2020. Yet even as we seek to maximize the potential of IoT, industry is mindful of some of the challenges:

1. Protecting personal information
2. Securing networked systems
3. Minimizing risks to personal safety

---

[1] CompTIA 2016 IT Pro Security Report

[2] CompTIA 2016 IT Pro Security Report

The U.S. government and industry must work together to help promote an atmosphere of "human trust" in the design of our networked services. In their 2015 IoT report, the Federal Trade Commission recommended that "companies should build security into their devices at the outset, rather than as an afterthought," and our companies are designing their products in just this way. CompTIA member companies take security protections very seriously and design products for their customers with these considerations in mind.

That's not to say that there isn't still work to be done. As new technologies take root or become ubiquitous, industry must continue to examine and adopt additional "best practices." IoT is one of the fastest-growing sectors of the economy, and new companies are releasing products every day. Some companies, particularly small businesses and new start-ups, may simply not be aware of what it takes to properly secure their customers' data. Furthermore, as IoT creates new tranches of data, we need to examine ways to keep pace with the intake of that data.

In the next section of these comments, we detail some of the technology trends that are unfolding and we make two sets of recommendations:

- IoT-enabled security solutions that will generate vast amounts of data, testing the ability of human beings to keep up with threat intelligence and alerts;
- Security solutions designed for the digital age that incorporate machine-to-machine intelligence (automation) for immediate, automated security control.

While security protections must be a part of the design of technology, increasingly we need to upgrade the essential skills of the workforce. First, we must make end-user/employee training for cyber hygiene ubiquitous. Second, we should seek to enhance the training for cyber professionals with increased analytics training and adding a new team to "live fire" anti-hacking exercises.

Cloud adoption: What to Watch For

The IT industry has gradually implemented sophisticated cloud solutions over the last decade and has made great strides in addressing security concerns. However, as with any still relatively new technology, moving services to the cloud may present challenges over the next several years that include:

- Going beyond traditional uses of encryption and authentication: While a strong first defense, encryption is not the only answer. It is, however, vital for enabling multi-factor authentication. The pick-two combination of something you have (like a credit card or a token generator) with something you know (a password, for example), or what you are (biometric information) is our best line of defense for protecting what is sacred. Multifactor authentication is a vital solution that should be embraced.
- Detecting lateral movement in virtualized environments: As innovations continue in regards to "bare metal" virtualization and containerization, a premium will be placed on staying ahead of security requirements for data in a virtualized environment. Data centers and cloud providers are working to detect and prevent malicious code from being inserted "beneath" the operating system or any virtualization environment.

As cloud adoption continues to expand, security protections must be a part of the design of technology while upgrading the essential skills of the workforce. To that end, we must make end-user/employee training for cyber hygiene ubiquitous. We should also seek to enhance

the training and certification for cyber professionals with increased analytics training and adding a new team to "live fire" anti-hacking exercises.

Data, search, and analytics

As the value of data has become overwhelmingly clear in recent years, we have seen companies of all sizes collecting personally identifiable information (PII). This data is used to enhance our lives through the many conveniences that technology has to offer. Furthermore, industry is conducting sophisticated analysis of structured and unstructured data. The results of this analysis can provide key strategic information that determines how a company will act in a particular market. Collecting this information ensures that IT departments continue to implement best practices for data at rest and data in motion.

Data At Rest:

IT departments, IoT users, and cloud providers will need to ensure that “big data” analysis of information remains secure. Information derived from analytics will continue to increase in value. Therefore, these assets will need to be secured in sophisticated ways to reduce intellectual property leakage and theft.

Data In Motion:
Increasingly, analytics service organizations have been created which help companies to crunch data and identify trends. These services will be used more and more by small and large companies worldwide. IT departments for both the analytics services and for the clients will need to create specific encryption schemes to ensure data streams are secure.

As threats to data security increase, professionals will need to adopt an analytics-based approach to network security. A combination of penetration testing, hardware-based solutions like firewalls and intrusion detection, and software-based solutions like antivirus and patch updates are needed to lower attack frequency and success.

Cybersecurity analytics greatly improve threat visibility across a broad attack surface by focusing on network behavior, including an organization’s interior network. Over the past decade, the industry has taken a much more aggressive stance as the mantra has been to, “think like a hacker to stop a hacker.” While attacks will inevitably continue, “white hat” and “ethical” hackers are entering the workforce in increasing numbers, and will hopefully continue to grow. An environment where workers obtain skills to evaluate information in more creative ways will enable them to keep pace with the pervasive security issues that tech trends such as IoT present.

Ensuring Our Workforce Is Equipped For the Cybersecurity Challenges Of Today and Tomorrow

The continued adoption of new and emerging technologies has presented expanded the attack-surface. Some of the challenges we face today include increased opportunity for human error due to Advanced Persistent Threats (APTs) and the need for business continuity plans. Below we take a closer look at these challenges and some proposed solutions:

Human Error and APTs

The majority of attacks focus on exploiting naïve end-users or the technologies they use.

According to the IBM 2015 Cyber Security Intelligence Index, unauthorized access incidents rose from 19 percent in 2013 to 37 percent in 2014. Furthermore, according to the report, "with an ever expanding array of malware from which attackers may choose— including viruses, worms, Trojans, bots, backdoors, spyware and adware—it seems fairly certain that malicious code incidents will continue for the foreseeable future."[3]

Today's Advanced Persistent Threats (APTs) involve the introduction of malware by unsuspecting end-users to compromise traditional security measures and create malicious "overlay" networks. These networks introduce botnets, ransomware, and spying software designed to obtain a company's intellectual property. Many of these networks are designed to store information – such as credit cards and industry secrets – culled from individuals and companies around the world. Most of the time, these persistent threats are introduced over long periods of time, rather than through a single event

Because APTs can be successful through any employee, all employees should be aware that these threats exist. Cybersecurity training for all company employees is vital, and the evolution of that training to keep pace with the evolving attacks will undoubtedly present a challenge. In many government entities, other forms of training are mandated annually for all employees (i.e. sensitivity training) yet cybersecurity training is optional and stagnant. We urge the federal government to lead by example by requiring basic cybersecurity training/hygiene for all employees.

Furthermore, security workers should be trained and equipped to identify long-term threats. Training and certification of the security and IT workforce ensures that workers are trained to configure systems so that they are able to gather and interpret seemingly innocuous events that occur over time to detect long-term, continuous threats.

Business Continuity / Disaster Recovery

Too few organizations are prepared to answer the question, "What happens when your defensive measures and auditing tactics fail?" In an era where man-made and natural disasters have become daily events, business continuity will become an increasingly important topic.

The ever-increasing sophistication of cyber threats means that we will never be able to prevent all attacks. The focus then turns to how quickly an entity can recover. Technologies that help businesses and governmental agencies respond to security breaches will become increasingly popular. These plans are especially important for government entities that provide essential services to citizens. Again, we believe that the government should lead by example by ensuring that necessary plans are in place. The government should work with industry to ensure that entities that want to adopt contingency plans have the necessary tools and resources available to them to keep the ecosystem running in the event of disaster.

Skills for the IoT Workforce

---

[3] IBM 2015 Cyber Security Intelligence Index, file:///Users/randi%20parker/Downloads/SEW03073USEN.PDF

The key to cybersecurity success is enhancing the skill set of the individual worker so that he or she can carefully evaluate and interpret critical information before a security event occurs.

Over the next decade, continued adoption of IoT will change the nature of the workforce. For example, the IT department role will evolve from a service provider to a valued partner in virtually every part of the business. This development alone will demand new organization, skills and lines of authority.

But as with IoT, we will see the IT department concern itself with myriad issues, with an increased focus on privacy. As intellectual property, trend information, and personally identifiable information begin to fall under the purview of IT departments, workers will need to understand the privacy implications involved in making even the most basic decisions concerning how to secure data. IoT implementations necessitate IoT security based training and certification capabilities to be a vital component of any entity's IoT security architecture.

Lessons Learned: Solutions and examples from public and private sector cooperation

The United States Department of Defense (DOD) has worked closely with the training and certification community to consistently up-skill workers. Many certification organizations have participated in the 8570 and successor 8140 initiatives. These initiatives, which require DOD personnel and contractors with information assurance titles to have cybersecurity certifications, are vital for the US government workforce. This requirement ensures individuals are trained and certified in the skill sets required by their job.

The National Initiative for Cybersecurity Education (NICE) is also a critical element to properly training the nation's workforce. We have also worked closely with NICE to provide real-time information concerning the location of qualified IT workers. Like with DOD, CompTIA continues to provide input and support to this initiative to ensure that skills are being appropriately mapped to jobs.

Furthermore, in 2015, CompTIA, in partnership with Burning Glass Technologies, received a three-year grant from the National Institute of Standards and Technology (NIST) to develop an interactive cyber jobs heat map that will show the demand for and availability of critical cybersecurity jobs across the nation. The project, which is being funded through NICE, will provide data to help employers, job seekers, policy makers, training providers, and guidance counselors in order to meet today's increasing demand for cybersecurity workers. The first version of the heat map will be released in October 2016.

Moving forward, we find that the following steps are critical to ensuring our workforce has the skills they need:

- Hands-on training: It is not enough to simply lecture about security during training events. It is vital that we continue to cooperate and develop:
    - "Live fire" training exercises; and
    - Experiential learning solutions that quickly evaluate existing worker skill sets and provide consistent, quick feedback concerning necessary new skills.
- Continued assessment: Workers should be given high-quality, fair assessments to ensure that they have the skills to protect today's networks.

- Continuing education: We are convinced that effective continuing education programs are essential to up-skilling workers. As new technologies and techniques emerge, they change the complexion and substance of a network. Professional cybersecurity workers should be given ample opportunity to re-learn existing skills and also learn new skills.

Future developments

We regularly work with subject matter experts (SME) panels at CompTIA. They have recommended the following six areas of emphasis in the future:

1. Risk and compliance: Insurance companies, financial backers, and government agencies alike all have determined that a proper approach to compliance and analytics-based analysis is vital. Financing and merger activity will not move forward unless an organization can prove that they have taken proper steps.
2. Secure software development: Zero-day attacks, including those caused by buffer overflows and other results of flawed coding processes, continue to be a problem. Proper oversight of code development procedures promises to reduce these issues in both the proprietary and open source development communities.
3. Offensive security (e.g., penetration testing, threat/exploit modeling): An analytics-based approach is vital to improving penetration testing.
4. Defensive security (e.g., detection and response): It is not enough to simply use vulnerability assessment software. Cybersecurity workers must be trained in identifying trends and identifying both false positives and "false negatives" as they conduct scans and review logs.
5. Cyber intelligence: The activity of sifting through gathered information and analyzing it to discover trends.
6. Security engineering/architecture: Careful review of planned network infrastructures (cloud, IoT, and traditional) to ensure that networks are designed securely.

Conclusion

While technology has made so many facets of our daily lives easier, it has also brought challenges that will continue to be addressed. Industry's commitment to security remains strong and the future security of devices will rely on a modernized workforce that is well-trained and equipped to address the challenges that inevitably exist when rapid technology innovation and bad actors exist. To that end, enhanced cooperation between government and industry is vital for our overall security posture. This partnership, which has had a great deal of success in past challenges, must remain nimble and easily adaptable as the threat landscape evolves. With a strong public-private partnership and a well-trained workforce, we trust that together we will be able to rise to the challenges that the future brings.