RESEARCH REPORT

THE EVOLUTION OF SECURITY SKILLS

April 2017

There's little doubt that cybersecurity has become a critical topic—not just for IT, but for business in general and society as a whole. Today's digital organizations are driven by new technology and dependent on orderly data, and everyday life increasingly happens on top of connected infrastructure. The risks posed by cybersecurity attacks are monumental.

To mitigate those risks, new skills are needed. This study examines the state of security skills in business—which skills are needed, which business units need training, and what companies are doing about the problem.

KEY POINTS

Security is a growing business imperative

Cybersecurity is not a new concept, but it is taking on new importance. As businesses invest more in technology to directly drive their outcomes, potential attacks can carry disastrous consequences. As security becomes a higher priority, companies are viewing it as a standalone discipline, combining technology, procedure, and education to create an overall posture.

Security skills need to be deep and wide

A range of skills is needed to secure modern infrastructure, respond to incoming threats, and ensure proper operations. Between 18% and 32% of companies say that they need significant improvement to existing security expertise across various topics. The new skills also must come with a new mindset: building an impenetrable defense is no longer practical, and proactive efforts can help find problem areas before attackers discover them.

New training is needed to close skill gaps

Some companies are in a position to hire or partner in order to meet security needs, but the most common approach is to improve the existing workforce. For technical workers, 60% of companies use training to build security expertise, and 48% pursue certifications. Many companies are also extending training to the general workforce. Ongoing programs that measure knowledge can improve security literacy for employees that are increasingly using and procuring technology.

Source: Burning Glass

CompTIA

THE DOMAIN OF CYBERSECURITY

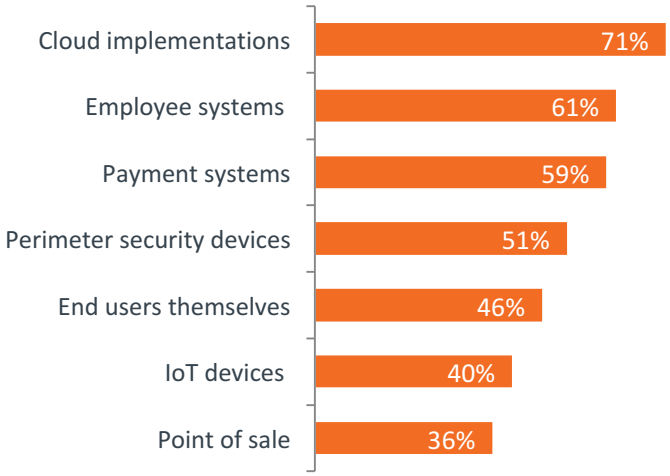
There's nothing new about the concept of securing digital assets. As early as the 1950s, organizations (especially government agencies) recognized the potential risks involved in the use of computers. The National Security Agency's TEMPEST specification and the United States Communications Security (COMSEC) Board are examples of early initiatives born out of this awareness.

In the 1960s, it quickly became apparent that computers would become a mass market phenomenon rather than remaining relegated to those companies with the deepest pockets. Systems evolved to meet growing demands, but this evolution led to design flaws that were uncovered by a growing army of computer science researchers. While early discoveries were academic, flaws were soon exploited by those with less noble intentions. The game was afoot.

Today, security is top of mind for nearly every business. New breaches hit the headlines on a regular basis, and while the impact so far has stopped short of being truly catastrophic, the stakes are getting higher. Thirty-three percent of companies in CompTIA's survey say that security is a significantly higher priority for them today than it was two years ago, but 49% expect that security will be a significantly higher priority in two years than it is today. FURTHER READING

Modern technology trends are changing the nature of the security domain, though. Where the goal used to be a secure perimeter, movement to the cloud has emphasized the need for security in discrete systems and data sets. Cloud implementations are getting heavy attention, but employee systems (such as CRM or HR) and payment systems are also getting focus, even if those systems are not immediately targeted for a cloud migration.

Areas of Higher Priority in Past Two Years



As the technology stack for security becomes more complex, going beyond firewalls and antivirus programs, the domain is also growing to include other disciplines. The creation of secure processes and policies—such as risk analysis or compliance management—ensures safe operation in digital environments. In addition, end user education is needed to raise security literacy as more and more workers use technology for their jobs.

To properly address all these issues, companies are building teams focused solely on security. Steven Katz is generally regarded as the first CISO, a role created for him when he joined Citibank in 1995. Now every Fortune 500 company has a CISO, and the development of security teams is slowly spreading to firms of all sizes and all industries.

Unfortunately, those teams are still scrambling. Security is a game of leapfrog. Many tech products come with security baked in to hardware and software, yet attackers continue to find loopholes. Businesses must constantly monitor for breaches, respond to any incidents, build new defenses, and test their strategies before cybercriminals find a new weakness.

Most companies are left with skill gaps, areas where the in-house workforce or partner network lacks expertise. Only 33% of companies feel that they have a very high level of security understanding within the organization. While this is primarily driven by the security knowledge of the overall workforce, skill gaps among those responsible for security also factors in. FURTHER READING

The first step in closing the gaps is understanding that while security is a standalone domain within IT, it is still an advanced domain built on an understanding of IT basics. This is especially true for the technical aspects of security, where knowledge of networks, storage, devices, and cloud systems is needed to properly construct and monitor a layered security defense. To a smaller degree, foundational knowledge is also important for building the right processes and delivering effective education. Once foundational knowledge is in place, specialized skills can be added. This study explores the details behind the demand for security, touching on all three facets of the overall domain.

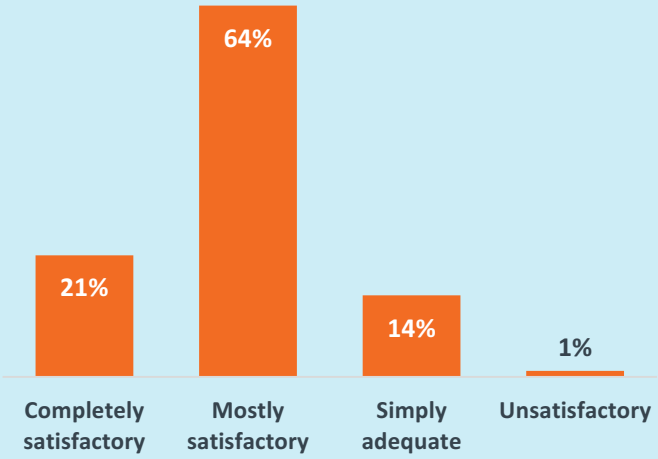
To move forward, a new awareness is needed. The mentality of the 1950s and 1960s led to solid practices around information security, based on the view that data was a new type of corporate asset. Modern cybersecurity requires both an understanding that data is now critical to business survival and a strategy around technology, process, and education that all serve to protect that vital resource.

THE STATE OF CORPORATE SECURITY

Before entering a discussion on security skills, it is instructive to know how companies view security in general. Views on security will drive the urgency with which firms assess and improve their skills. Businesses that believe their security is adequate will not be very motivated to raise the level of expertise.

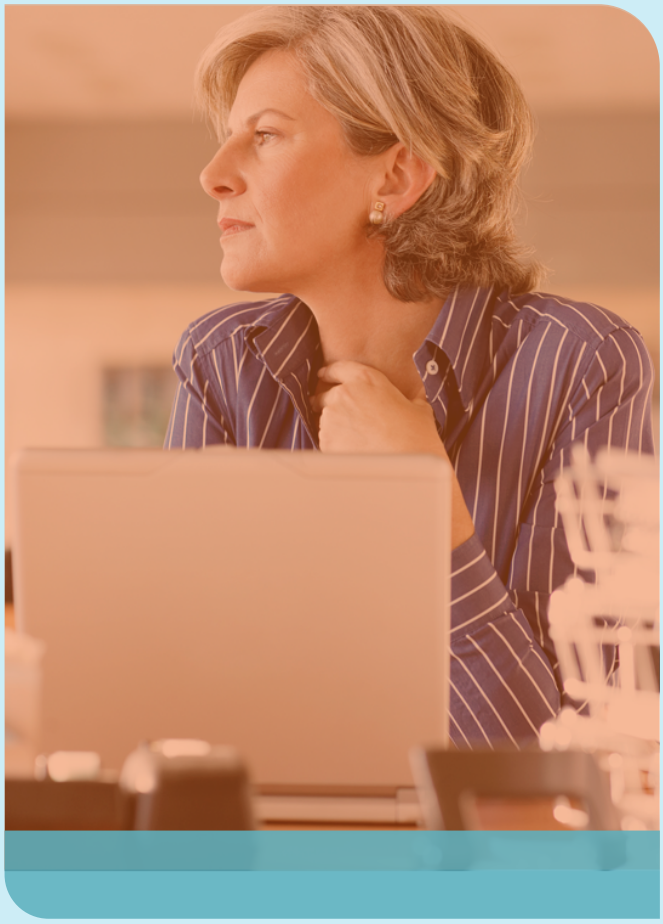
As it turns out, not many companies fall into that camp. Just 21% of businesses feel that their current level of security is completely satisfactory. This sentiment is relatively consistent across companies of different sizes, though there is some difference based on job role. IT staff tend to view security more positively than business staff, perhaps due to a more technical view of security rather than a view that includes processes and employee awareness. FURTHER READING

Self-Assessment of Security



Many businesses may feel unhappy with their security condition thanks to events that have precipitated a change in their security approach. The most likely example of such an event is a change in IT operations, cited by 56% of businesses. Cloud computing and mobility introduced significant shifts to IT architecture, and many organizations moved to adopt these models without fully appreciating the security impact. Now they are correcting for that and taking the appropriate steps.

Unsurprisingly, reports of security breaches at other firms is another primary motivator, cited by 44% of businesses. Security breaches are hitting the headlines regularly. While the public attention may fade after the initial attack, those that choose to follow the aftermath see that these breaches drive significant cost. While none of the major companies breached have gone out of business yet, there is financial cost in recovery and lingering cost to reputation.



The final major driver for a security change is knowledge gained from training or certification, cited by 37% of businesses. This driver is directly related to improving skills, and as more companies begin to close their skill gaps, it may create a virtuous cycle whereby new knowledge drives new approaches which drive a need for even more knowledge.

What about those companies that are completely satisfied with the state of their security? Certainly some of those firms truly have done due diligence, analyzing their security posture and making the necessary changes. Others, though, may have their head in the sand. The top challenge in pursuing new security initiatives is a belief that security is "good enough." Other challenges include a prioritization of other technology and a lack of budget that is dedicated to security. FURTHER READING

Overall, most companies are not quite where they want to be with security, but this may be more of a general feeling than a specific assessment. With a focus on technology that directly drives business outcomes and a lack of dedicated security budget, businesses may need more help in understanding the exact skills needed and the way that those skills fit into an organizational structure.

CompTIA

RANGE OF SECURITY SKILLS

Transition is a common theme throughout CompTIA's recent research. Data from various studies show businesses and industries that are straddling the line between an old way of doing things and a new model. Perceptions of security skills fit into this pattern. Companies are shifting from a technology focus and a defensive mindset to process improvement and a proactive approach.

Security Skills in Need of Improvement

In a case of familiarity breeding contempt, the top two skills in need of improvement are general infrastructure security and knowledge of various threats. Infrastructure security has expanded from basic firewalls and data encryption into application-aware firewalls, intrusion detection/ prevention, and network monitoring. Similarly, the variety of attacks grows unabated, with Kaspersky Lab reporting that it discovers 323,000 new malware samples each day and other attacks such as denial of service and SQL injection adding to the complexity.

However, building a modern security framework involves much more than beefing up infrastructure defenses in light of new attack vectors. The desire for improvement among the remaining security skills shows a growing awareness for the breadth of expertise needed for modern operations.

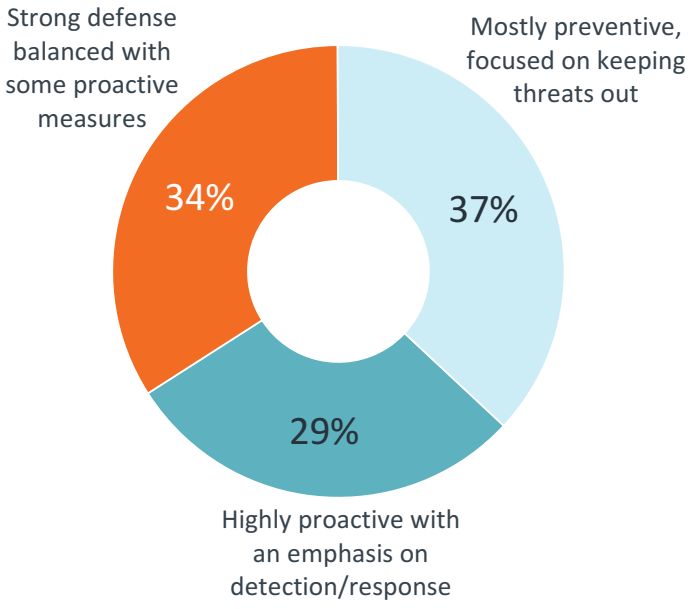
On the technical side, cloud computing drives a need for security directly attached to applications and data. As these components move from on-premises systems into cloud providers, they need specific safeguards on top of the security provided at the layer of the cloud offering. Identity management is one example of added security, where access is granted on a granular level within an application, rather than being granted at a corporate perimeter.

Compliance, risk management, and incident response are all examples of areas where better procedures can lead to an improved security posture. The complicated regulatory environment drives a need for a thorough understanding of various state and national laws, and expertise in business process management (BPM) can help ensure that all functional areas are following best practices.

Across the board, small businesses trail their larger counterparts in reporting a need for skill improvement. Given a history of de-prioritizing security, it is highly unlikely that these firms currently have the appropriate level of skill. Small companies must quickly realize that new skills are needed as new attacks may target the lowest defenses rather than the most profitable victims. FURTHER READING

For all companies, new skills must be combined into a new approach. In a world of constant, evolving attacks, a mentality of preventing all breaches is outdated. Organizations must shift to proactive measures, including external audits, penetration testing, and security training. Strong defenses will always play a role, but they must be coupled with ongoing offensive activity.

Shifting from Defense to Offense



CompTIA

DEALING WITH THREATS

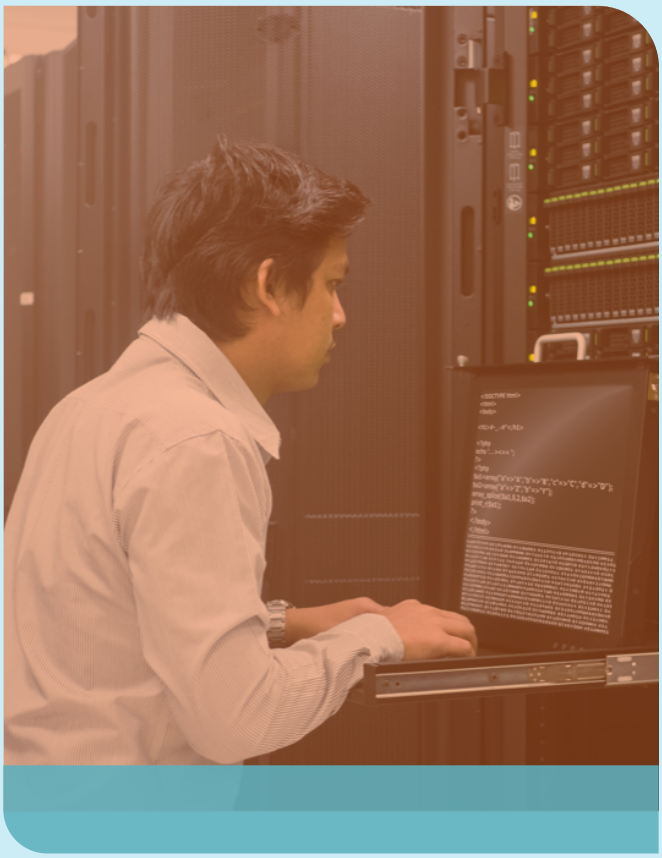
The volume and variety of cyberattacks is one of the primary factors contributing to the security skills shortage. Today's technology stack contains a diverse set of components, and any of these pieces could be vulnerable. A breach in any one element could disrupt operations, leak data, or create access to other parts of the system.

CompTIA research has consistently shown that companies place the most emphasis on those threats that they understand the best. Malware and viruses, two of the oldest forms of cyberattack, are typically the categories that get the most attention.

Cyber Threat	Likely to affect	Need to understand better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware hacking	34%	29%
IP spoofing	32%	29%
Ransomware	31%	30%
Attacks on virtualization	30%	30%
Social engineering	26%	26%
Hardware-based attacks	26%	25%
DDoS	24%	22%
IoT-based attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the middle attacks	20%	23%
SQL injection	18%	20%

To the extent that viruses and malware continue to be effective, there will certainly be a need to remain vigilant and informed about the latest variants and techniques. However, many other forms of attack have emerged, often utilizing different methods for the ultimate goal of digital disruption. For example, phishing and social engineering are not direct attacks on business systems, but on users. With the information provided by unsuspecting individuals, attackers can then access more valuable resources.

Unfortunately, after the three high-profile threats, there is a dramatic drop in the number of companies that feel specific attacks are likely to cause an impact. SQL injection, one of the most common ways to infiltrate a web database, ranks



last on the list. Even ransomware, a topic that has received a great deal of press, is only a topic of concern for 31% of companies.

Even more unfortunately, there is not much difference between executives and IT professionals in the desire to better understand various threats. Only a few percentage points separate these groups in each threat category. Even the technical specialists responsible for security are likely spread too thin to fully comprehend and appreciate the new threats to digital organizations.

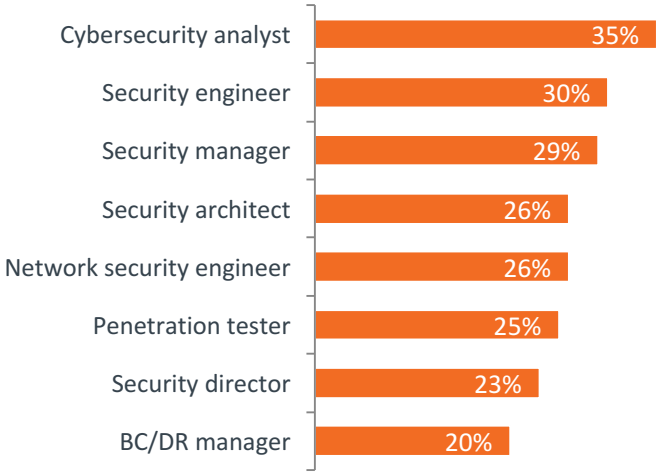
The first step in threat management, then, is simply in gaining an appreciation and an understanding of the many types of threats in play today. Many companies have moved aggressively in the direction of new technology—such as cloud computing and mobile devices—but have not fully considered the security implications in broadening their IT architecture.

With an understanding of various threats in place, companies can build a layered defense. SIEM, which provides an aggregation point for the different layers in a defense strategy, is the most popular tool for threat management , but other tools and techniques such as host scanning, network segmentation, and sandboxing are also utilized. FURTHER READING

BUILDING A SECURE WORKFORCE

As the practice of security begins encompassing more disciplines and the majority of security breaches are due to human error, companies must turn their attention to the skills and literacy of their workforce. The primary focus may be the specific roles and expertise of the technical team, but the solution must extend to awareness and training for all workers.

Security Roles Companies Have Difficulty Filling



Although 14% of companies do not have dedicated security roles, likely folding security into the responsibilities of an infrastructure team, many firms are searching for security specialists. The top role in demand is cybersecurity analyst, an individual that proactively monitors networks and uses analytics to assess threats and provide remediation. CompTIA's CSA+ certification validates the skills needed for this quickly-growing position.

If there is sufficient budget, companies hire additional security personnel or partner with a third party on security issues. However, training and certification are generally the favored methods for building advanced security expertise. Sixty percent of companies use training to close their security skill gaps, and 48% pursue certifications for their technologists. While some companies are deterred by the cost and time required to earn formal certifications and feel that training is adequate, those that follow through on certs find that they provide a higher degree of credibility, better proof of knowledge, and improved candidacy for open positions. FURTHER READING

More and more companies are extending training efforts to the overall workforce. With increased technology usage and technology procurement by business units, stronger security literacy is needed to avoid pitfalls and ensure secure operations.

Organizations are starting to understand that security training is needed for all jobs and that some oversight is needed to develop a security-aware culture. The top segments identified as needed security training were middle managers, in both business units and the IT function. Executives are next in line, and this focus on management shows that security is imperative to business success and that a top-down approach will help drive the right behavior. FURTHER READING

The types of training offered run the gamut, from new employee orientation (offered by 58% of companies) to random security audits (offered by 46%) to "live fire" hands-on labs (offered by 35%). Only about half of all companies perform training on an ongoing basis. In a rapidly changing environment, simple one-time efforts such as new employee orientation or posting security policies for review will have low efficacy.

Instead, businesses must consider comprehensive security training programs; ideally, these programs will assess the level of security awareness and will be customizable for industry and job role. Highly regulated industries already have procedures for ensuring awareness and compliance, and soon all companies will need to view security training as a cost of doing business.

As expected, the topics that companies are looking for in security training range from the basics of password management to the minutiae of threat analytics. Obviously a single training module would not cover all these areas, nor would all employees need the same level of information. But one way or another, the appropriate knowledge needs to make its way to the right people.

Topics Needed in Security Training

1. Password practices **[59%]**
2. Risk management/analysis **[57%]**
3. Types of attacks **[55%]**
4. Threat analytics **[51%]**
5. Proper response for security issues **[45%]**
6. Physical device security **[44%]**
7. Security budgets **[42%]**

Closing the security skills gap is no easy task. Companies must determine their overall security posture, ensure a solid technical foundation, and invest wisely in both highly technical measures and basic security hygiene. As time marches on, this difficult undertaking becomes more critical, as businesses find themselves in a race between building skills and being the next big security headline.

RESEARCH METHODOLOGY

This quantitative study consisted of an online survey fielded to U.S. workforce professionals during October 2016. A total of 350 businesses based in the United States participated in the survey, yielding an overall margin of sampling error proxy at 95% confidence of +/- 5.3 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

CompTIA is a member of the market research industry's Insights Association and adheres to its internationally respected Code of Standards.

ABOUT COMPTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry.

With approximately 2,000 member companies, 3,000 academic and training partners, 100,000 registered users and more than two million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

USEFUL RESOURCES

RESEARCH

CompTIA publishes 20+ studies per year, adding to an archive of more than 100 research reports, briefs, case studies, ecosystems, and more. Much of this content includes segmentations or analysis by company size, providing insights on the small business market.

CompTIA Research Library

EDUCATION & CHANNEL TRAINING

CompTIA has an extensive catalog of Quick Start Sessions, Executive Certificate Programs, Playbook Workshops, and Vender & Distributor Education. Many aspects of the training focus on sales and solutions for the SMB market.

CompTIA Training Catalog

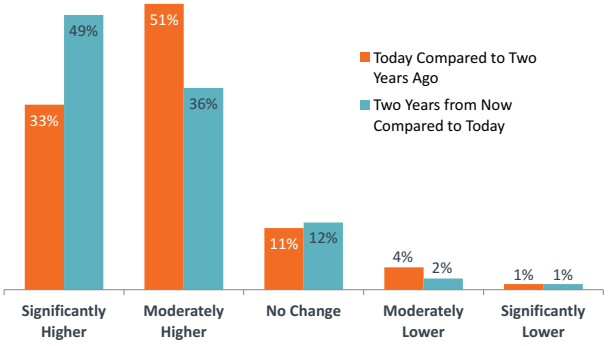
COMMUNITIES

CompTIA member communities are forums for sharing best practices, collaborative problem solving, and mentoring. Discussions frequently revolve around the SMB market.

CompTIA Communities

APPENDIX

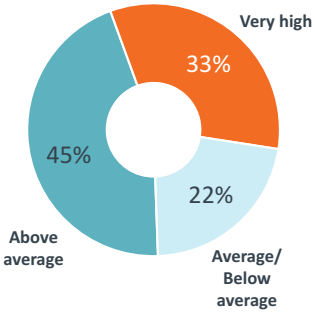
Priority of Cybersecurity Continues to Rise



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 394 U.S. workforce professionals

Many Firms Have Room to Improve Security Understanding



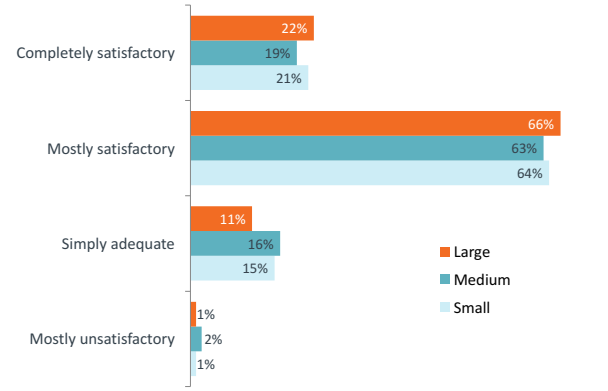
Very High/Above Average Understanding by Company Size

- Small firms: 69%
- Medium-sized firms: 81%
- Large firms: 87%

CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 399 U.S. workforce professionals

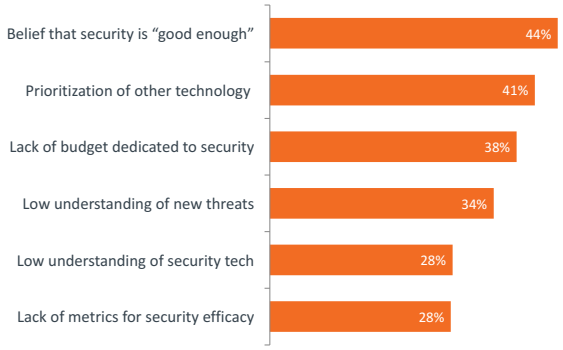
Satisfaction with Security Fairly Uniform Across Company Size



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 396 U.S. workforce professionals

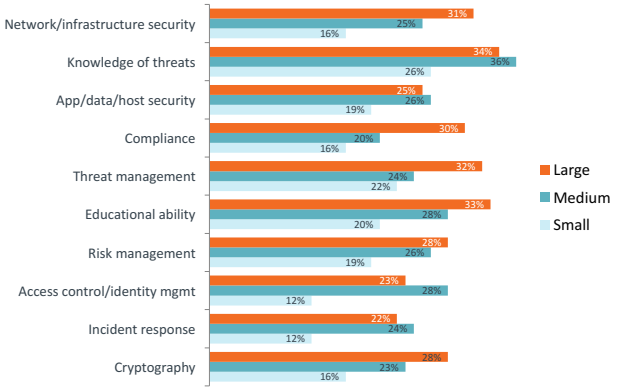
Factors Contributing to Difficulty Pursuing New Security Initiatives



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 397 U.S. workforce professionals

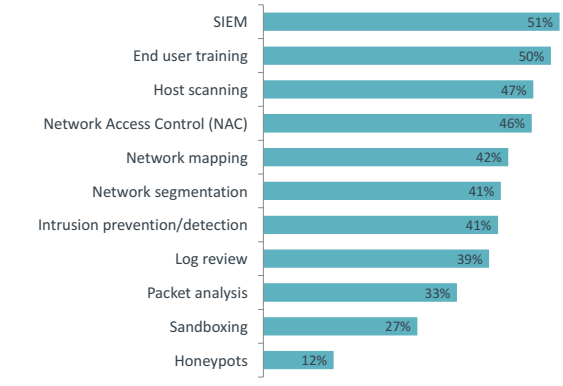
Small Firms Generally Trail Larger Firms in Desire to Improve Security Skills



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 396 U.S. workforce professionals

Security Information and Event Management (SIEM) Leads the List of Tools Used to Manage Threats



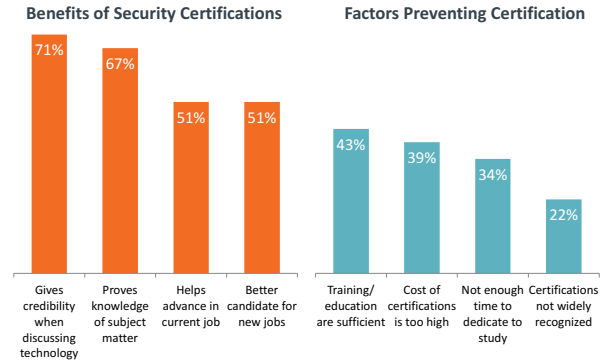
CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 395 U.S. workforce professionals

CompTIA

APPENDIX

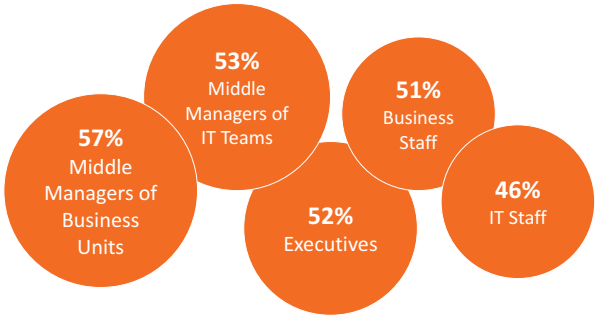
Certifications Carry Many Benefits, But There Are Also Hurdles to Consider



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 175 U.S. workforce professionals pursuing certifications
192 U.S. workforce professionals not pursuing certifications

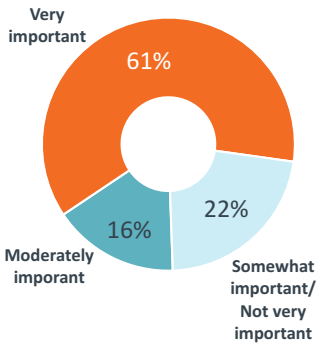
All Job Roles Are in Need of Security Training



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 397 U.S. workforce professionals

Privacy a Growing Concern within Security Efforts



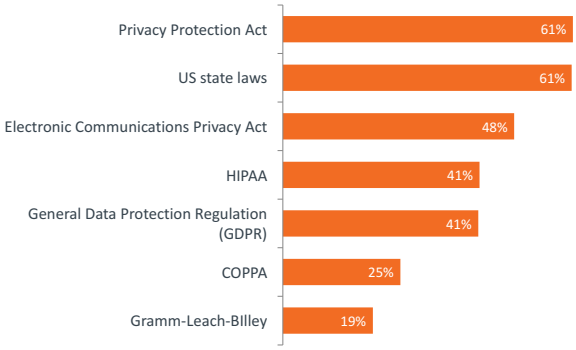
Steps Taken to Protect Privacy

- **65%** Standard security tech
- **51%** Intrusion detection
- **45%** Privacy law compliance
- **30%** NIST-based controls

CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 398 U.S. workforce professionals

Many Privacy Laws in Play for Companies to Consider



CompTIA

Source: CompTIA's *The Evolution of Security Skills* study | Base: 398 U.S. workforce professionals

CompTIA