RESEARCH REPORT

Cybersecurity for Digital Operations

Provided Courtesy of

MJ SHOER, LLC
www.mjshoer.com

CompTIA

RESEARCH REPORT

CYBERSECURITY FOR DIGITAL OPERATIONS

September 2019

As the technology industry enters a new phase of maturity, there are more and more questions around the implications of emerging trends operating at global scale. Aside from societal repercussions, an extreme reliance on digital data and the extensive collection of personal information are highlighting the critical nature of cybersecurity and privacy. This report examines the general state of security within business today, exploring the hurdles that are preventing companies from an ideal security posture and suggesting the steps that can lead to improved security in the digital economy.

KEY POINTS

Cybersecurity is evolving into a distinct practice

Although the number of companies that report complete satisfaction with their security posture is rising (45% in 2019 compared to 21% in 2017), the majority of companies still see room for improvement. Dramatic changes in technology mean that a new cybersecurity approach goes beyond a checklist of new techniques. Instead, businesses are shifting to a dedicated practice around cybersecurity, whether that function is performed by internal staff, external partners, or a combination of both.

Understanding tradeoffs will improve prioritization

When it comes to balancing cybersecurity and technology innovation, companies are trying to get the best of both worlds. This is especially true among executives and business staff. IT staff are more likely to recognize that tradeoffs exist, and it is increasingly the responsibility of technology professionals to educate the organization on those tradeoffs in terms of business impact. A change in IT operations is still the leading driver for a new security approach (cited by 57% of companies), and security should be a primary component in describing the total cost of new adoption.

Skills are the most critical part of the security function

There are two different areas companies must consider when addressing security skills. First is the general workforce. Only 44% of companies feel that their business staff have an ideal level of security expertise. Training is provided at 77% of the firms with skill gaps, but that training is only viewed as extremely effective 45% of the time. The second area to consider is the skills of technology professionals. Deeper skills are obviously needed here, and most companies are using training, partnering, or certifications to build modern security skills.

Security metrics are still in early stages

Measuring cybersecurity progress is still a new concept for many companies, especially as IT and security shift from tactical activities to strategic initiatives. Small companies are the most likely to report a heavy use of metrics for security, probably due to the fact that these firms are the most likely to use a third party that provides metrics around their services. As businesses invest more in developing a dedicated security center of operations, they will need to agree on the best metrics to use for tracking and also set a plan for reviewing these metrics at the appropriate levels of the organization.

MARKET OVERVIEW

The field of cybersecurity continues to be one of the hottest topics in all of technology. Emerging trends draw the most headlines, and established models provide the bulk of support for business operations, but cybersecurity is the constant that draws the two sides together and demands ever-evolving techniques.

Recent CompTIA research in the field of cybersecurity has focused on the skills that companies are looking for or the way that they construct their security teams. In 2019, as another decade draws to a close, it is worthwhile to take a step back and take a broad look at the overall state of corporate security.

To start, consider the drastic ways that the business and technological landscapes have changed over the past 10 years. In 2010, there was no concept of a megabreach. The Target hack that many consider the first modern megabreach would not occur for another three years. Social platforms were just beginning their meteoric rise. Facebook hit 608 million users, compared to just 360 million in 2009 and 145 million in 2008. Twitter was at an even earlier stage of growth, with just over 50 million users in 2010. The platform for social engineering was just becoming viable for cybercriminals.

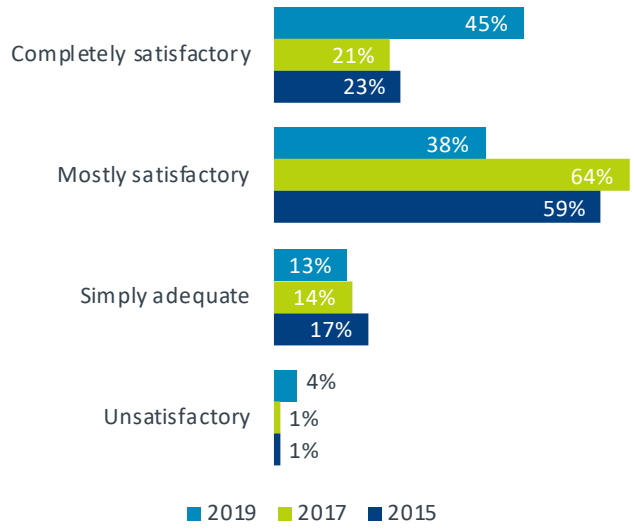
Clearly, the threat to business operations, not to mention the threat to public and private safety, has never been higher. At the same time, the appetite for experimenting with and implementing new technology has never been higher either. In 2010, there were two main technology trends that companies were exploring: cloud computing and mobility. These technologies (cloud computing in particular) have now led to a much longer list of topics that businesses are pursuing. Internet of things, artificial intelligence, blockchain, and augmented reality are just a few of the trends that promise new business possibility but also create new security complications.

Given these dynamics, it is no surprise that security continues to show strong growth for the next several years. IDC predicts that global spending on security will hit $103.1 billion in 2019, then grow at a compound annual growth rate of 9.2% through 2022, eventually reaching $133.8 billion. This growth is indicative of cybersecurity's role in both established and emerging technologies. Established technologies, along with the corresponding security techniques, are expected to grow at a fairly slow rate thanks to the sizable install base. Emerging technologies, which require new security methods, will experience more explosive growth.

IDC further breaks down security spending into several buckets. The largest in 2019 is the amount spent on managed security services. CompTIA's latest data sheds light on some of the drivers for this spending, which will be discussed throughout this report. The second largest category of security spending according to IDC is network security hardware, which falls into the more traditional realm of firewalls and threat management. Rounding out the top four are integration services (growing more critical as emerging technologies are adopted) and endpoint security (another traditional category that is evolving with mobile devices and IoT).

The primary takeaway from the history of the past several years and the projections for the next several years is that cybersecurity is not a field where there is a well-defined new approach that companies must adopt. Instead, cybersecurity is a moving target. There may be new elements that companies must now consider, but the plan must be ongoing and flexible.

Satisfaction with current cybersecurity



While there was a significant increase in the number of companies rating their current security as "completely satisfactory" after several years of treading water, that number is still less than half of all companies surveyed. Given the high priority that companies claim to place on cybersecurity, one would expect to see a greater number of companies satisfied with their efforts.

To make matters worse, the aggregate numbers might paint an optimistic picture. When looking at job role, 55% of executives believe their current security is completely satisfactory, and 61% of business staff assign the same rating. However, among IT staff—those employees that best understand the risks inherent in the security architecture—the number drops to 35%.

The typical prescription for modern cybersecurity has been to expand beyond a pure technology approach into process initiatives and workforce education. The lack of satisfaction with current security efforts suggests that further transformation is needed. The complexity and speed of security require a deep level of dedication and constant management; to achieve these things, companies must be willing to consider the level of investment they have in this critical area.

CORPORATE VIEWS ON CYBERSECURITY

One of the things that makes cybersecurity initiatives so difficult is the tension that exists. There is tension between tight cybersecurity and convenience for end users, and there is tension between robust cybersecurity and aggressive technology adoption for the organization. The early days of cloud computing helped shed light on the latter type of tension and also highlighted the need for a modern approach to cybersecurity. Many companies leapt into cloud projects without fully appreciating how an old secure perimeter mindset did not translate to the new model. Over time, cloud security became a much lower barrier to adoption as companies discovered best practices, and there has generally been a greater appreciation for security issues with subsequent technology trends.

The tension can still be seen when asking companies how they handle cybersecurity and tech innovation. A balanced approach seems to be the most common, with 48% of companies saying they try to balance these two areas. The importance of cybersecurity can be seen in the 40% of companies that prioritize cybersecurity above technology innovation. Finally, the desire to be on the cutting edge of technology is clearly strong, with 35% of companies prioritizing innovation above cybersecurity.

The issue, of course, is that respondents clearly chose multiple selections from a group that should be mutually exclusive. The survey was intentionally designed to determine how much confusion there is around tradeoffs between technology pursuits and security needs, and a degree of confusion clearly exists. It makes sense that executives and business staff take more of an "all of the above" approach, as they are still learning about these tradeoffs. IT staff are much more likely to realize that breaking new ground can also mean breaking business operations.

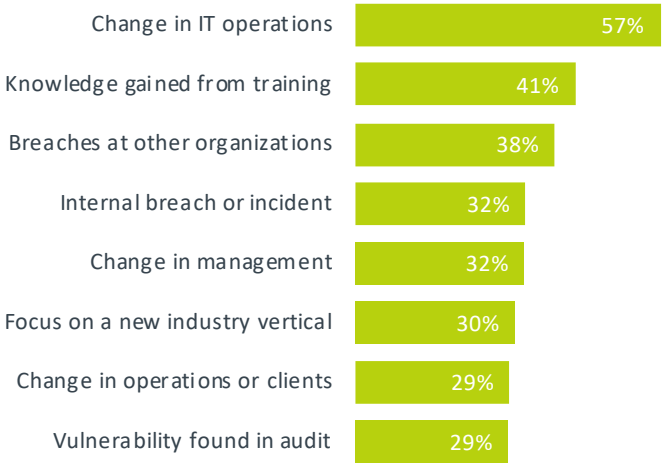
Approach to technology innovation and security

	Executives	Business Staff	IT Staff
Prioritize innovation above security	39%	46%	29%
Prioritize security above innovation	47%	43%	35%
Balance security and innovation	50%	49%	45%
Total	136%	138%	109%

Although there has been significant progress in understanding cybersecurity issues over the past few years, there is still room for improvement, especially among those employees without a strong technology background. Executives and business staff tend to feel that there is strong understanding of cybersecurity within the company, with 91% of both groups rating the level of understanding as "very high" or "above average." However, only 78% of IT staff feel the same way.

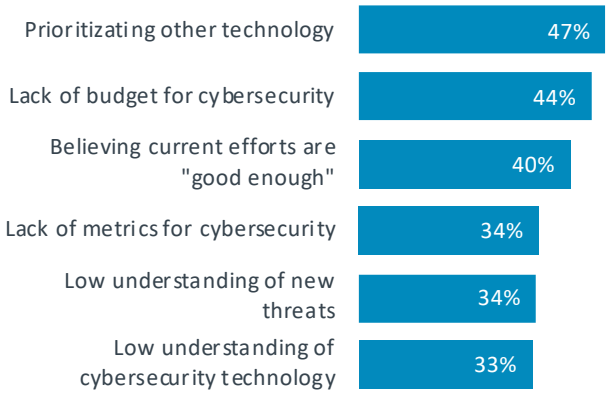
Building a better understanding of the issues is a key part of being a digital organization. Consistent with past years of security research, the top driver for greater emphasis on security is a change to IT operations. Along the same lines, 86% of companies agree that they have made some change to their technology approach in the past two years (e.g. accelerated adoption or explored emerging areas), and 87% of companies agree that they have changed their security approach in the same timeframe (e.g. added new technology or implemented workforce education).

Drivers for changing priority of cybersecurity



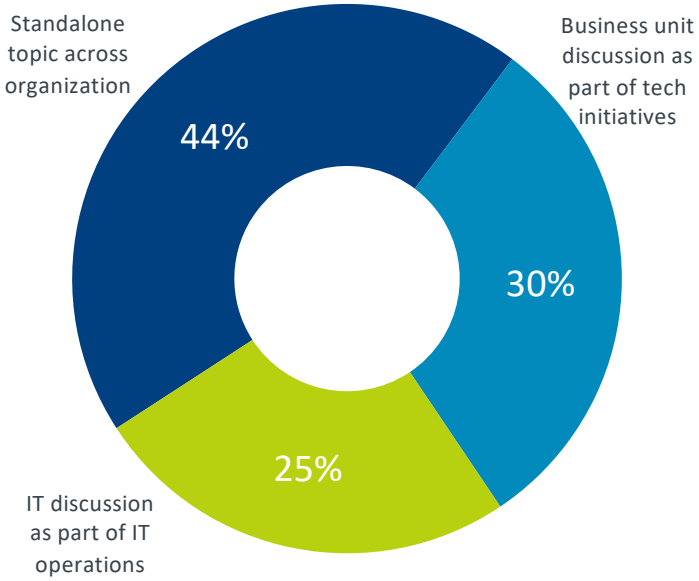
As much as companies may be changing their cybersecurity approach, there are always going to be challenges in achieving the ideal state. The top challenge cited—prioritizing other technology—is a signal that amidst all the confusion around technology innovation and cybersecurity, technology innovation still has a strong pull. Budget concerns are naturally a hurdle for most technology initiatives, but if security is truly rising as a priority, that suggests that budgets must rise as well. Generally speaking, The cost center approach to IT is changing as technology becomes more strategic, and that especially applies to cybersecurity.

Hurdles for cybersecurity initiatives



In order to tackle the wide array of problems involved with cybersecurity, businesses are starting to recognize that they need to treat security as a separate focus rather than one of many components in an IT strategy. In 2016, CompTIA's whitepaper on *A Functional IT Framework* projected that security would soon become a distinct discipline for many companies. Today, nearly half of all companies say that cybersecurity is discussed across organizational boundaries as a standalone topic (note that 2% of companies said that cybersecurity is treated as an afterthought in technology decisions).

Characterization of cybersecurity discussions



These cross-company discussions may serve to highlight the issues associated with cybersecurity, but they may not necessarily provide the structure for building the proper solutions. Forming cybersecurity teams was the central theme of CompTIA's security research in 2018, and one of the main takeaways was that the concept of security teams is still a very new idea for most companies. That continues to be the case in 2019. Furthermore, dramatic shifts in the data regarding the location of the cybersecurity function shows that many firms are unsure about how to even define a cybersecurity center of operations. Even with all the movement, though, there are a few key points worth noting.

First, companies show a tendency towards internal resources as the center for operations. Conceptually, this makes sense; the challenges of assessing risk tolerance, classifying data, and responding to security incidents are best addressed by internal employees who understand the corporate DNA. The obvious challenge is the difficulty in creating a specialized team, especially for small businesses that may not even have general IT staff on board.

That leads to the second key point, which is the diverse nature of security teams. The majority of firms that claim to have an internal center of security operations also say that they use third parties on either an ongoing basis or for occasional projects. Among the small handful of companies who view their center of operations as an external function, most say that they supplement this function with internal employees, usually employees who have security as a part of their overall IT responsibilities.

Taken together, these trends paint a picture of how security is likely to be handled in the future as it evolves into a general business concern. The closest comparison is not to think of how companies have handled their IT in the past, but how they have handled other critical business functions, such as legal and accounting.

The smallest businesses cannot afford to have a specialist in these types of roles, but it usually does not take too much growth before a business wants to have a dedicated individual. When a third party is managing these areas, it is not a firm that handles a wide range of business operations. It is a firm with deep expertise in the field, if not the specific industry of their clients.

If security is a critical business issue on par with these other disciplines, then it requires the same type of team. Internal staff should be security specialists that drive overall strategy and daily operations. The reporting structure for security staff is something that is evolving as security teams are being formed. There are cases to be made for the security function reporting to a CIO, COO, or even a CEO.

When it comes to third parties managing security, the same criteria applies regarding expertise. To own the function, security firms need depth and breadth to cover the full range of security topics. There is the possibility for a general IT firm to act as the lead on security and subcontract the expertise, but that type of partnering is still not the norm in the marketplace, and the firms that might be looking to simplify their own third party contracts also might not have the budget to support a hierarchy of outside help.

When IDC projects that managed security services will be the primary component of security spending, they are most likely referring to those firms that have significant expertise. Like so many other terms in the IT industry, the label of managed security services is broad, and it can be applied to companies that only have a limited number of offerings. To fully benefit from the projecting growth in spending, IT firms may need to improve their security portfolio and skills.

The situation in security mirrors the situation happening across all technology. As companies become more strategic, their requirements grow more ambitious and complex. Simply providing the basics may have been a sufficient business model in the past, but a modern technology provider needs a strong understanding of the technology. For security, that means knowledge of the many tools and techniques being used, the processes that lead to secure business operations, and the methods for ensuring low security risk among the workforce.

BUILDING SKILLS FOR CYBERSECURITY

Up-to-date expertise is incredibly important for security practitioners, but the fusion of technology into every business process has made security expertise an issue across the entire workforce. Businesses have to determine the best way to mitigate human error, which has consistently been the leading cause of security incidents. This means thinking broadly about basic cybersecurity awareness as well as thinking specifically about job roles that may need deeper knowledge.

Level of cybersecurity expertise

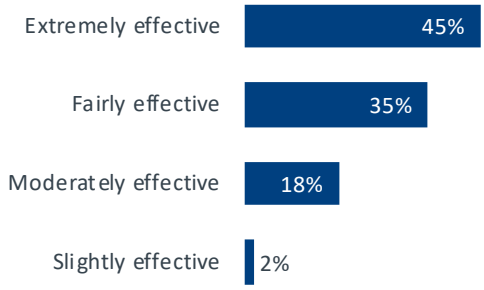
	Business staff	General IT staff	Security specialists
Exactly where we want to be	44%	47%	54%
Slightly behind the ideal skill set	32%	36%	32%
Moderately behind the ideal skill set	15%	9%	7%
Not at all where we want to be	4%	5%	4%

Generally speaking, most companies are not where they want to be when it comes to security awareness and skills, especially for those staff that are not security specialists. Business staff are the first segment to address when it comes to workforce expertise. Employees who are not directly working in IT do not need extensive security skill, but that expectation is almost certainly baked into any assessment. The fact that business staff rank lowest against companies' expectations signals a need for a new approach.

The surprising part of this low ranking is that most companies seem to be taking the obvious step to address the problem. Three out of four companies with cybersecurity gaps among their business staff say that they are providing cybersecurity training for their general workforce. This number is consistent across different company sizes—training is provided by 74% of small companies (less than 100 employees), 75% of mid-sized companies (100-499 employees), and 81% of large companies (500+ employees). There is a stronger correlation between training and satisfaction with security posture. Training is provided at 93% of companies who are completely satisfied with their current security but only 61% of companies who feel that their current security is adequate or unsatisfactory.

While security training is apparently getting delivered, it is obviously not improving the perception of workforce awareness. Among those companies who are providing workforce training, it is interesting to note that the rating of effectiveness maps closely to the rating of business staff expertise. Understanding the possible explanations for a lack of effectiveness in training can help companies determine what their next step should be in building a secure workforce.

Effectiveness of workforce cybersecurity training



The most likely culprit behind both ineffective training and unskilled staff is a lack of hard data for defining success. For now, CompTIA's survey did not dig into the reasons behind individual perceptions of skill gaps or effective training. However, the survey did examine the use of metrics for the overall security function. Full results appear later in this report, but the short answer is that most companies do not have a strong use of metrics, and this is presumably the case for workforce training, which is a relatively new concept in the field of cybersecurity.

Anecdotally, several companies have made attempts to build metrics around the effectiveness of the training and the state of workforce awareness. Companies that use simulated phishing attacks can track how many employees correctly handle suspicious emails, then compare numbers before and after training. Regular assessments of security knowledge can pinpoint areas of weakness and provide ideas for targeted training. These types of metrics can give businesses concrete data around initiatives rather than leaving it up to a best guess.

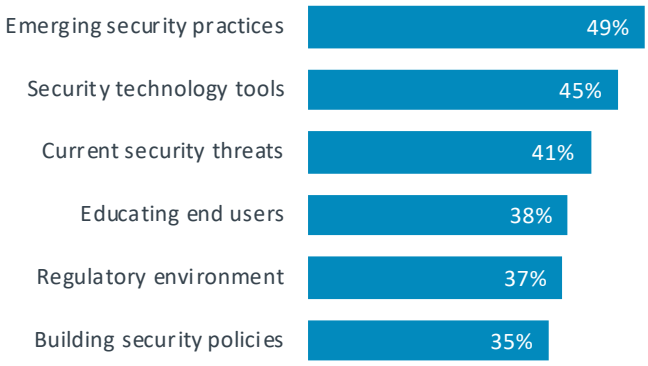
Getting metrics in place requires understanding what to measure, and this may be a larger problem for companies to solve. Given that workforce training is a relatively new concept, businesses may not have a strong grasp on what constitutes an ideal skill set. The problem quickly gets complicated when thinking about different job roles. For example, a worker on a manufacturing floor with no access to email does not have a critical need to identify phishing emails. In order to apply metrics and understand if progress is being made, there must be a decision on the appropriate levels of skill.

This leads to a final complication: knowing what level of skill truly mitigates the risk of human error. Ultimately, it may be impossible to perfectly correlate training to reduced risk. Since there are already struggles with making training effective, pouring more money and energy into the problem is not guaranteed to drive improvement. Aside from determining the approach to cybersecurity training, companies must determine their overall approach to human error. Getting to this decision requires agreement across all players at the highest levels of the business, which increasingly includes a board of directors or other governing body.

Moving beyond the general workforce, addressing skill gaps among IT staff requires a more focused approach. Two major shifts have taken place that have driven demand around security skills. The first is that cybersecurity has broadened beyond the IT function. Where companies could once view security as one of many skills needed by every IT employee, there is now a need to consider employees whose sole responsibility is the security of digital assets.

The second shift stems from the first. As security emerges as a distinct discipline, the complexity of securing cutting-edge infrastructure and operational processes calls for a diverse set of skills. These two shifts are responsible for significant growth in security job postings. According to Burning Glass Technologies Labor Insights, cybersecurity job postings grew 34% between 2017 and 2018. Demand is incredibly strong, but supply is having a hard time keeping up.

Cybersecurity skill gaps among IT staff



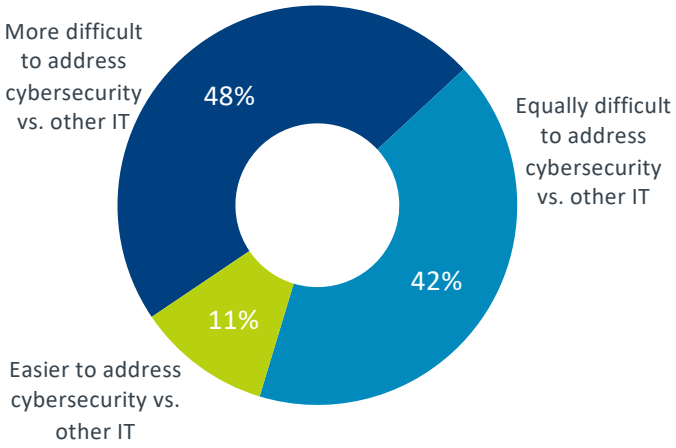
In-demand skills fall into the three main categories of modern security: technology, education and process. The most sought after skills are in the more traditional category of technology. Whether it is new practices that reflect a more proactive mentality (such as cybersecurity analytics or penetration testing), new tools that address a cloud/mobile infrastructure (such as data loss prevention or identity and access management), or new threats that take advantage of digital reliance (such as social engineering or denial of service attacks), companies need their IT and security specialists to be up to speed on the technological landscape.

Along with the workforce education challenges described earlier, there is the issue of who will manage the training and the ongoing monitoring of end user behavior. Most companies are looking to their IT department or security solution provider for this, and that drives a need for skills around education. Many IT practitioners may have delivered training on specific tools, but security education is aimed at actually modifying behavior and implanting a solid understanding of the reasons behind security policies.

The final group of in-demand security skills covers the processes needed for secure business operations. This includes knowledge of laws and regulations, which are quickly spreading beyond the typical highly regulated industries. It also includes other policies that should be implemented across the entire organization, such as managing relationships with outside parties or performing formal risk analysis of systems and data.

The scarcity of available cybersecurity professionals is just one reason that companies are finding it difficult to address their security skill gaps. In fact, the shifts in the corporate security approach (cited by 58% of companies) and the complex nature of modern security (57%) are the leading reasons for cybersecurity being more difficult to address than other IT skills. Other reasons include a lack of well-defined training options and a lower priority placed on cybersecurity compared to other technology initiatives.

Difficulty of addressing cybersecurity skills



Perhaps due to the lack of skilled workers on the open market, hiring is the least popular options for closing cybersecurity skill gaps, with only 33% of companies having recently pursued additional hiring. In terms of seeking additional help, partnering with outside firms is a much more popular option, with 49% of companies using partners to address security shortcomings.

The most economical choice, as well as the choice that gives businesses more ability to manage security strategically, is to focus on existing employees. This could either be through training (used by 69% of companies) or certifications (48%). Certifications obviously represent a more substantial investment, and some companies feel that training is sufficient or that there is not enough organizational understanding around the value of certifications.

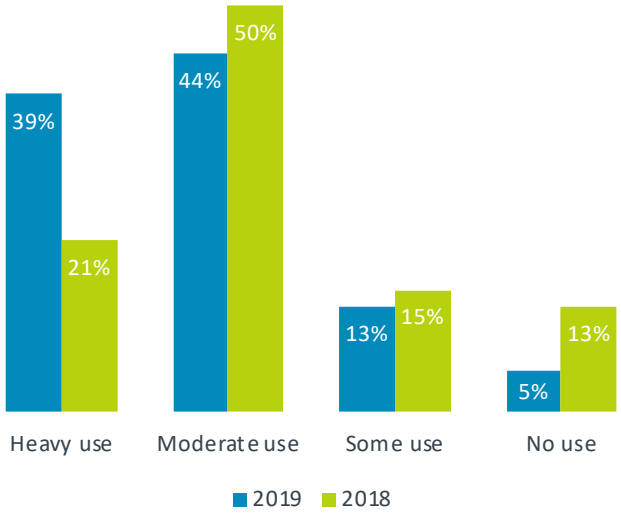
Along with giving companies the knowledge needed to adjust their security approach, certifications provide many benefits to the individual and the organization. Companies can feel more confident that their security professionals have deep knowledge, are following up-to-date practices, and maintain consistency when working with other internal or external teams. For more on the value of certifications, see the IDC whitepaper sponsored by CompTIA, *Impact of Certifications and Training on Career Milestones*.

TRACKING PROGRESS WITH CYBERSECURITY

As cybersecurity shifts to a strategic ongoing concern, there is a greater need to measure progress and make data-based decisions. In previous environments where security efforts focused on simply installing firewalls and antivirus software, the metric was correspondingly simple: zero security breaches. In an environment where security efforts are far more complex—inevitably driving a higher cost—there must be a better measurement of effort and investment.

Compared to 2018, there has been a sizable increase in the number of companies using metrics to drive their security function. Surprisingly, small companies seem to be taking the lead in this area, with 48% of small companies reporting a heavy use of metrics compared to 37% of large companies and 27% of mid-sized companies. While there may be some doubt around this number since small businesses have the least amount of security expertise, they are also the most likely to use a third party for managed security, which drives metrics around the service being provided if not the actual efficacy of the security activities.

Use of security metrics on the rise



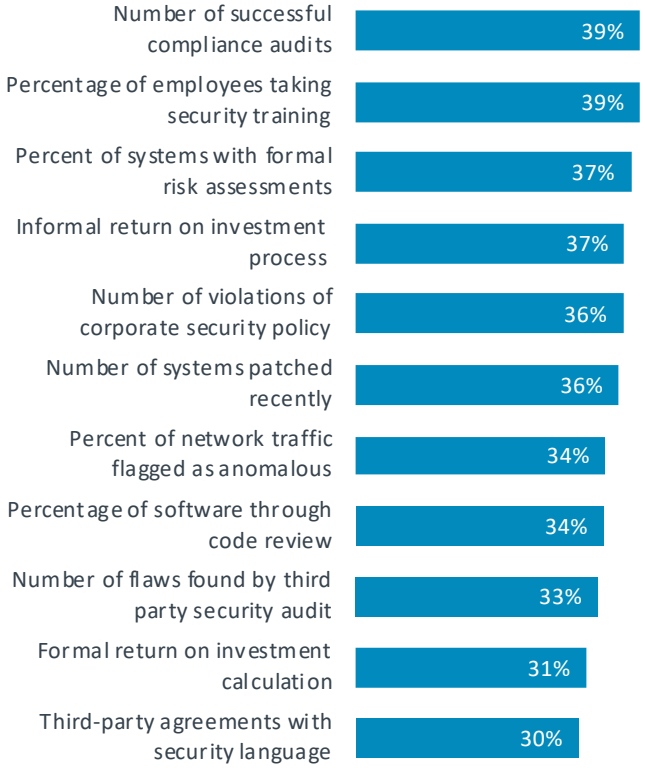
There is an even more stark contrast when examining companies based on satisfaction with their current security posture. The majority of completely satisfied companies (64%) claim a heavy use of security metrics. In comparison, only 19% of moderately satisfied companies use metrics at the same rate, and companies who feel their security is merely adequate or unsatisfactory rank even lower at 16%.

Clearly those companies who feel they are completely satisfied with their security posture are able to speak with more confidence because they are measuring their efforts. Establishing metrics is no easy task. In a resource-constrained field, the top reason given for not using security metrics is that there are not enough resources available for regular metric tracking. However, putting in the work to include metrics as the security function becomes more formal will pay dividends in shaping the corporate discipline.

The starting point for security metrics is determining which parts of the organization will be involved in the process. With security becoming more and more critical to business operations, it makes sense that monitoring success would spread beyond the IT function. IT employees are most likely to set the relevant metrics, with 69% of companies reporting this behavior. Reviewing metrics, though, is a much more collaborative activity. Every level of an organization is well represented in the review of security metrics, from the IT function (in place at 51% of companies) to middle management (57%) to senior executives (55%). The most significant year-over-year jump in terms of organizational involvement took place among boards of directors or other governing bodies. In 2018, 30% of companies reported a board of directors being involved in setting security metrics, and 38% reported involvement in reviewing metrics. In 2019, those numbers stand at 42% and 53%, respectively.

If a collaborative environment is in place, the next question is which security metrics are the best ones to use. There is no definitive answer at this stage; a tight clustering of various security metrics in use indicates that companies are experimenting to find the right mix. It is not surprising to see that best practices around metrics have not emerged yet. Businesses are in the early stages of recognizing that security is a function that requires dedicated focus. As they build out this function, becoming more proactive in the areas of technology, process and education, they will learn which metrics best quantify their efforts and allow them to correlate cybersecurity with overall success.

Types of metrics used for cybersecurity



RESEARCH METHODOLOGY

This quantitative study consisted of an online survey fielded to workforce professionals during July 2019. A total of 400 businesses based in the United States participated in the survey, yielding an overall margin of sampling error proxy at 95% confidence of +/- 5.0 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 / 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 research standards and ethics.

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-plus 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.

OTHER 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 workforce analyses, providing insights on jobs, skills, hiring practices, and professional development.

CompTIA Research Library

CERTIFICATION | LEARNING

CompTIA is the leading provider of vendor-neutral skills certifications and education of the world's IT workforce. CompTIA has four certification categories that test different knowledge standards, from entry-level to expert, in cloud computing, mobility, Linux, networking, security, help desk and technical support, servers, project management and other mission-critical technologies.

CompTIA Certification and Resources

COMMUNITIES | COUNCILS

CompTIA member communities and councils are forums for sharing best practices, collaborative problem solving, and mentoring. Discussions frequently revolve around the types of emerging trends covered in this report.

CompTIA Communities

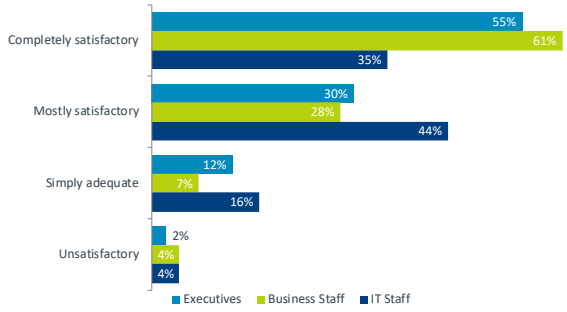
ADVOCACY

Through its public advocacy efforts, CompTIA champions member-driven business and IT priorities that impact the continuum of information technology companies – from small IT service providers and software developers to large equipment manufacturers and communications service providers. CompTIA gives eyes, ears and a voice to technology companies.

CompTIA Advocacy

APPENDIX

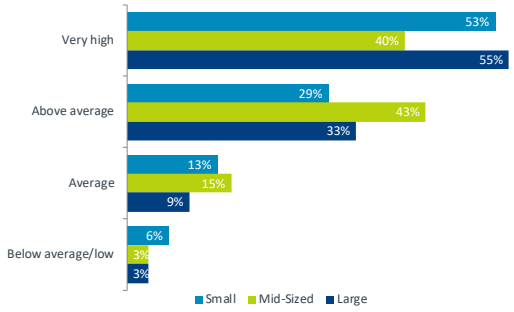
Current Level of Cybersecurity



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

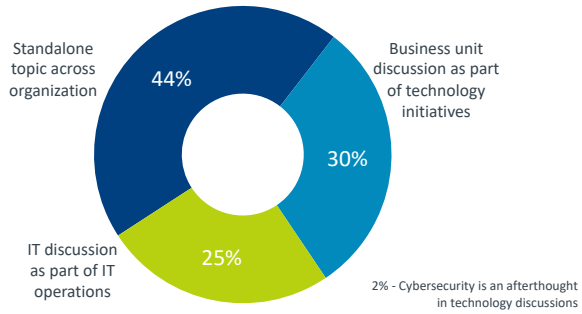
Current Level of Cybersecurity Understanding



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

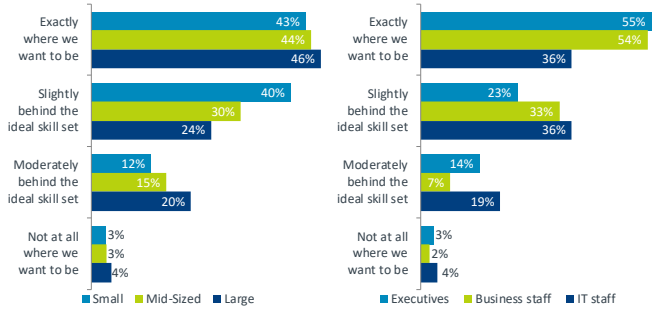
Characterization of Cybersecurity Discussions



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

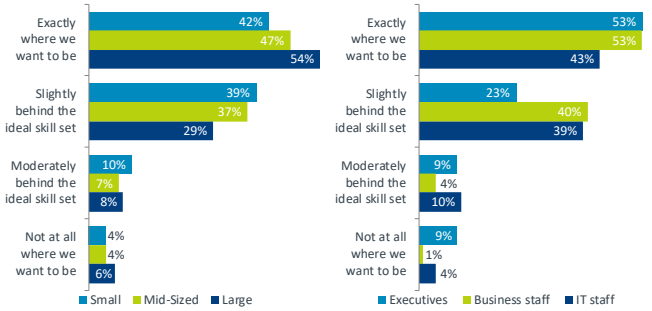
Level of Cybersecurity Expertise Among Business Staff



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

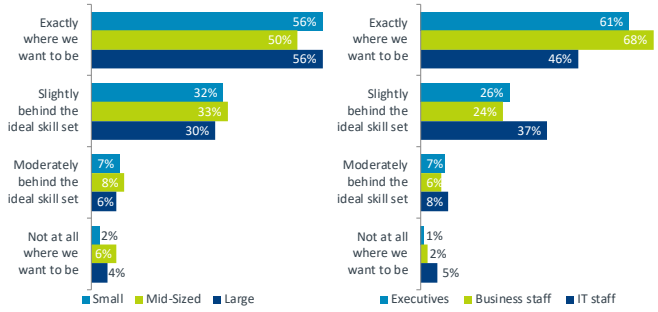
Level of Cybersecurity Expertise Among IT Staff



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

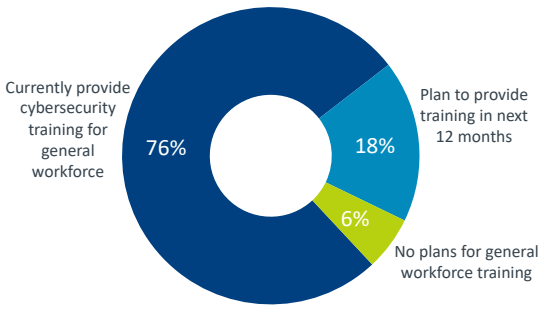
Level of Cybersecurity Expertise Among Security Staff



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

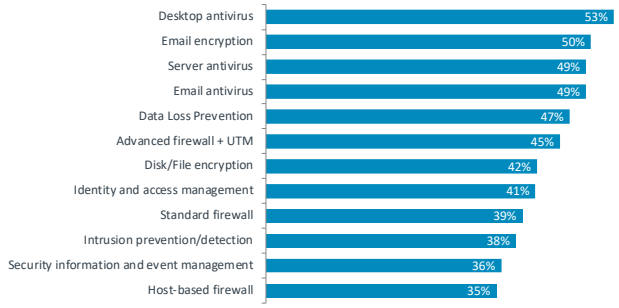
Incidence of Workforce Cybersecurity Training



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 204 IT and business professionals in the U.S. with cybersecurity skill gaps among business staff

Cybersecurity Products in Use



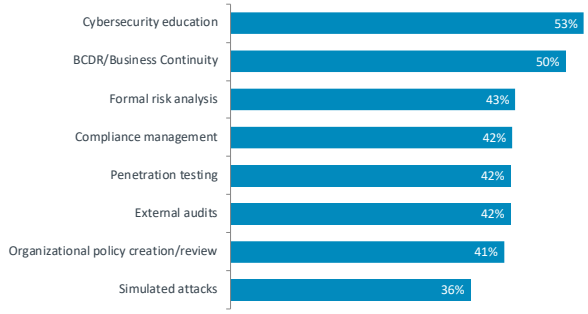
CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

CompTIA

APPENDIX

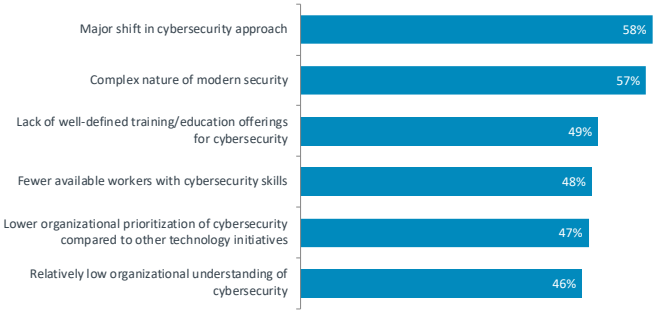
Cybersecurity Processes in Use



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 400 IT and business professionals in the U.S.

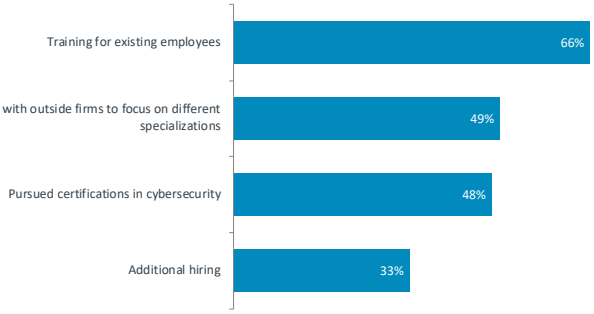
Reasons for Greater Difficulty Addressing Cybersecurity



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 191 IT and business professionals in the U.S. viewing cybersecurity skills as difficult to address

Actions Taken to Close Cybersecurity Skill Gaps



CompTIA

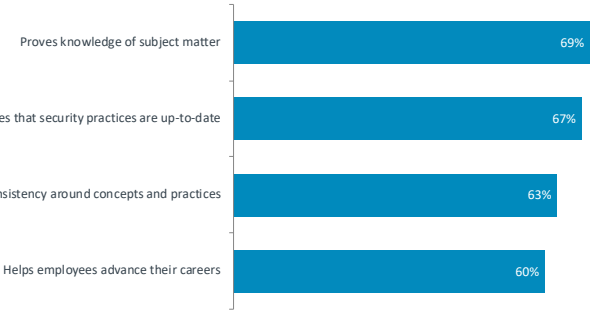
Source: CompTIA's *Cybersecurity for Digital Operations* | n = 263 IT and business professionals in the U.S. who see cybersecurity skill gaps among IT staff

Reasons for Not Pursuing Cybersecurity Certifications

CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 137 IT and business professionals in the U.S. not utilizing cybersecurity certifications

Reasons for Pursuing Cybersecurity Certifications



CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 126 IT and business professionals in the U.S. utilizing cybersecurity certifications

Parts of the organization involved with security metrics

	Set metrics	Review metrics
IT function	69%	51%
Some business units	43%	53%
Middle management	44%	57%
Senior executives	49%	55%
Board of directors	42%	53%

CompTIA

Source: CompTIA's *Cybersecurity for Digital Operations* | n = 382 IT and business professionals in the U.S. using cybersecurity metrics

CompTIA