RESEARCH REPORT

2018 TRENDS IN CYBERSECURITY

BUILDING EFFECTIVE SECURITY TEAMS

September 2018

As cybersecurity has become more complex, traditional methods do not account for the wide range of issues related to securing corporate data and handling privacy concerns. New technology, improved processes and broad workforce education are all required for a modern security posture. Adopting a new approach requires cultural change within an organization, but it also requires a diverse set of skills. This report examines the ways that businesses are building security teams, using internal and external resources to assemble the expertise needed for security in the digital age.

KEY POINTS

The focal point of cybersecurity activity for most companies is internal

Whether companies have security resources that are part of a general IT infrastructure team or they have dedicated security employees, 72% of firms believe that their security center of operations is an internal function. With cybersecurity becoming a critical ingredient to operations and reputation, it is no surprise that businesses want to keep a close eye on things.

Even with internal focus, most companies utilize external resources for cybersecurity

Among companies that have internal security resources, 78% also use third parties for their security needs. This could be an ongoing contract with a third-party firm for certain security activities, or it could be the occasional use of third parties for individual projects. In fact, half of the businesses that use external partners use two or three different firms for security purposes, further emphasizing the complex nature of cybersecurity.

Cybersecurity skills are in need of improvement

Certain skill groups—such as access control or network security—are relatively strong within businesses, while others—such as vulnerability management or security analytics—are weaker. However, even among the strong skills, companies are looking for improvement. For example, 25% of companies say that significant improvement is needed in network security, and an additional 64% say that moderate improvement is needed.

Stronger metrics are needed to quantify cybersecurity efforts and success

Only 21% of companies say that they heavily use metrics as part of their security efforts. As security moves from defensive tactics to proactive initiatives, metrics such as “percent of systems with formal risk assessment” and “percent of network traffic flagged as anomalous” can serve as measures of success or justification for further investment.

MARKET OVERVIEW

Over the past decade, the technology world has been split into two major domains. On one side, there are new technologies that are redefining business operations. Cloud computing and mobile devices were early examples and have now become established parts of IT architecture. Internet of Things, artificial intelligence and blockchain are more recent examples, promising to further disrupt traditional technology usage and management. On the other side, there are traditional technologies that are critical for day-to-day operations but are not driving new growth. Servers, networks, and storage may not feature in many headlines, but IT pros remain keenly focused on these areas as they evolve to meet modern needs.

Cybersecurity is interwoven into both of these area. In the early part of this new era, cybersecurity was viewed more as a traditional technology, something that would simply be extended into new ventures without a drastic change to the existing model. Today, companies recognize that security requires a new approach for new technology usage. Traditional pieces may still remain, but new components and processes must be added.

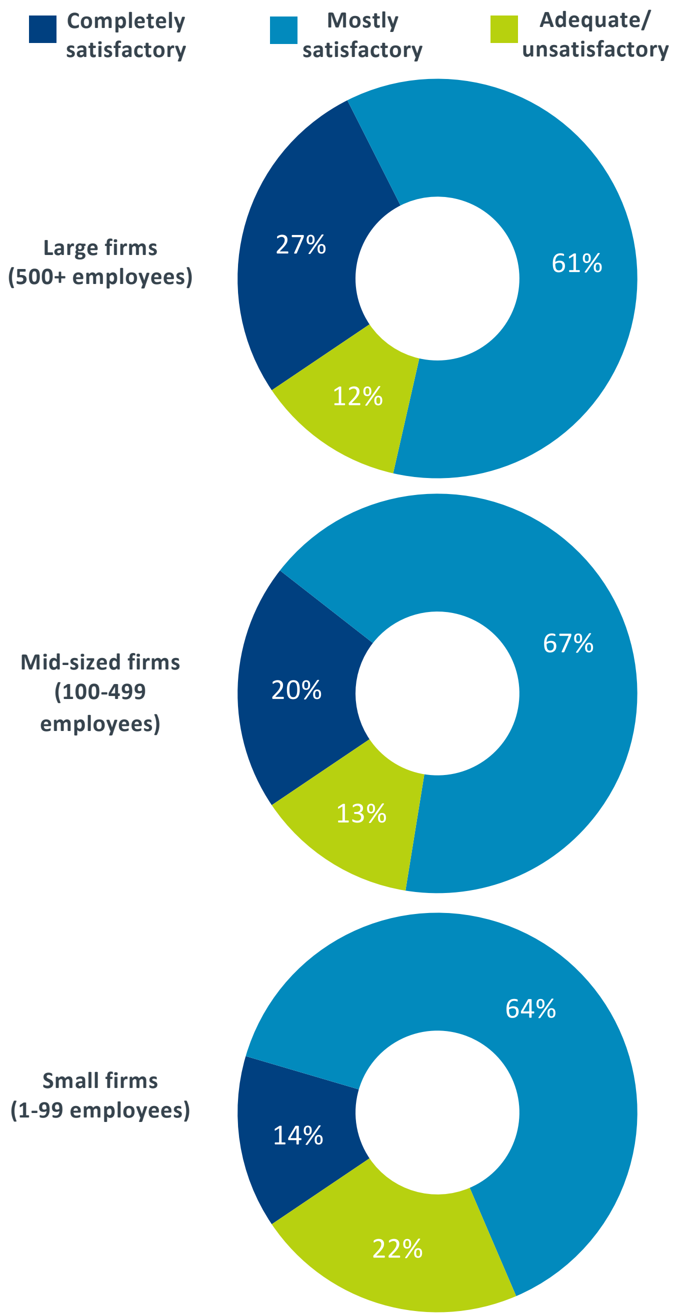
The dual nature of cybersecurity, with one foot planted in traditional methods and another foot planted in emerging technology, leads to above average revenue expectations. CompTIA's *IT Industry Outlook 2018* projected 5.0% growth for the overall IT sector in 2018. For the field of cybersecurity, IDC is projecting 10.2% growth in 2018, resulting in $91.4 billion in global revenue. It is worth nothing that this figure covers security-related hardware, software, and services; the traditional approach to IT security relied heavily on hardware and software, but a modern approach includes services such as compliance management or end user education.

Thanks to this extra layer of services, along with a growing technology toolbox, IT security has become far more complex. CompTIA's *Functional IT Framework* whitepaper describes how security has become a separate function, rather than existing as a part of the broad infrastructure function. Extra focus is needed as IT security incorporates new methods and becomes more critical to ongoing business success.

Unfortunately, this added complexity is not something that every company can easily absorb. Businesses with fewer than 100 employees are far more likely than their larger counterparts to feel that their IT security is simply adequate or unsatisfactory. Without a deep resource pool to lean on, smaller firms struggle to address new facets of cybersecurity. As the volume of attacks is rising, companies need to give serious thought to the way they are securing assets and protecting customer data. FURTHER READING

In order to address the technologies, processes and education that are needed for modern security, companies are exploring the formation of security teams. These teams often combine internal and external resources to ensure that specialized skills are in place as needed in order to create a robust cybersecurity strategy.

Satisfaction with current security posture



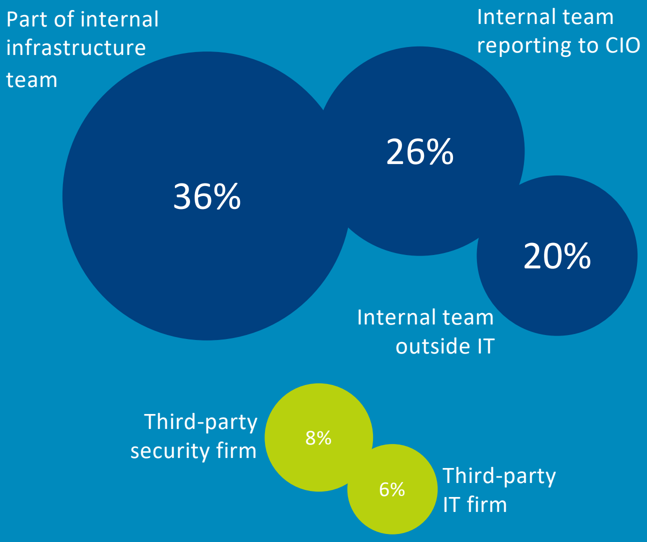
For companies without much focus on cybersecurity, it may be difficult to generate the momentum needed to build a functional team. A full 46% of firms report that their companies believe that security is "good enough," and 45% report that there is a lack of budget dedicated to security. However, as the critical nature of security is felt by more and more businesses, there will be more directives—possibly from the very highest levels—to ensure the right level of expertise needed for comprehensive cybersecurity coverage.

SECURITY TEAM BASICS

While dedicated cybersecurity teams are becoming more popular, they are still not commonplace. The largest companies are leading the way. These are the companies with the most resources at their disposal, and they also face the greatest risk from cyberattacks. The vast majority of large enterprises employ a CISO, though even here there are various reporting structures (e.g. reporting to CIO, reporting to CEO, reporting to CFO, etc.). Across all firms, creating a dedicated security team is the least common change taking place within cybersecurity. FURTHER READING

However, a company does not need dedicated resources in order to recognize some center of security operations. Even where the security function is still part of the overall IT infrastructure team, most companies have a set of resources they view as the focal point for cybersecurity.

Location of security center of operations



While it is somewhat surprising to see such a low incidence of third-party focal points, it makes sense that most companies would want to rely on internal resources to drive security strategy. As organizations go through digital transformation, they develop a tighter relationship between technology and business success (for more on this topic, see CompTIA's whitepaper on *Using Strategic IT for Competitive Advantage*). Ensuring the security of that technology is becoming a core competency that justifies an investment in internal resources.

The different approaches based on company size fall in line with expectations, but they still provide some insight into future direction and opportunities. Two thirds of large companies have dedicated teams for cybersecurity, with a nearly even split between teams within the IT function and teams reporting elsewhere. As dedicated teams become more prevalent, the exact reporting structure may vary based on industry vertical or corporate culture.

Mid-sized firms do not have as many dedicated teams, but they still place emphasis primarily on internal resources. The use of general infrastructure employees as security champions follows a typical pattern for mid-sized businesses: the scope of the business drives the creation of discrete departments, but there are still limitations that prevent a high degree of specialization.

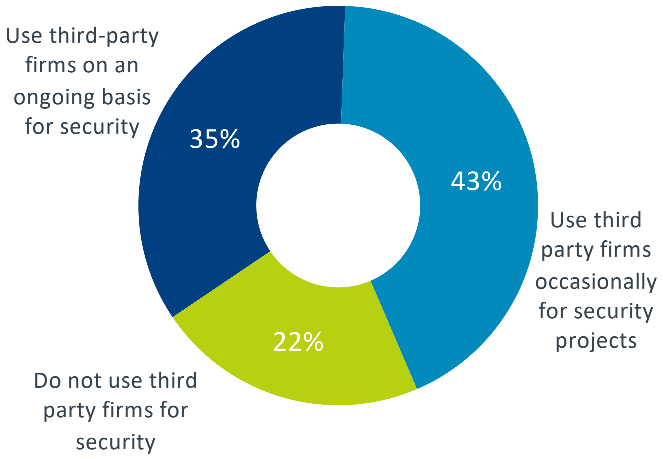
The smallest companies diverge from the pattern of internal resources. Not only are they far more likely to use a third party as their cybersecurity focal point (26% compared to 8% of mid-sized firms and 5% of large firms), but they are also the dominant group that does not have enough security focus to require a defined owner (12% compared to 1% of mid-sized firms and 0% of large firms). At first glance, this seems like a ripe opportunity for third parties to take the lead on security issues, but of course these small businesses also have the least amount of budget to spend.

Whether a company is forming a cybersecurity team, shifting the reporting structure, or setting priorities for the team, the main driver for determining the strategy will be the changes taking place within IT operations. As in past years, these IT changes are the leading motivator for a new security approach, yet there is still a gap between IT tactics and security transformation. Only 48% of companies say that a change in IT operations has driven a new approach to security. This number has remained consistent over the past several years, when there have clearly been more companies transitioning to cloud models and mobile devices, which both require significant changes to a traditional security approach.

UTILIZING EXTERNAL RESOURCES

Although most companies consider internal resources the focal point for cybersecurity matters, external resources still play a role in a field with such a high degree of complexity. Among the companies that have their own security resources, 78% also use third parties in some way. There is a relatively even split between the use of third parties in an ongoing partnership and the use of third parties on a project-by-project basis, showing the breadth of opportunity for companies specializing in IT security implementation and management.

Use of third parties by companies with internal security resources



It may come as a surprise that there is little difference in the use of third parties across company size. In fact, larger companies report a higher incidence of using outside help with security initiatives. For occasional projects, the use of third parties is very consistent—43% for all company types. For ongoing work, though, 39% of large firms use third parties, compared to 35% of mid-sized firms and 30% of small firms.

The takeaway is somewhat obvious, but still bears mention: the scope of a security strategy grows in direct relationship to architectural and operational complexity. Certainly there are many small businesses that are underestimating the appropriate level of security for modern technology, but it is also true that they are operating at a smaller scale. As they grow, though, they will need to be aware of security vulnerabilities that get created from expanding IT architecture or adding operational procedures.

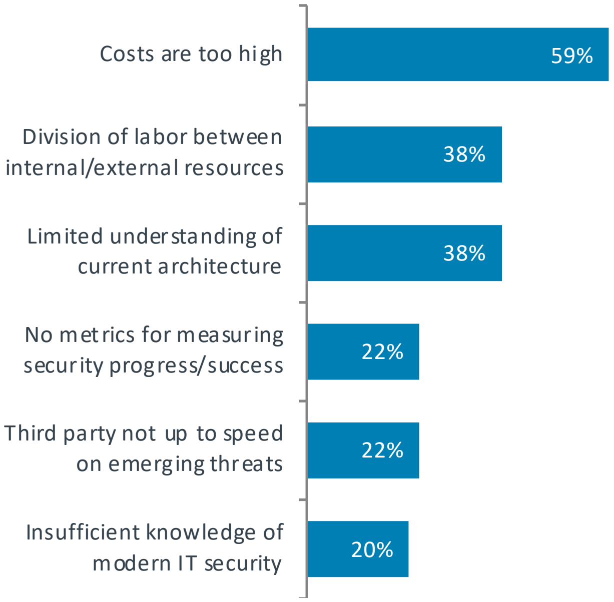
Just as security has become a specialization within IT departments, it has become a mini-industry among companies who provide IT services. Many solution providers highlight security as a distinct offering rather than folding it into other offerings related to network management or cloud services. Other firms have gone a step further, choosing to focus exclusively on IT security. Most often, these firms are known as managed security service providers (MSSP). This segment has become robust enough for Gartner to publish a Magic Quadrant evaluating 17 of the largest companies in this space. MSSPs are not the dominant model for security outsourcing, though. Among companies that use a third party for security services, just over half (51%) use a general IT solution provider. Additionally, 38% use a general security firm, one that might manage physical security along with IT security; 35% use a focused IT security firm such as an MSSP; and 29% use a firm that provides technical business services, such as digital marketing or content management.

These numbers indicate that companies use more than one outside firm for their security needs. In fact, only 37% of companies use a single firm for cybersecurity. Another 50% use two or three partners, and 13% use four or more. Using multiple partners enables a high degree of specialization but also requires a greater degree of oversight and coordination, especially as some partnerships are well-established and some are more recent. FURTHER READING

Whether companies are currently utilizing external security resources or not, there are several challenges that must be managed. First and foremost are the costs associated with using a third party. While costs are typically a hurdle for IT operations, security poses an interesting question for businesses. If the security landscape is getting more complex at the same time that security is becoming more critical to business operations, it stands to reason that the ongoing cost of security will rise from previous levels.

Beyond cost, there are some technical and procedural hurdles that must be cleared. On the technical side, solution providers need to make sure they understand their clients' current architecture, especially where business units may be introducing applications outside the purview of the IT department. Logistically, the division of labor and coordination between different areas require ongoing management, clear communications, and defined metrics for progress and success.

Current/expected challenges with outside security firms

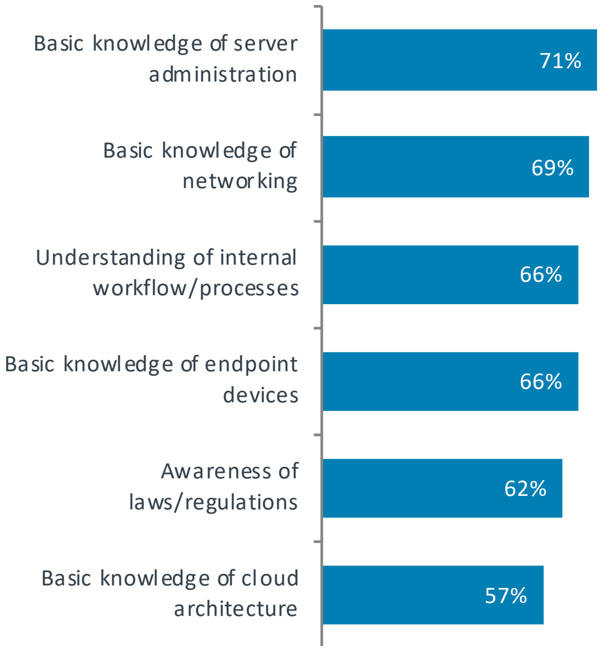


ADDRESSING SKILLS WITHIN TEAMS

As cybersecurity has become its own domain separate from IT infrastructure, there has been speculation around what types of career pathways will emerge. For example, what might an entry position in security look like, considering that most security positions have traditionally emerged as extensions of an infrastructure team?

For now, it seems that even an entry-level position in IT security is somewhat more advanced than an entry-level position in infrastructure (such as help desk). Before learning security-specific skills, a candidate needs competency in those things that are being secured. These prerequisite skills may start with servers and networks, but holistic security now involves internal workflow and processes as well as the ever-changing regulatory environment. A strong grasp of skills validated by a certification such as CompTIA A+ is the first step in a cybersecurity career.

Prerequisite knowledge needed for IT security



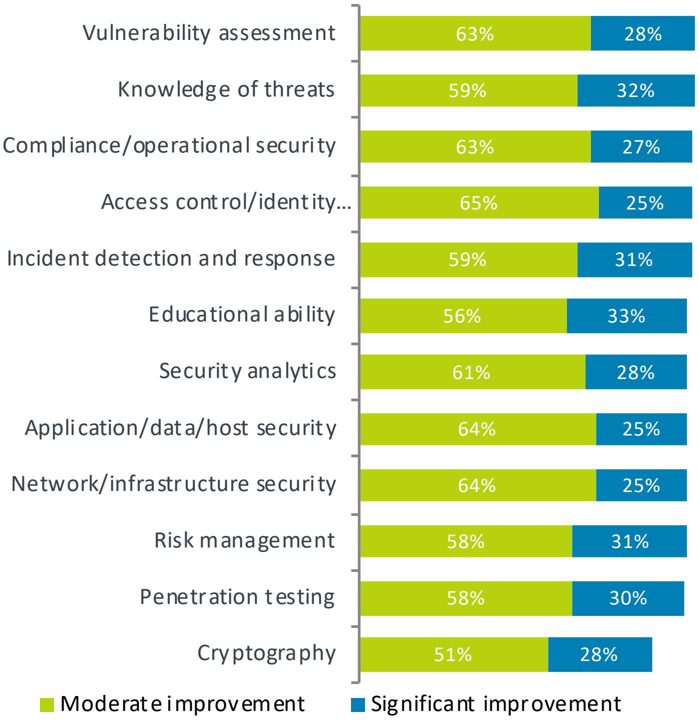
Building on this foundational skill set, there are a wide range of IT security skills that contribute to success. Some skills have been in practice for quite some time. Network security, endpoint security, and threat awareness are all examples of skills that have long been a part of a security strategy. Correspondingly, those companies that have an internal security focal point see relatively strong expertise in these areas among their internal resources, and those companies with an external focal point see relatively strong expertise in their security partners.

Moving up the skill stack, there are some skills that have become more important as cloud and mobility have become ingrained into IT operations. Companies leaning on internal resources may have started responding to these skills, whereas third parties with established offerings may struggle more to add the necessary expertise. Consider the example of access control and identity management. Eight out of ten companies with internal security focal points feel that this skill is current in-house, but less than half of all companies with external focal points feel that their partners are up to speed on this skill.

Finally, there are skills that are emerging as important parts of security monitoring and proactive tactics. These skills have relatively low degrees of understanding across the board, and represent prime areas of growth and opportunity. Security analytics involves using data to detect anomalous behavior, and penetration testing is the practice of actively seeking out any vulnerabilities in a system. Newer certifications such as CompTIA CySA+ and CompTIA PenTest+ can help ensure that security practitioners are proficient in these modern skills.

Even when companies believe that certain skills are relatively strong, there is still a desire for further improvement. The consistency in the number of companies looking for significant improvement does not necessarily correlate to the current strength of that skill; rather, it is likely a statement of familiarity. Companies know more about network security, so they know exactly which areas need improvement. They know less about vulnerability assessments, so they simply know there's a long way to go.

Improvement needed across a broad set of skills



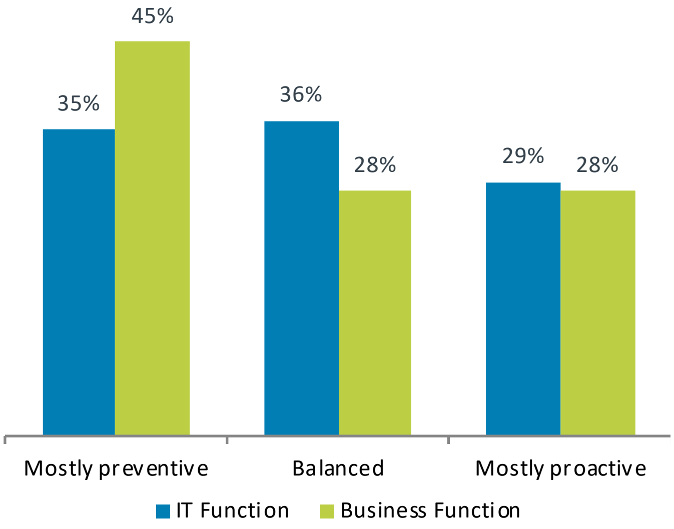
In order to close skill gaps, companies are primarily looking to bolster current efforts, whether that means training current employees or expand the use of third parties. New headcount or new partnerships are secondary considerations, and certification may quickly grow as a method for ensuring that the correct skills are in place. FURTHER READING

MAKING SECURITY TEAMS MORE EFFECTIVE

Although skill growth is the most direct way to improve the effectiveness of a security team, there are many other steps an organization can take to ensure that a security team has the best chance for success. From a cultural perspective, understanding that IT is now a strategic activity drives new mindset and behavior. Likewise, there are new attitudes and practices that must emerge as security becomes a separate operational function, and quickly integrating a new mentality throughout an organization will help security efforts move forward.

The most critical aspect of modern security for an organization to grasp is that the objective is no longer about building the ideal defense. Implementation and maintenance of a secure perimeter is still a necessary task, but it is no longer sufficient. Cloud computing and mobile devices have introduced workflow and data storage techniques that require new models, and the incessant nature of attacks makes total prevention an unreasonable goal. As such, companies are turning to more proactive methods to ensure a strong security posture.

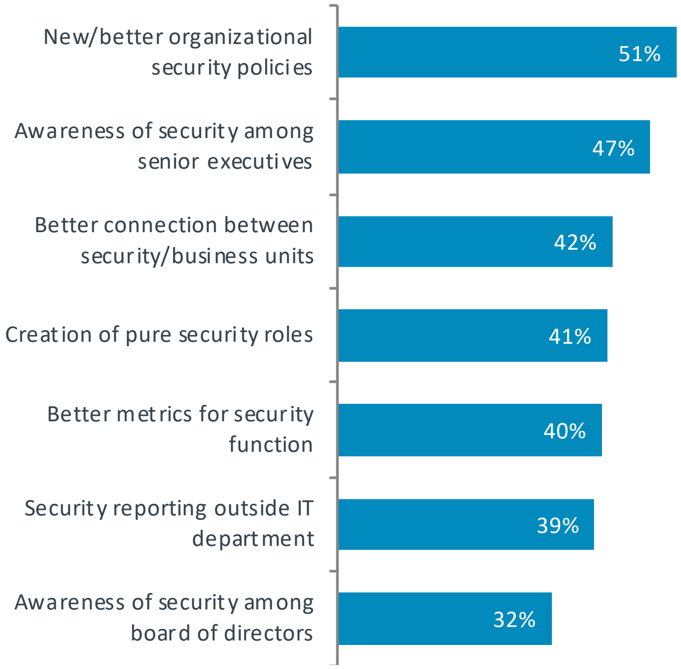
Security mindset shifting away from pure defense



Many employees in a business function may not understand the distinction. For them, there is still the assumption that no news is good news when it comes to security. IT professionals have a better grasp of the proactive steps that are being taken, but even so the majority have not shifted to a mostly proactive approach. When considering the constant vigilance required to monitor for breaches along with educational needs that may only be in very early stages, it seems likely that future security efforts will be largely concentrated on proactive endeavors.

The recognition that security is an ongoing activity is critical because it drives actions and investments. With a proper understanding of how the security function needs to operate, an organization can do what is needed to empower and enable a security team.

Organizational steps for effective security teams



The first step for many organizations is the creation or modification of security policies. Not only can new policies address issues with new technology models, but they can also define enforcement, giving security practitioners the leverage they need to drive workforce behavior.

Another major effort lies in building awareness of security among executive leaders and the board of directors or other governing body. This emphasizes a common theme weaving through recent IT discussions: the need to place technical decisions within a business context. Technical specifications do not equal business justification, so part of the new security role is tying security activity and investment to corporate success.

One example of a security activity that requires strong consensus is risk analysis. Although most companies understand the concepts of risk analysis within a project management framework, rigorous risk management for security is a less common practice. Businesses are getting more granular in assessing risk, but there are still potential gaps in areas such as social media and partner/supplier relationships. FURTHER READING

Investing in security is not a new concept; the new part is the breadth and extent of investments. The standard security items in the corporate budget are firewall and antivirus, and these items still dominate the infrastructure tools currently in use. Less than half of all organizations utilize data loss prevention (DLP) or identity and access management (IAM), two tools that are finding a strong foothold in cloud/mobile environments. Of course, the technical budget is now just a portion of the overall budget, especially considering the workforce education content needed to mitigate the leading cause of security breaches—human error. FURTHER READING

INCIDENT RESPONSE

One of the most challenging aspects of modern security for many firms is the assumption that breaches are certain to occur. For many years, the primary mindset around cybersecurity was the prevention of any breach. Accepting that breaches will happen runs counter to the security objectives companies have historically pursued.

As stated before, though, the volume and complexity of cyberattacks makes total prevention unattainable. Security professionals may be able to theoretically construct impenetrable defenses, but the end result is either astronomically expensive or impractical for a modern workflow. To be honest, this has probably always been the case. Any perception that security breaches were not occurring in the past was more likely the result of lower overall attacks than of perfect defenses. Awareness obviously plays a role as well—knowledge of security breaches is a direct function of the ability to detect a breach.

One of the biggest surprises of the study is the number of companies saying they have had no security breaches in the past year. In 2015, 34% of companies claimed they had not experienced a recent security breach. Today, that number still stands at 33%. Given the rampant nature of cyberattacks and the increasing risk of new threats from the use of emerging technology, it seems highly unlikely that a third of all companies remain safe from phishing, data leaks, or other incidents that compromise digital assets.

One clue to this low number might be found in the number of companies classifying their breaches as serious. In 2015, 55% of those companies with knowledge of a breach classified their breach(es) as serious. In 2018, that number is 46%. While the definition of "serious" in the survey is subject to interpretation by the respondent, this still points to a difference in how companies view security activity.

The growth in companies that recognize security breaches but classify them as non-serious suggests that some breaches are being treated as a standard part of digital business. However, even recognizing these as breaches further suggests that some sort of mitigation is in place. For those companies that feel they have had no security breaches, they may also see data loss or misplaced devices as par for the course; but by treating these as isolated incidents, there is a higher risk that root causes are not being addressed and deeper damage is taking place.

Once it is accepted that security breaches are a near certainty, the next step is determining how to respond when a breach is detected. Two thirds of companies say that they have formal policies and procedures for incident detection and response and that these policies are documented and communicated throughout the organization. This seems like a healthy foundation, but additional data reveals that the situation may be more precarious. To start, there is a major difference between the IT function and business functions—75% of IT employees believe that formal incident response is in place compared to just 45% of business employees. Furthermore, only 33% of companies with either formal or informal plans in place believe these plans are highly effective. FURTHER READING

Common parts of incident response plans

71%	Identification of affected systems
69%	Identification of attack
69%	Holistic business continuity/disaster recovery plan
57%	Definition of roles and responsibilities
54%	Post-incident education and mitigation
39%	Public communications plan

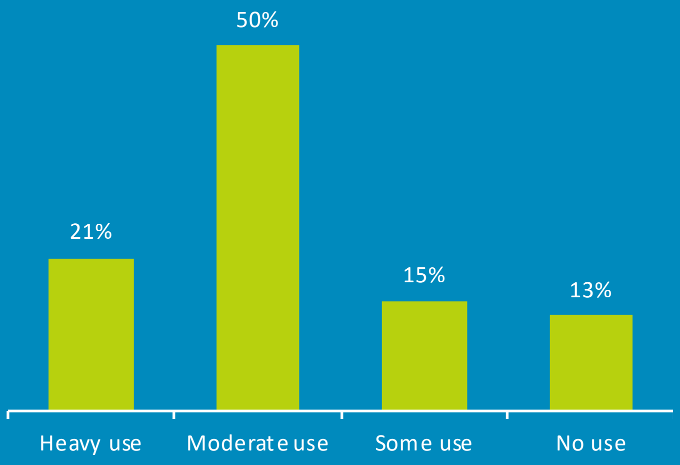
The differences in awareness of a formal incident response plan are further emphasized by the number of companies that have certain plan elements in place. The most common elements are technical—identifying affected systems, identifying the type of attack, and having a solid BC/DR plan. Elements that have more potential to reach into different parts of the organization are less common. Perhaps most troubling is the relatively low number of companies that have a public communications plan in place. Given the reputational damage that comes from a security breach and the public missteps that many companies have taken with their breaches, this is one area that will not only improve the overall security posture but will drive cross-departmental communications.

There is also a greater need to understand the types of threats in today's landscape. Incident response has limited effectiveness if the variety of incidents is not well understood. The most common threats that companies want to know more about are those threats that have a long history or have a tendency to make headlines. Spyware, phishing, ransomware, and viruses are top of mind for many organizations, and these attacks certainly should not be ignored since they are constantly evolving. However, there are many other threats which attack in different ways and should have a higher priority. Social engineering, IoT-based attacks, SQL injection, and DDoS are all very likely in any connected digital environment, and low understanding of these threats could have significant consequences. FURTHER READING

ESTABLISHING SECURITY METRICS

One of the most important actions a security team can take is defining metrics that will measure success and drive operations. As with many cybersecurity concepts, metrics are an area going through dramatic change. In an environment where security efforts have typically 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.

Use of security metrics on the rise



Just one in five companies reports a heavy use of metrics within their security function. As expected, this usage happens most often among larger firms—26% of large enterprises report heavy use of security metrics, compared to 20% of mid-sized firms and 17% of small firms. It is actually somewhat surprising that the disparity is not even greater; given the breadth of resources that large companies have available and the ways in which they are pushing the cutting edge of security practices, one might expect more of those firms to be focused on metrics.

In fact, mid-sized firms may be the ones exploring this area in greater detail: 61% of mid-sized firms have a moderate use of security metrics, compared to 49% of large enterprises and 43% of small businesses. Mid-sized firms could be at a sweet spot for this emerging area. Although they do not have the same resource pool as a large organization, they are often more nimble, giving them more opportunity to define a new function in the business as the need arises. IT pros at mid-sized firms and solution providers that work with these firms may find a receptive environment for the introduction of security metrics.

The discussion on metrics is one that mirrors many discussions happening in IT, in that it provides an excellent opportunity to bring together many parts of the business. From the board level through different layers of management, all the way down to the people executing daily security activities, many groups have a vested interest in either setting the proper metrics or reviewing progress against established goals. Security professionals will need to be adept at communicating across various levels in order to ensure that metrics are aligning security activities with business objectives.

Organizational functions involved with metrics

	Set metrics	Review metrics
IT function	73%	57%
Some business units	43%	50%
Middle management	48%	54%
Senior executives	47%	52%
Board of directors	30%	38%

When considering which metrics to use, there are a wide variety of items companies are beginning to examine in their security practice. The most important guideline for security metrics is to make sure the metrics chosen cover all aspects of security. There should be technical metrics (such as the percent of network traffic flagged as anomalous) alongside compliance metrics (such as the number of successful audits). There should be workforce metrics (such as the percentage of employees completing security training) alongside partner metrics (such as the number of external agreements with security language). There is no perfect list that applies to every organization, but a robust set of metrics will ensure a comprehensive approach. FURTHER READING

The use of security metrics and the formation of security teams can be complementary activities. The reasons companies give for low use of metrics are the same reasons that might drive creation of a focused set of resources. Above all, companies say they simply lack the resources for metric tracking. It can be difficult to add a fine level of detail to a security function that is multitasking with other infrastructure activity. Beyond this, companies struggle to find the right level of skill for monitoring their metrics, and they lack confidence in choosing the right metrics to use. Again, a focused set of individuals or a focused third party can bring or build the right skill set, and they can also focus on tailoring a set of metrics for a vertical or a specific company.

Cybersecurity is not just a higher priority for companies today; it is a critical function that demands unique handling. The decision to form a security team may not be the right one for every company in the short term, but all signs point to security eventually becoming a concentrated discipline, with a combination of internal and external resources to set strategy, execute tactics and manage metrics. Security teams will take many forms depending on the size of a business and the specific security requirements, but the net result will be a greater specialization of skills, a broader approach to methodology, and a better connection between cybersecurity and business success.

RESEARCH METHODOLOGY

This quantitative study consisted of two online surveys. The first was fielded to workforce professionals during July/August 2018. A total of 402 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. The second, covering security metrics, was fielded to workforce professionals during May 2018. A total of 478 businesses based in the United States participated in the survey, yielding an overall margin of sampling error proxy at 95% confidence of +/- 4.6 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 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

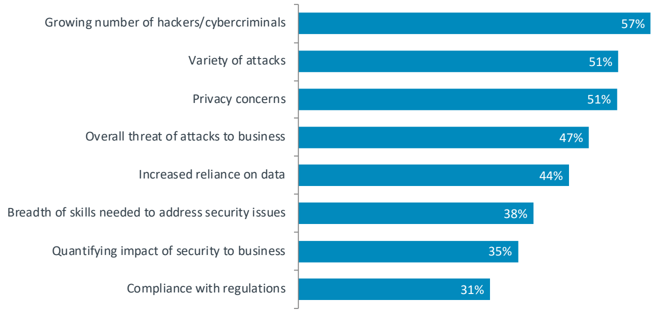
ADVOCACY

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

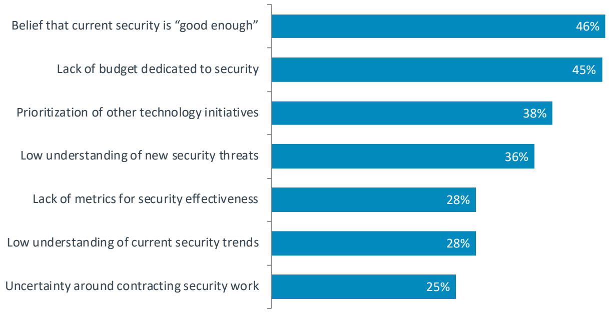
APPENDIX

Major issues driving IT security



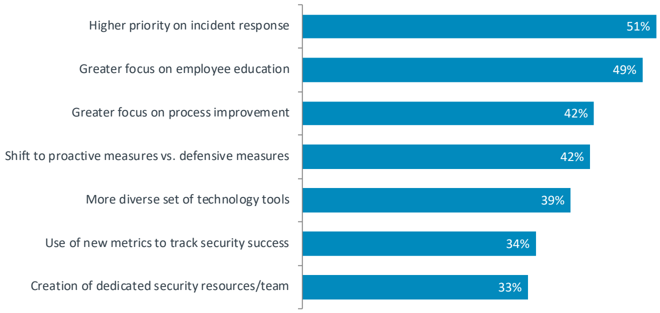
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

Hurdles for changing approach to IT security



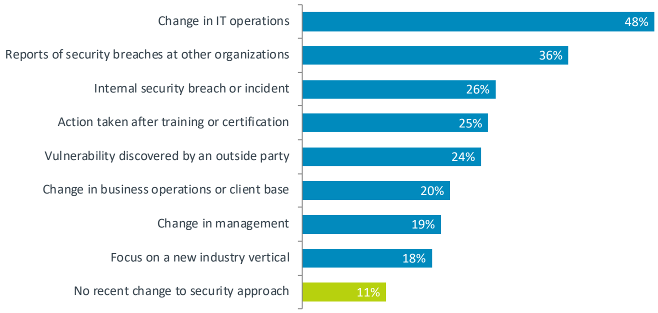
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

Many ways that IT security is changing



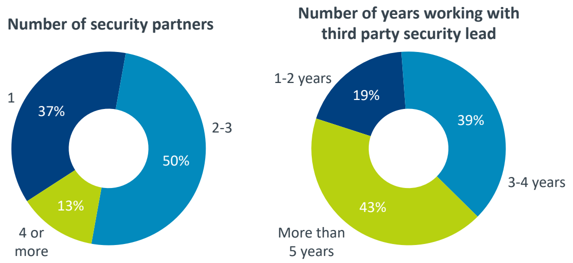
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 356 IT and business professionals in the U.S. with recent changes to cybersecurity

Drivers for changing approach to IT security



Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

Demographics of third party security partners



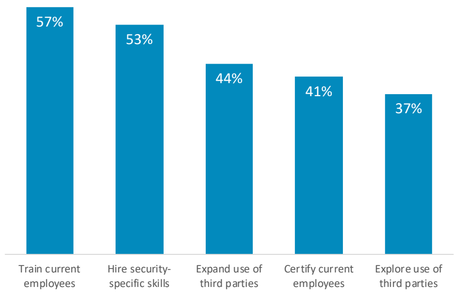
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 314 IT and business professionals in the U.S. working with third party security firms
n = 54 IT and business professionals in the U.S. working with third party security firms as center of security operations

Companies rating security skills as "current"

	Center of security operations is internal		Center of security operations is external	
	Internal	External	Internal	External
Network/infrastructure security	76%	41%	41%	80%
Compliance/operational security	74%	33%	54%	54%
Knowledge of threats/vulnerabilities	78%	42%	63%	76%
Application/data/host security	76%	36%	48%	72%
Access control/identity management	81%	28%	50%	48%
Vulnerability assessment/management	64%	45%	37%	63%
Cryptography	45%	38%	19%	46%
Incident detection/response	76%	35%	32%	79%
Security analytics	65%	44%	28%	67%
Penetration testing	51%	45%	22%	56%
Risk management	68%	39%	48%	63%
Educational ability	69%	36%	55%	51%

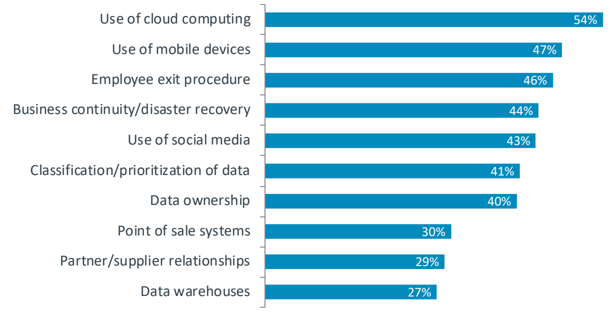
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

Options being considered for improving security skills



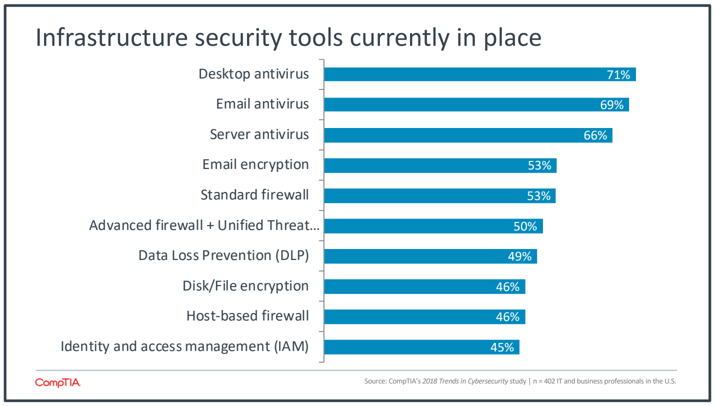
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

Areas addressed with risk management



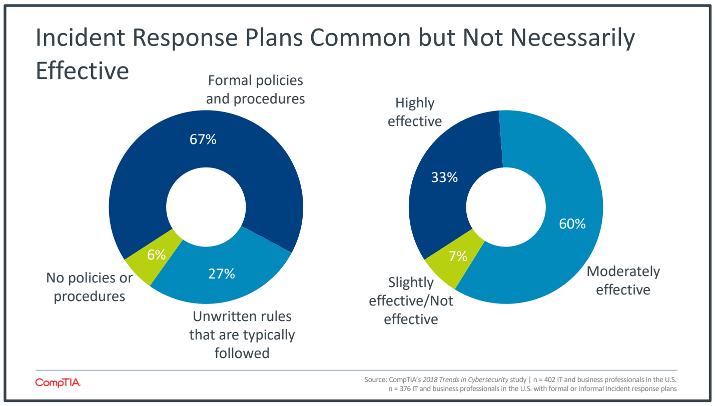
Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.

APPENDIX



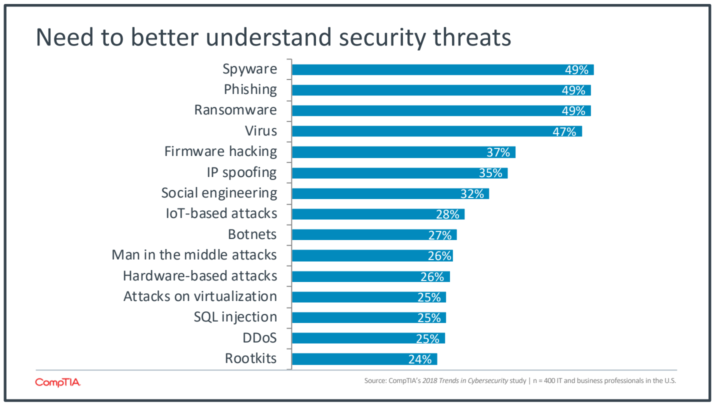
Infrastructure security tools currently in place

Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.



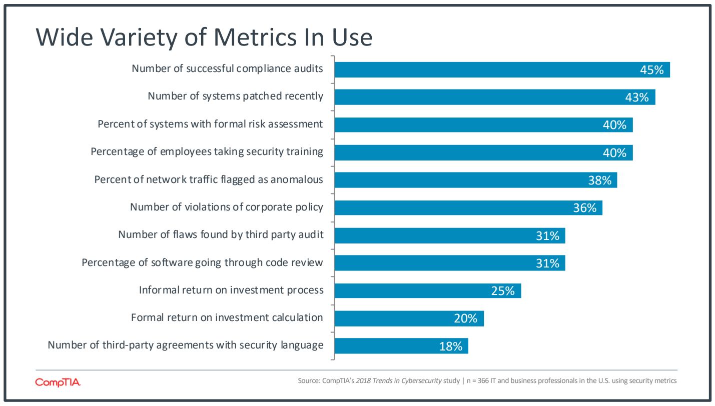
Incident Response Plans Common but Not Necessarily Effective

Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 402 IT and business professionals in the U.S.
n = 376 IT and business professionals in the U.S. with formal or informal incident response plans



Need to better understand security threats

Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 400 IT and business professionals in the U.S.



Wide Variety of Metrics In Use

Source: CompTIA's *2018 Trends in Cybersecurity* study | n = 366 IT and business professionals in the U.S. using security metrics