RESEARCH REPORT

CompTIA

Practices of Security Professionals

APRIL 2016

About this Research

CompTIA's *Practices of Security Professionals* study examines the practices of channel firms focusing on security as a primary or exclusive line of business.

The study consists of three sections, which can be viewed independently or together as chapters of a comprehensive report.

Section 1: Market Overview
Section 2: Usage Patterns
Section 3: Workforce Perspectives

The data for this quantitative study was collected via an online survey conducted during February/March 2016. A total of 500 IT security professionals in the U.S. participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 4.5 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 Association (MRA) and adheres to the MRA's Code of Market Research Ethics and Standards.

SECTION 1:

Market Overview

CompTIA

Key Points

- Security is becoming the top IT priority for companies, as the recent history with new technology models and the reliance on data has brought focus to the need for tight security and privacy. Accordingly, the market is growing, with Gartner projecting overall spending on enterprise security to reach $100.3 billion globally by 2019.

- Three different movements are driving the modern security approach: the shift away from the secure perimeter, the balancing of prevention and detection, and the increased focus on proactive security activities. Businesses must combine technology, processes, and education in order to properly protect their digital assets.

- Security workforce issues are split into two parts. Core technical skills are in high demand, with BLS data showing that the number of job postings in the classification “Information Security Analysts” rose 48% between Q4 2014 and Q4 2015. Separately, companies must consider how to train the general workforce, as the average use of technology has outpaced average security literacy.

The Rise of Security

The past several years have seen dramatic shifts in enterprise technology. Companies have moved past early experiments with cloud systems to adopt a cloud-first mentality when planning infrastructure. Mobile devices have become ubiquitous, extending the personal computing platform and increasing productivity and efficiency. Digital data has grown in relevance as businesses collect data from new sources and extract new insights.

Yet for all the focus on cloud, mobility, and big data, a more traditional topic is quickly becoming the top priority in the IT industry. Cybersecurity has been a concern for businesses ever since they started building digital assets, but new technology models along with a greater reliance on that technology are driving changes in how companies approach security, resulting in a field rich with opportunity.

Each new technology model comes with its own specialized security issues. In the early days of cloud computing, security was commonly cited as a barrier to adoption. Over time, companies have resolved their concerns adequately enough to begin experimentation or migration, but this does not signal that cloud security has been solved. Cloud providers commonly take the position that they secure their infrastructure, leaving security of data and applications to the client. Clients may benefit from a cloud provider's excellent infrastructure security, but they still need to determine their desired security profile and close any gaps between the cloud provider and their ideal outcome.

Mobile security naturally started with a focus on devices as smartphones and tablets charged onto the business landscape. IT departments and solution providers had some experience with mobility thanks to laptops and Blackberry phones, but these devices were designed to be enterprise-grade. Consumer-grade devices presented brand new challenges. As companies made decisions on BYOD and MDM, they realized that devices were only the first new piece in the modern mobile ecosystem. The nature of

Sizing Security Market Segments

Market sizings are notoriously abstract, with different firms using different definitions for various markets and business conditions constantly changing estimates. For a broad field like security, sizings are especially elusive. Still, the projections give some shape to the overall market and some of the major components.

- Gartner reports that overall enterprise security spending hit $75.4 billion in 2015. They project that the market will grow at 7.4% CAGR through 2019, resulting in revenue of $100.3 billion.
- The cloud security market—meaning the application of security to assets residing in the cloud—reached $5.1 billion in 2015, according to Transparency Market Research. They call for 12.8% CAGR through 2019, resulting in revenue of $8.2 billion.
- Mobility has a stronger consumer side than cloud computing, but focusing on just enterprise mobility, MarketsandMarkets estimates that $1.97 billion was spent in 2015. They expect even more robust growth than the cloud security market will experience, with 30.7% CAGR leading to $5.8 billion in revenue by 2019.

software has changed with the app model, and there are network considerations as public Wi-Fi has proliferated and cellular networks are robust enough for productive work.

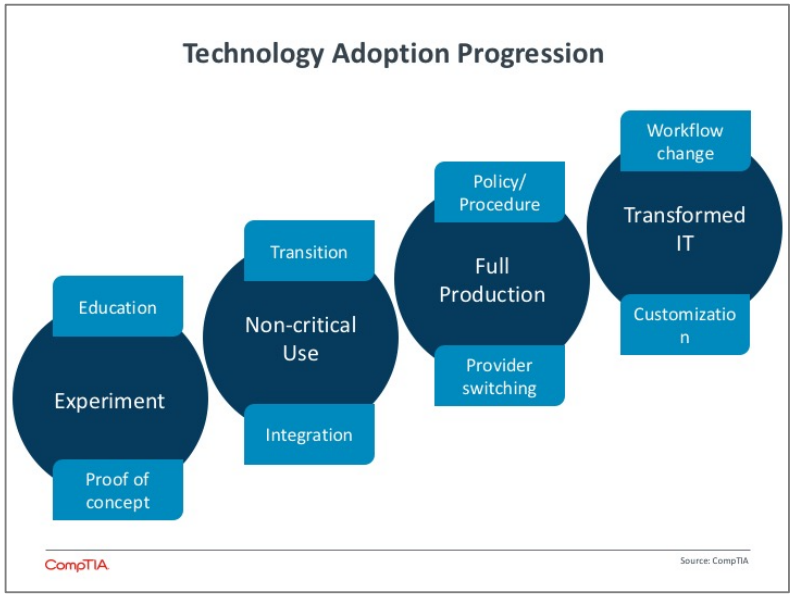
As companies transform into digital organizations, their data becomes a critical resource. Businesses are making great strides towards managing their data better and effectively using data to improve business operations. Better data security is a big part of better data handling. With data now traveling regularly outside a company's secure perimeter, the data itself needs to be monitored and analyzed. In addition, data privacy is becoming a concern separate from security as customers also try to ensure that their data is being handled appropriately.

All of these new technology trends carry security implications, and one of the huge challenges moving forward is folding these new implications into existing security practices that may require improvements of their own. The major security breaches over the past several years from Target, Home Depot, Anthem, and others have highlighted the growing importance of technology, but most of them have not involved mistakes using cutting edge models. Instead, they have been caused by failure to follow established best practices or attacks of a more traditional nature. New models will simply exacerbate the problem as criminals and bad actors learn how to exploit them. Keeping company assets safe will require a new mindset around cybersecurity.

Taking a New View

Extensive changes in IT operations, increased reliance on technology, and heightened awareness around breaches have all led to an evolution in the corporate security approach. What was once an isolated function within the IT department is now a broader initiative, driven by three primary shifts in the way companies think about building a secure posture.

First, the notion of a secure perimeter has mostly vanished. Companies may still create secure zones to hold their most prized information, but for the most part they must contend with data and applications running in cloud providers and on mobile devices. The technology adoption progression that CompTIA has defined ends with Transformed IT, where the overall infrastructure has been re-architectured to take advantage of new models. Building security into data and applications is part of this effort.



The shift away from a secure perimeter begins as a technology discussion, where standard security tools such as firewall and antivirus are supplemented with new tools such as Data Loss Prevention (DLP) and Identity and Access Management (IAM). However, the discussion quickly broadens. Businesses must add new processes, such as risk analysis, compliance management, and cloud provider evaluation. In

addition, businesses must consider how to educate end users who have become the weakest link in the chain as their technology skills outpace their security knowledge.

Unfortunately, all of these measures only lessen the chance of a breach in today's environment, not remove it altogether. The second shift, then, is towards less prevention and more detection. Leading security practitioners now place a high priority on the ability to find anomalous behavior in an application or a network and quickly resolve the situation.

Again, part of the solution is technical. One of the more robust segments of the security software market is Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS). MarketsandMarkets predicts that this field will grow at a Compound Annual Growth Rate (CAGR) of 13.2% between 2014 and 2019, placing it behind fields such as DLP (22.3%) and IAM (14.9%), but ahead of firewall (6.5%) and endpoint security (8.4%).

Looking at Layered Security

Layered security is not a new topic, but it is one that is getting more focus as a wider range of tools are being used by companies to create a secure posture. The basic notion of layered security is to combine a variety of tools and practices to catch different types of threats or to isolate different parts of a system. In a simple form, think of multiple firewalls creating different zones for network traffic to pass through, allowing for multiple levels of analysis. Most layered security implementations are significantly more complex, leading to the major challenges with the practice. A complex configuration requires a high degree of maintenance, especially in a constantly-changing field like security. Even with the proper configuration, organizations must know how to properly respond when a problem is discovered. This highlights the three-pronged approach required for modern security: technology, process, and education.

The final shift adds to the thinking that breaches are inevitable, as companies move from a defensive stance on security to an offensive strategy. In part, an offensive strategy builds on the second shift towards detection, as companies proactively audit and test their own infrastructure and security solutions in order to find possible faults. The offensive strategy also helps mitigate risk in the event a breach does occur; it will be increasingly prudent for a company to demonstrate due diligence in order to protect their reputation.

Clearly, security is no longer a discipline confined within a single department. Businesses still look to the IT function to direct overall security activities, but those activities involve discussions and processes that happen throughout the organization. In order to successfully implement a new security approach, companies must consider the skills that they need to build or bring in.

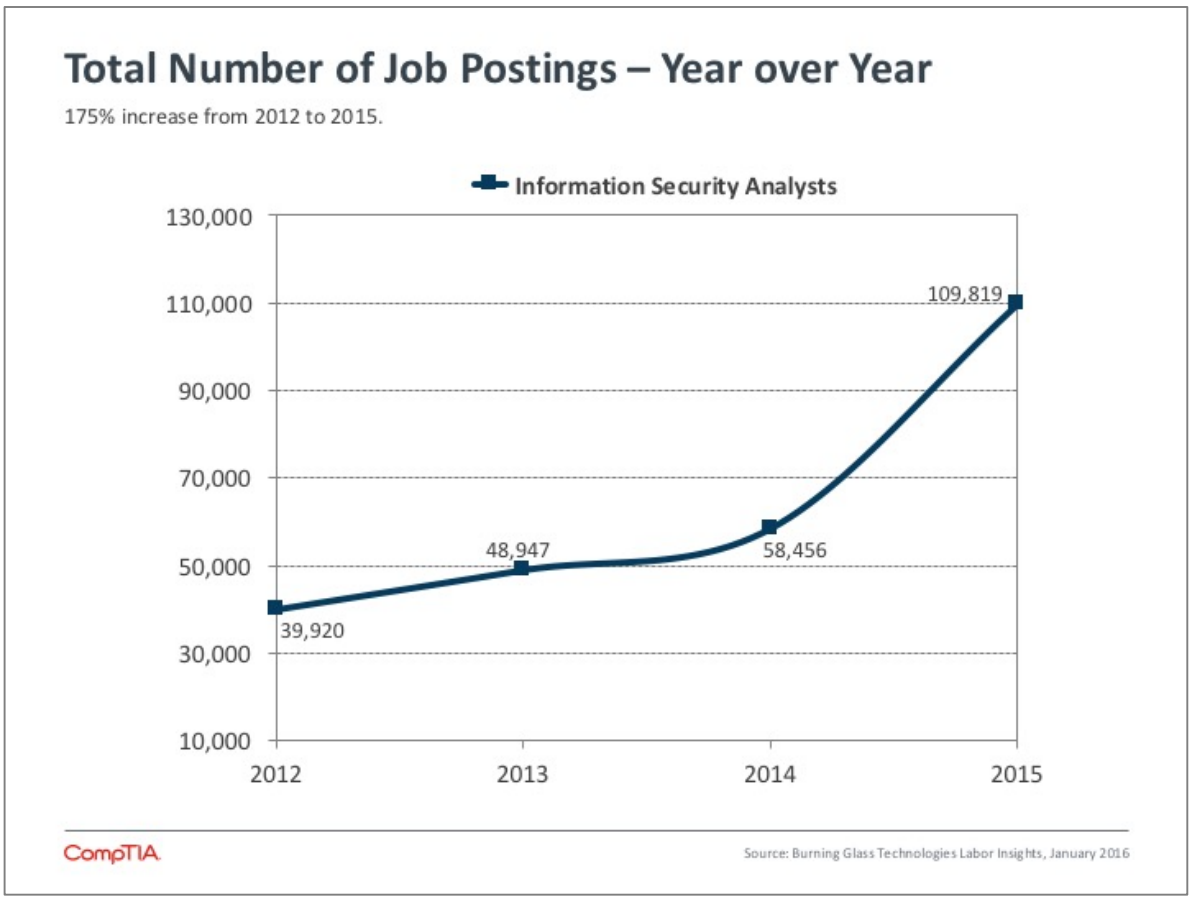
Workforce Issues

The wide array of technical skills needed for security and the difficult task of educating the general workforce both contribute to a complex picture for companies trying to build a security team. Adding to the complexity, companies have different approaches to the IT function, using a mix of internal resources and third party expertise.

At the top end of the scale, security is becoming its own function. Many large corporations are creating the role of Chief Information Security Officer (CISO) or Chief Security Officer (CSO), and some companies have explored organizational restructuring with these roles. In some cases, the CISO continues to report to the CIO (or possibly the COO). Other companies have the CISO report directly to the CEO, giving broader organizational reach and integration. Booz Allen has actually taken this a step further and reversed the traditional arrangement so that the CIO reports to the CISO. With its recent cybersecurity budget including a provision for a federal CISO, the U.S. government is one of the highest profile organizations to demonstrate the need for a specific security focus.

At the other end of the scale, companies with no formal IT function have major challenges in bringing dedicated security skills on-board. As they commonly use outside firms for IT activities, they will naturally turn to these firms for security activities as well. The IT channel has seen a rise in managed security service providers (MSSPs), where the entire portfolio of products and services is built around security. Of course, working with such a firm adds to the list of partners a company must employ, but the complexity of security and of IT overall is making a jack-of-all-trades partner a difficult proposition.

The net effect of all this churn is a rapidly increasing demand for security skills. According to BLS data from January 2016, the number of job postings in the classification "Information Security Analysts" rose 48% between Q4 2014 and Q4 2015. This was the second-highest rate of growth across all BLS IT classifications, trailing only "Computer & Information Research Scientists."



Job postings are a proxy for true job demand, given that hiring firms may change their plans, post multiple times for the same job, hire internally, or try different approaches to find the right candidate. The strong growth in the Information Security Analysts category matches with anecdotal evidence that companies are seeking a variety of technical skills, from firewall administration to intrusion detection to the use of data analytics to target potential security threats.

Beyond security-specific roles, companies are expecting security to be a larger part of general technical positions along with non-technical functions. CompTIA's Security+ certification also experienced growth of 18% between Q4 2014 and Q4 2015. While this certification is often used as the first step towards an InfoSec career, the vendor-neutral approach provides a solid foundation in security for professionals pursuing paths such as cloud architecture or data science.

For the general workforce, companies are exploring ways to raise security literacy and mitigate the risk of human error. Educational offerings delivered via an online classroom are a good first step and hold the potential to factor into the cost of cyberinsurance. Going further, some companies are using more novel approaches such as simulated phishing attacks or gamification to measure and improve awareness.

Security is on the rise, but not because companies are suddenly recognizing the importance of protecting their assets. Businesses with serious IT investments have always viewed security as a high priority, but the stakes are now higher. With the changes happening in enterprise technology, digital organizations have a lower tolerance for data breaches or infrastructure attacks. With the changing motivations of cybercriminals, companies of all sizes must be more vigilant about their data and the data of their customers. Both IT departments and solutions providers will need to build new tools, skills, and behaviors as they maintain corporate security in the modern technology era.

SECTION 2:

Usage Patterns

CompTIA

Key Points

- Although digital organizations have many different business units contributing to technology decisions, overall security is still seen as a primary function of the IT department. Less than half of all IT security professionals view the security at their company as “completely satisfactory,” suggesting a range of improvements that must be communicated to other business stakeholders.

- Companies have typically viewed security as a high priority, but there is a recent push towards taking new action to shore up defenses. The primary driver for a new security approach is a change in IT operations, but even here there are signs of hesitation—only 51% of IT pros cite this as a driver, far less than the number of companies currently adopting cloud and mobility strategies.

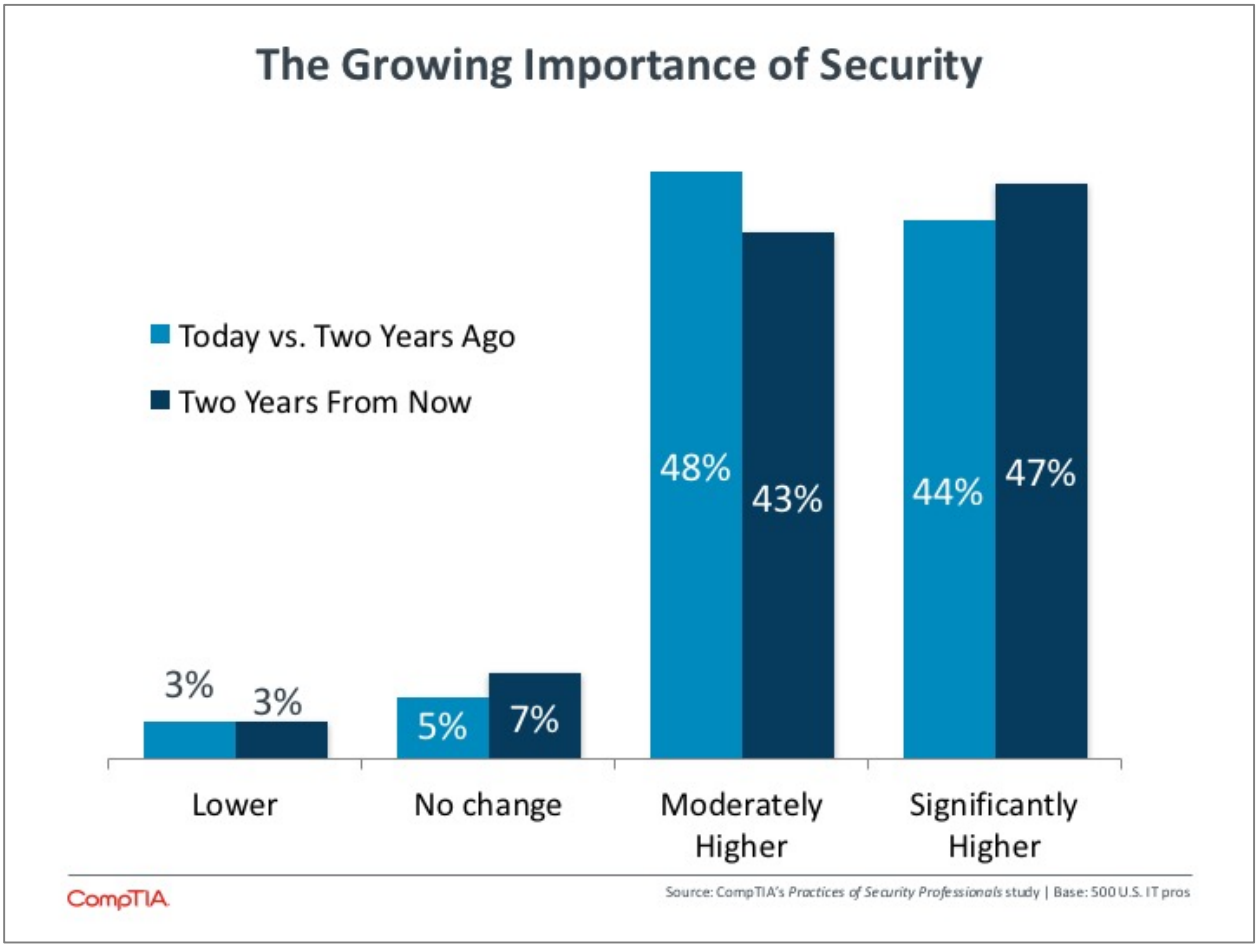
- One of the main challenges when pursuing new security initiatives is the belief that current security is “good enough,” cited by 47% of IT security pros. While this may be the reality for some companies with aggressive security approaches, education on modern security is a priority. Other challenges include prioritization of other technology investments and the lack of metrics around cybersecurity.

Security in Digital Organizations

The nature of enterprise technology is changing drastically. Cloud computing and mobile devices have ushered in a new era, where corporate behaviors and processes are shifting to take advantage of new technology models. IT departments are discovering new roles and responsibilities, overseeing decisions made by business units and taking ownership of specific subjects that utilize specific skills.

CompTIA's *Building Digital Organizations* study found that one of the primary areas of ownership for the IT team is security. While business units today want to share responsibility in many parts of technology planning, they expect the IT department to take the lead when it comes to securing the company's digital assets.

By making this statement, business units are not simply relegating an onerous task to their technical counterparts. As companies use technology more strategically and become more reliant on data, security is a critical factor for ongoing operations. The main factor throwing the brakes on the rogue IT movement is the fact that non-IT departments are highly likely to introduce weaknesses when choosing their own solutions.

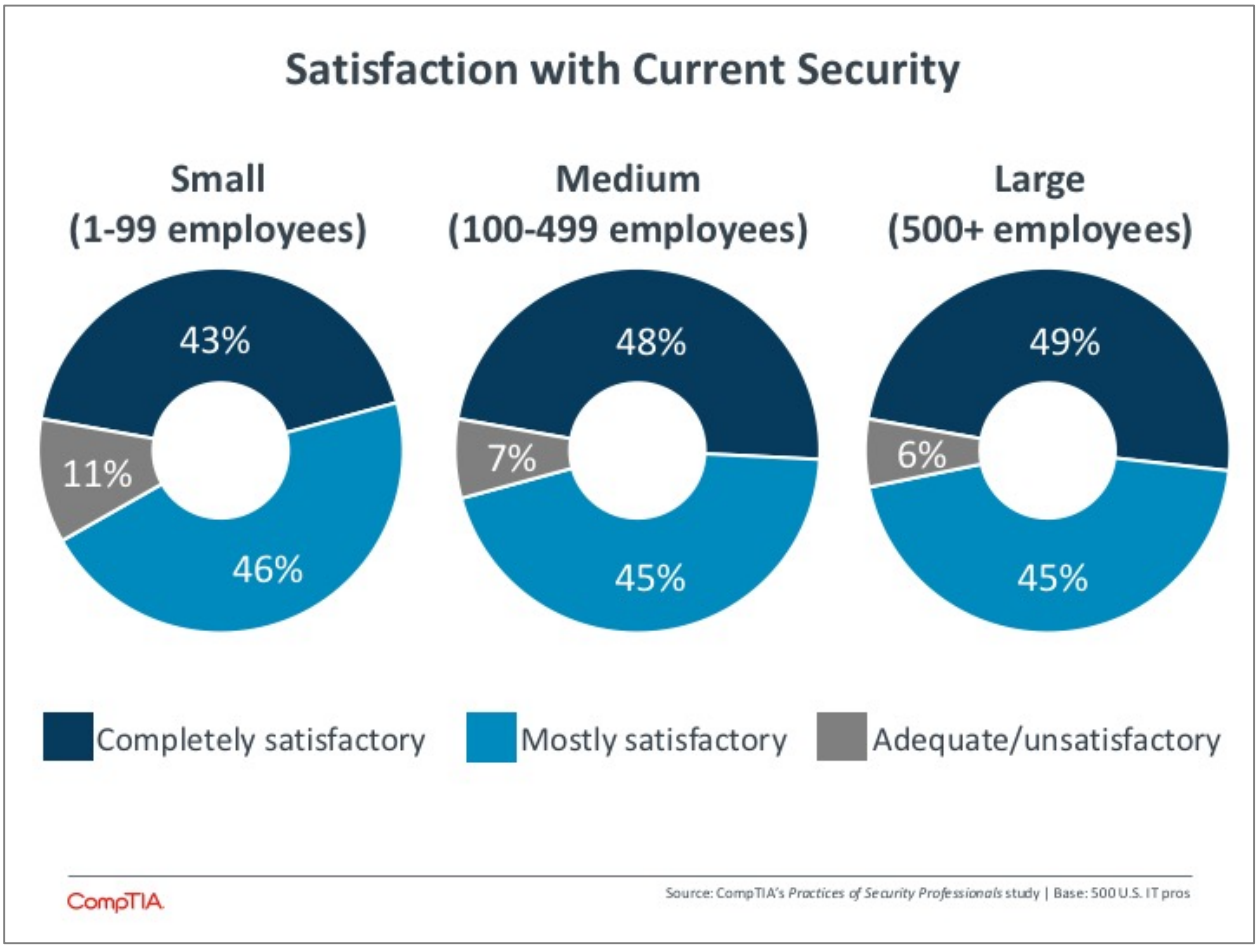


Given the critical nature of cybersecurity and the movement towards IT ownership, it is no surprise to see that IT security professionals see a rising prioritization of the topic within their companies.

Compared to CompTIA's data from 2015, the importance of security continues to trend upward. Previously, 34% of all business professionals and 32% of IT professionals felt that security held a significantly higher priority today compared to two years ago. Those numbers went up to 41% of both business and IT professionals when estimating the priority of security two years from now.

However, CompTIA's research has also found that simply placing a high priority on security may not lead to improved measures. Companies may not fully understand the nature of modern threats, the need to support technology with process and education, or the necessity of proactively monitoring events along with building strong defenses.

This is the challenge of the IT security professional: to apply rapidly changing protective measures in a business environment growing accustomed to speed and ease of use. Increased technical literacy and highly capable consumer products have changed expectations for the use of technology, and enterprise-grade security suffers from both a lack of understanding and a perception of red tape. InfoSec pros must close the perception gap while exploring new tools and methods.



At the most basic level, many IT security practitioners report less than complete satisfaction with the current state of their company's security. Large companies, with the most resources to devote to the problem, are slightly more likely to have adequate security in the eyes of the professionals. Although satisfaction has increased from previous years, there still remains a wide swath of companies that could

improve their standing—not to mention those companies where "completely satisfactory" may be a bit of an overstatement.

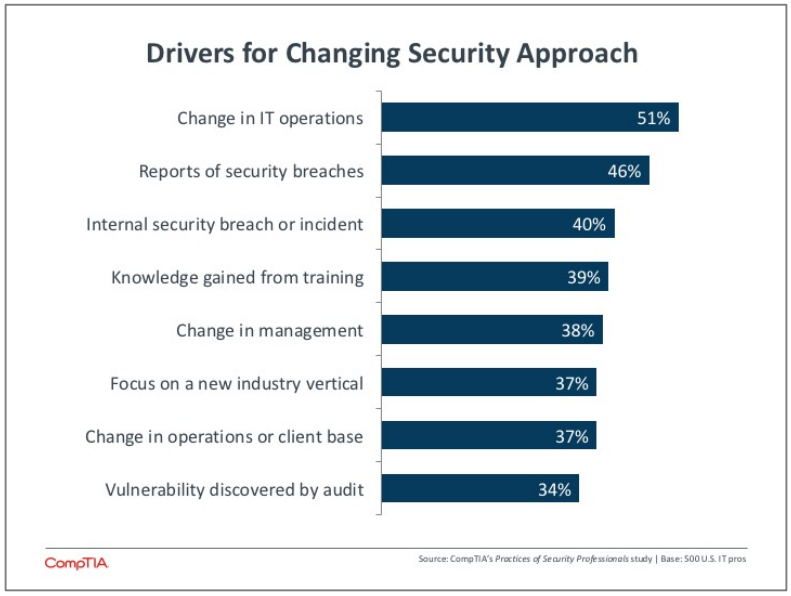
Closing the perception gap and improving security usually starts with education. The data suggests a strong correlation between satisfaction with security and understanding of the field. Overall, 46% of InfoSec pros feel that their company's security is completely satisfactory, and 54% believe that there is a very high understanding of the topic. The remaining respondents feel that there is room for improvement in awareness of issues, willingness to spend, or sensitivity among the general workforce.

Security knowledge is especially important among the smallest businesses. Approximately six out of ten workers at medium-sized or large companies feel that their company has a very high level of security understanding, but this drops to 46% at small firms. Historically, small firms have been somewhat lax with security, assuming that their data is not valuable to hackers. With today's cybercriminals being motivated by many different factors, though, attacks are just as likely to seek out poor defenses as they are valuable information.

Building a New Approach

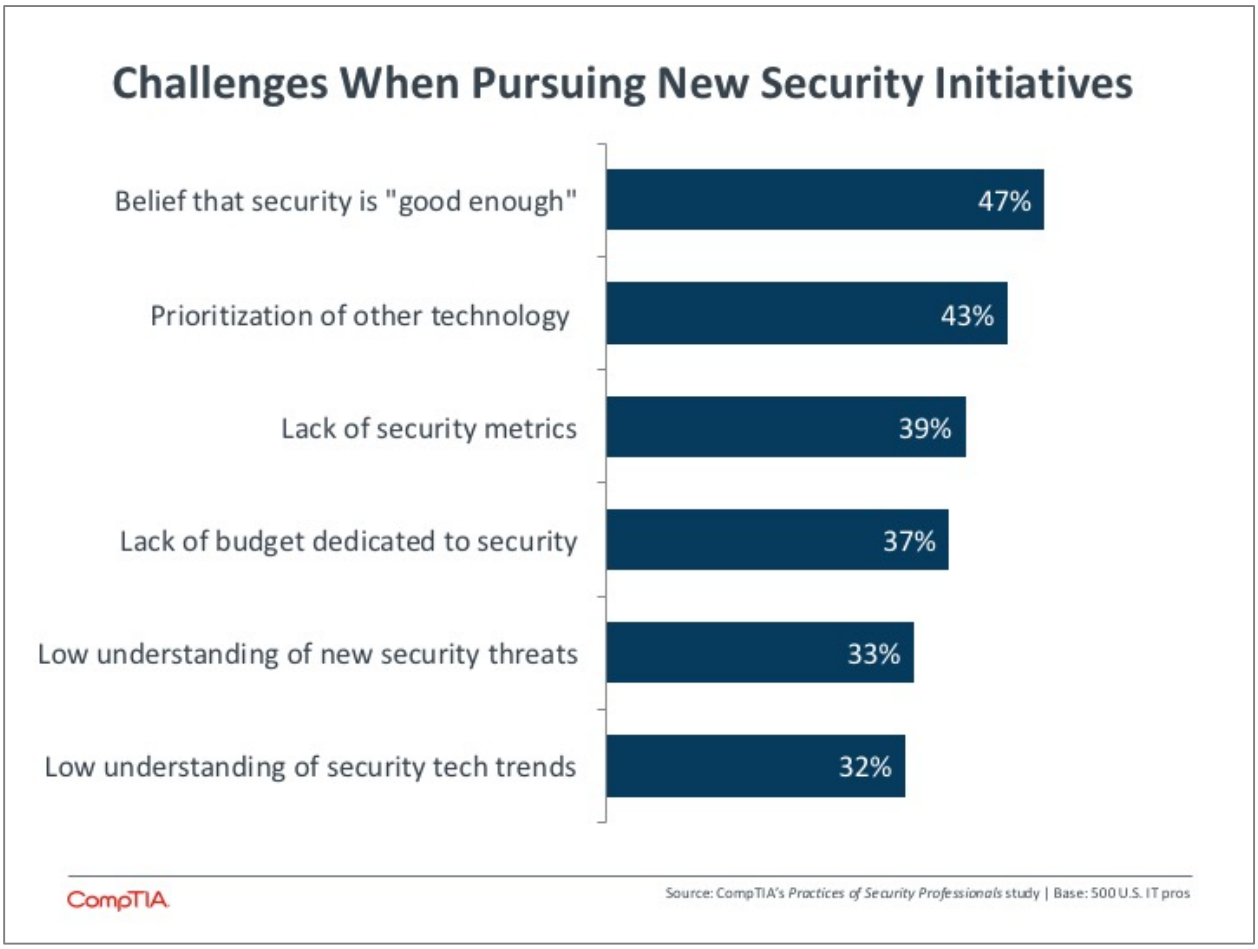
After companies get a handle on the different facets of modern security, it is time to take action. Since simply acknowledging security as a high priority does not lead to changed behavior, there needs to be a different starting point. For many companies, that start is a change in IT operations.

Consistent with previous research, IT pros in this study cite changing operations as the primary driver for a change in their security scheme. Most technology strategies are shifting today thanks to cloud and mobility, and that actually highlights the disconnect when it comes to the mindset around cybersecurity. Far more than 51% of companies have adopted cloud computing and mobile devices, suggesting that many companies are changing their operations without corresponding activities to build the proper defenses.



New knowledge that comes as a result of training is also a primary driver for a new approach, and this shows how outside training or certification can play a critical role in supplementing work experience. On-the-job activities are likely to be driven by existing knowledge. The dynamic nature of attacks can consume the bandwidth of a security professional, especially if security is just a portion of overall responsibilities (only 36% say that security is their sole focus). Third-party education is important for describing new problems on the horizon and best practices.

Third parties can also be instrumental in helping companies establish a security baseline. Building on the theme of employees feeling satisfied with their current setup, the main hurdle faced in pursuing new initiatives is the believe that existing security is “good enough.” One of the common issues in security is the difficulty in determining effectiveness; it is challenging to tell if a lack of events is due to good defense or happy coincidence. Comparing existing tactics to top performers or examining those tactics against current operations can expose weaknesses and suggest new approaches.



The lack of dedicated budget is not the top challenge for new security measures, but it definitely factors into the discussion. Budget challenges come in different forms. Sixty-one percent of IT pros in the study said that the security budget is completely within the IT function, but technology budgets are spread across business units, driving skewed views of the total cost of technology. Fifty-four percent said that security budget is typically allocated to specific technologies, such as firewall or antivirus, based on long-held beliefs about which products are needed for security. Finally, the budget may not account for ongoing training, either for the IT team or the general workforce.

Whether due to budget or due to lack of awareness about available tools, there is a definite adoption curve across the different technical pieces that are being used to build comprehensive solutions. As expected, firewall and antivirus lead the pack—nearly all companies have some form of these technologies installed. Encryption is also very popular, especially email encryption. Several tools are in the middle of the curve, including Data Loss Prevention (DLP), Identity and Access Management (IAM),

and Intrusion Prevention Systems/Intrusion Detection Systems (IPS/IDS). At the tail end is Security Information and Event Monitoring (SIEM), which collects events and information from the layers created by other tools and helps guide the proper response. It's no surprise that SIEM has the lowest adoption, given that effective usage relies on a comprehensive understanding of the security environment and on corporate policies around behavior.

Beyond specific technologies, there are security practices that involve processes or operational tasks. There is an adoption curve here as well. A process like Business Continuity/Disaster Recovery (BC/DR) is a natural progression of standard data backup, so most companies have some form of this in place. Fewer companies ensure that they are up to speed on the regulatory environment or the education they are delivering to their workforce. Fewer still are taking proactive steps in validating their security, whether that be through external audits or simulated attacks.

As the IT team takes the lead in driving security for the organization, they will have to account for new organizational dynamics around the way that technology is integrated. Ultimately, the implementation of security needs to follow the rationale for any technology: advancing the needs of the business. IT pros will need to adequately communicate the requirements for modern security, the potential cost of weak defenses, and the specific actions that should be taken.

SECTION 3:

Workforce Dynamics

CompTIA

Key Points

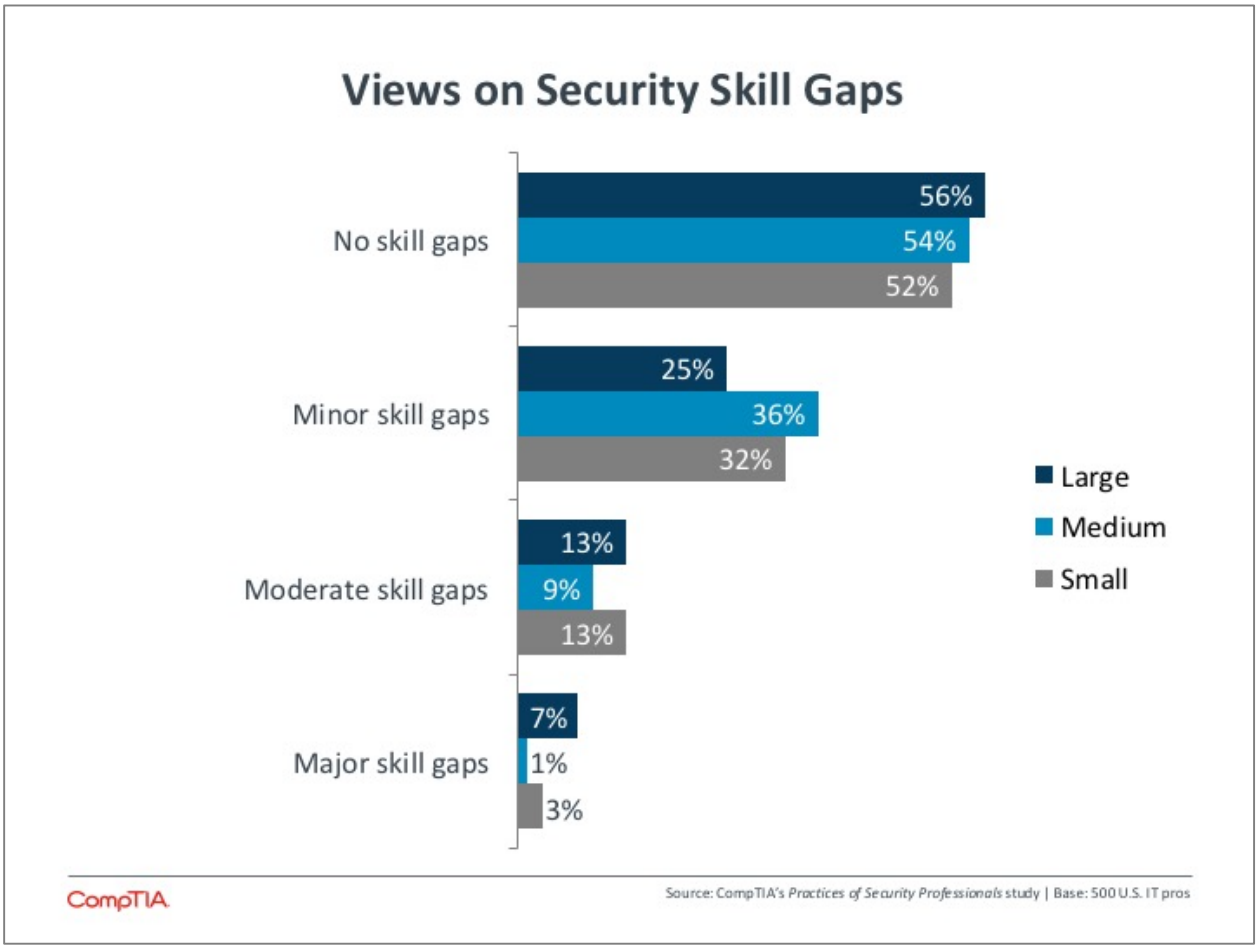
- Nearly half of all IT security professionals believe there is some degree of skill gap within their organization. Fifty-three percent of companies with gaps want to be more informed about current threats, followed by desired improvement in current security technology and awareness of the regulatory environment.

- Although there has been a dramatic uptick in security job postings, hiring is actually the least common method for closing skill gaps, with 31% of companies hiring new skills. Four out of ten businesses are pursuing partnering with outside firms, and the primary method for closing gaps is training and certification.

- Seventy-one percent of IT pros in the CompTIA survey feel that the workforce at their company has an advanced security mindset, but this sentiment may be inflated due to a focus on policy awareness rather than behavior or a consideration of technical staff rather than general staff. Previous CompTIA research suggests that poor workforce security practices are a prime factor in breaches, so companies should examine metrics for measuring the workforce and explore training that will improve the situation.

Closing the Skill Gap

As section 1 described, the number of job postings in the area of IT security skyrocketed in 2015. According to BLS data from January 2016, the number of job postings in the classification "Information Security Analysts" rose 48% between Q4 2014 and Q4 2015. Looking back to 2012, there has been a 175% increase in these types of postings. Considering the market signals that show an intensifying focus on security, this trend is likely to continue.



The number of new postings tracks with the sentiment of IT security pros as they examine potential skill gaps in the organization. It is worth noting that large enterprises are the most likely to say there are no skill gaps, but they are also most likely to feel that existing gaps are sizable. Although these companies have resources to apply to the security problem, the complexity of security still creates demand for unique skills that need to be developed in the marketplace.

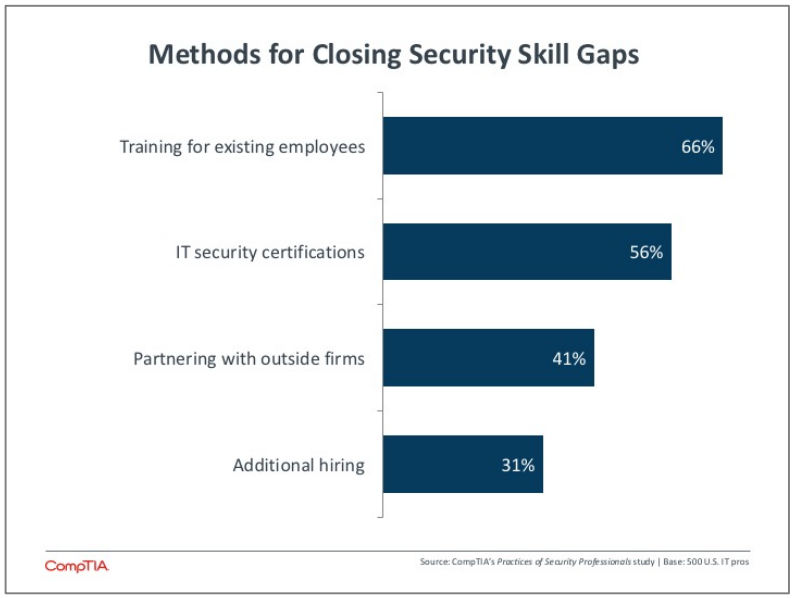
It is also interesting to note that there is little difference between those IT pros in a management position and those working at a staff level. Slightly more than half of both groups feel there are no skill gaps, and the largest difference is around moderate skill gaps, where 19% of management feel gaps exist, compared to 10% of IT staff.

This similarity in opinion suggests a certain organizational mindset. Staff employees, who are closest to the day-to-day operations, can see where the risk is highest due to a lack of coverage or the absence of the proper skills. This situation has been adequately communicated to managers, who hold a greater responsibility for the well-being of the company. Agreement on skill gaps implies that management feels that the investment is worthwhile, and this message must be further communicated to upper-level decision makers at the business.

In general, the appropriate level of security spending is one of the biggest unknowns for businesses today. Any increases in technology spending are likely directed towards solutions that will produce tangible results for the company, and security may be viewed more as a cost that should be contained. While businesses may have accepted a certain level of security cost, this level must be examined as technology usage increases and reliance on digital data creates a higher degree of risk.

The need for additional spending is further proven by the tight grouping of areas where InfoSec pros feel that gaps exist. Four out of ten companies with skill gaps feel that they need to improve their awareness of the regulatory environment, and slightly more than that feel that they should get better at educating end users or more knowledgeable about current security technology. At the top of the list, 53% of companies with gaps want to be more informed about current threats, a topic that is especially pertinent as businesses pursue new technology models.

So how are companies addressing their need for security skills? Hiring is actually the least common approach. Predictably, this strategy is seen most at large companies (39%), followed by medium-sized companies (33%) and small firms (24%). Since the steep increase in security job postings is tied to hiring activity, the other approaches have likely experienced dramatic changes as well.



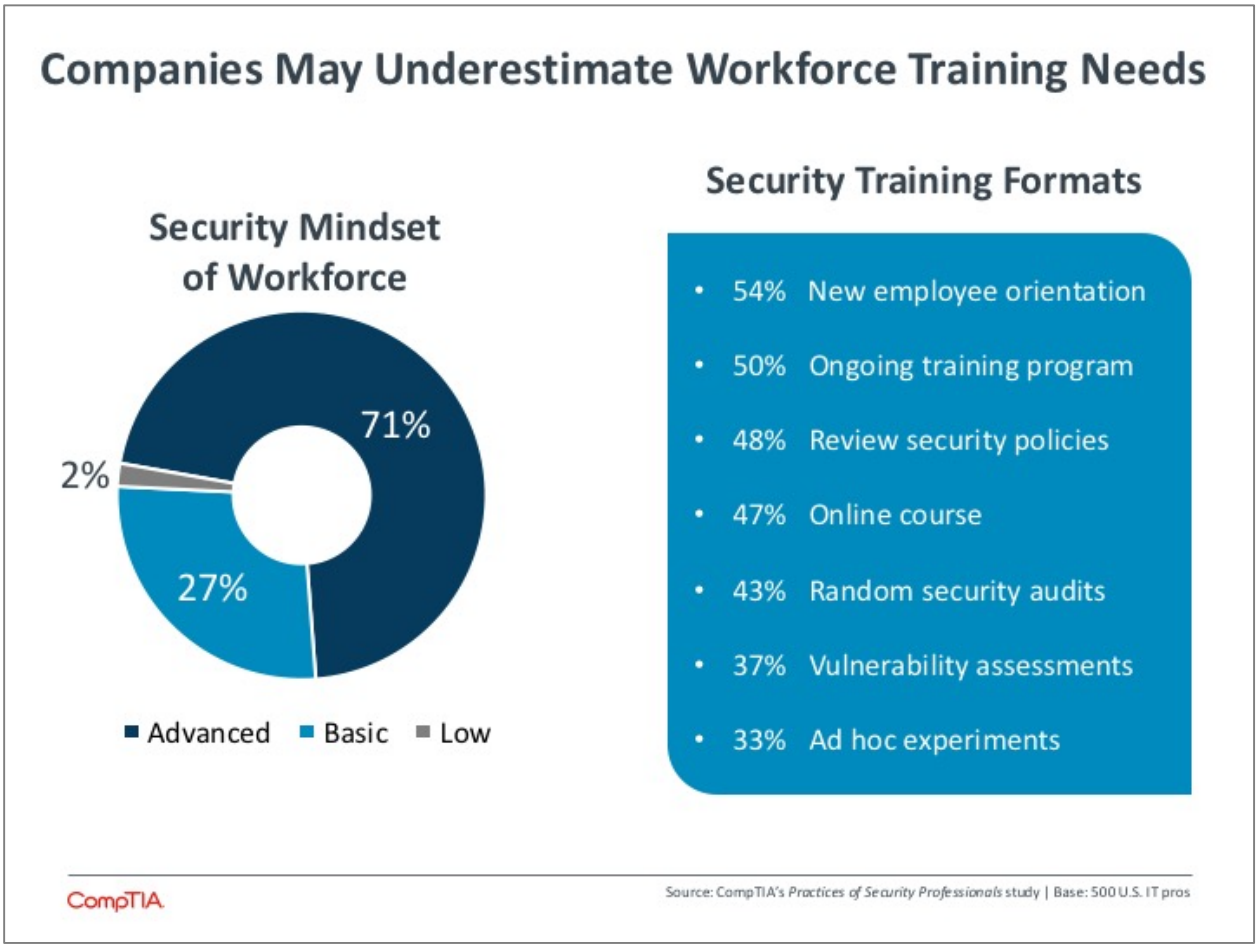
Growing interest in third parties has spurred activity in the IT channel. There is movement towards security offerings by IT firms, including an increase in the number of firms that specialize in security as Managed Security Services Providers (MSSPs). The offerings and practices of these security-focused firms are examined in depth in CompTIA's *Security in the IT Channel* study.

Training and certification are the primary means for closing skill gaps, and these two activities go hand in hand. Obviously, training alone can go a long way in developing skills—52% of those IT pros that have not pursued certifications say that training and education are sufficient for the time being. Cost is also a factor. Forty percent of IT pros that have not pursued certifications say the cost is too high, and training can be done at a lower price point.

However, the benefits of certification still appeal to a significant number of security professionals. The top benefit—cited by 73% of workers that have pursued certifications—is the level of credibility that comes with a certification. Especially as discussions around security take place with business units across the organization, this credibility can help add weight to arguments for security considerations in a fast-paced environment. Other benefits include the potential to help someone advance in the current job (57%) or improve candidacy for a new position (56%).

Building Workforce Literacy

Technical staff may need specialized training, but there is a growing need for the overall workforce to improve their knowledge and awareness of security issues. Thanks to cloud computing and mobile devices, the increased use of technology throughout an organization allows for new capabilities and greater productivity; it also creates new vulnerabilities as workers may be procuring or using tools without fully understanding the security implications.



Generally, IT pros in the CompTIA survey tend to view the workforce at their company as having a solid grasp on security. Small firms are the most likely to show some reservation, with just 65% claiming an advanced security mindset across their workforce compared to approximately three quarters of medium-sized or large companies.

This assessment, though, is at odds with findings from previous CompTIA research. In other security studies, companies have reported that the primary factor in breaches is human error. This has been a consistent trend over the past several years. Furthermore, companies in recent years have been able to describe in more detail the type of human error that is causing problems. Rather than simply stating that there is a general failure to follow policies and procedure, businesses are pointing to low awareness of new threats and lack of expertise with new technology.

There could be several reasons that IT pros in this study reported a more advanced security mindset within their organizations. For starters, the different mindset descriptions in the survey focus on policy. A more general business audience may broadly interpret this term to include official corporate policy as well as general technology aptitude. Technical employees may be more likely to think only of the official policy, withholding viewpoints on technical skills.

IT pros also may have assumed that the question referred more to the technical team rather than the overall workforce. With the entire survey focused on InfoSec professionals, it is reasonable to assume that some respondents assessed the security mindset of their departmental colleagues, where a more advanced security mindset would be more likely.

In reality, CompTIA's prior data along with many anecdotes from within the industry would suggest that the average employee today lacks knowledge of security concepts that can protect both their own identity and their company's interests. One of the things that makes a workforce assessment so difficult is the lack of good metrics for determining security literacy.

These metrics will go hand in hand with workforce training. The level of adoption and range of formats used for security training today do not imply that companies are aggressively addressing overall improvements in workforce understanding. As businesses begin taking more action in enhancing their security posture and exploring new risk mitigations such as cyberinsurance, evaluation and training will become more important.

IT pros today who focus on security must consider how to address this need as they also implement new technologies and establish new processes. By building expertise across all areas of modern security and connecting new initiatives to business objectives, security professionals can establish clear roles for themselves as their companies transform into digital organizations.