RESEARCH REPORT

STATE OF CYBERSECURITY 2020

September 2020

More than ever, companies are accepting that digital business is the way of the future. Regardless of the industry, offering or customer base, digital tactics are needed to survive in a dynamic and unpredictable environment. With this in mind, cybersecurity moves from a piece of IT operations into an overarching business concern. From formal policies to specialized teams, organizations are adopting the practices that will secure their new digital efforts, ultimately moving towards a new framework that defines a modern mindset. This report examines the state of cybersecurity as the world fully embraces digital transformation.

KEY POINTS

Digital operations drive new security approaches

Satisfaction with current cybersecurity efforts seems high, with 36% of companies reporting they are completely satisfied and 43% reporting that they are mostly satisfied. However, this sentiment is driven in part by an executive viewpoint, and it may not be sufficient for a function as critical as cybersecurity. The shift to remote work is driving companies to re-examine their security practices, and this examination should continue through to all parts of an IT architecture, especially those pieces that have changed in recent years.

Cybersecurity practices are becoming more formal

As cybersecurity becomes less exclusive to the IT function, the broad organization needs to consider the practices that will lead to a robust security posture. First and foremost is risk management, where companies must assess their data and their systems to determine the level of security that each component requires. Another key process is monitoring and measurement, where businesses must constantly track security efforts and build new metrics that tie security activity to business objectives. Moving forward, these formal processes will likely coalesce around the zero-trust framework, which defines a mindset around ubiquitous verification that is needed in today's distributed digital environments.

Security teams are expanding and becoming more specialized

The cybersecurity chain in a business now extends beyond the IT team to include the entire workforce, upper management, and even the board of directors. Each of these areas has specific responsibilities when it comes to cybersecurity, and creating a cohesive structure to the security discussion is a major challenge. Changes are also happening within the IT function. The complexity of cybersecurity is driving demand for a range of specialized skills, and most companies are upskilling internal resources and leveraging external firms in order to ensure the proper mix of expertise.

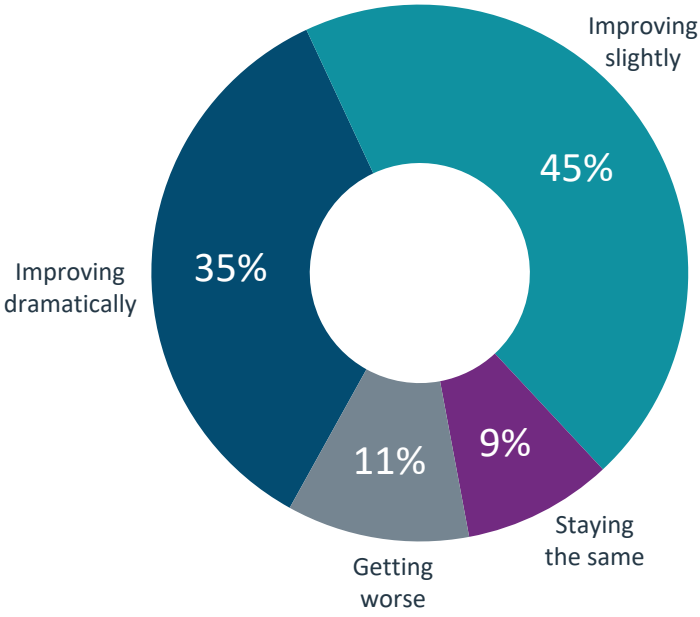
Cyber insurance is quickly becoming a business need

One of the main issues driving cybersecurity efforts is the growing impact that a breach can have on a business. As a result, cyber insurance policies are becoming par for the course, with 42% of companies currently holding a cyber insurance policy. Since this is a relatively new field, determining the appropriate coverage is a challenge. This involves not only the basic cost structure and coverage amounts, but also the initial work of determining a company's security posture and the regulatory work of determining potential impacts across state or country borders.

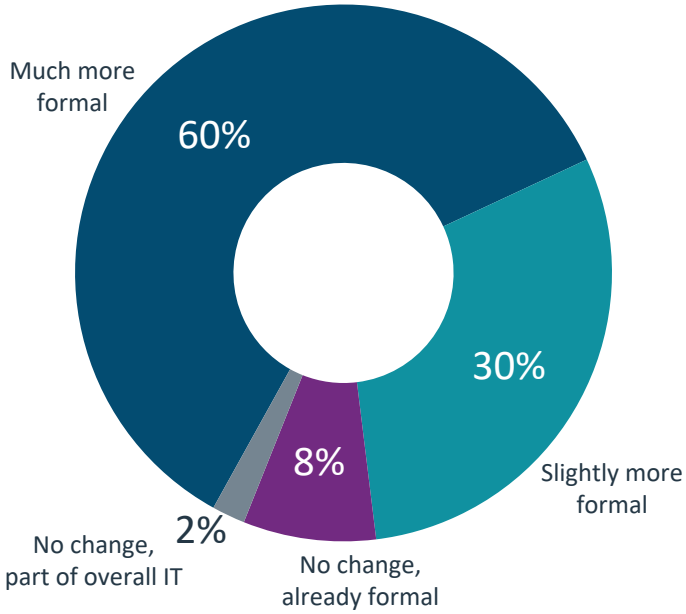
Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

1. Even with a COVID speed bump, cybersecurity has positive momentum. As with all areas of business, the COVID-19 pandemic shined a light on security practices, forcing businesses to re-evaluate their position and their investments. While remote work and new phishing attacks added new vectors to the long list of threats, companies generally feel like cybersecurity is headed in the right direction

The State of Cybersecurity



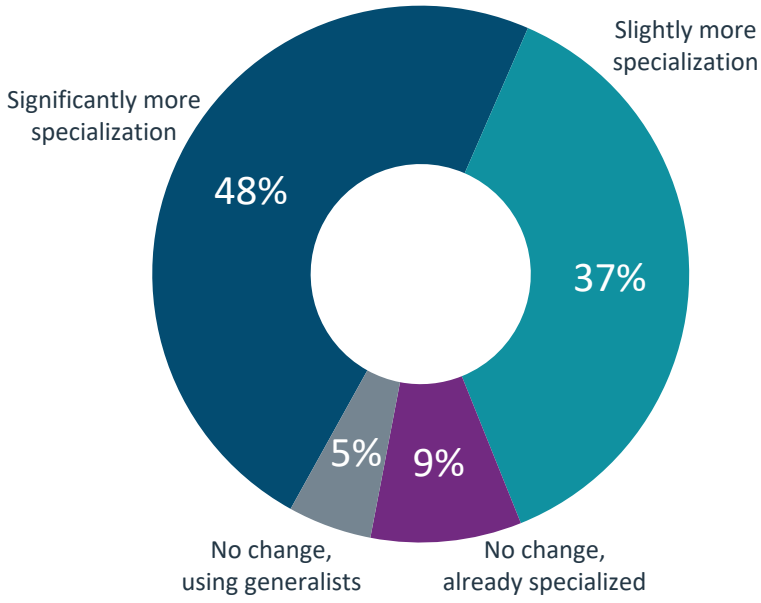
Approach to Cybersecurity Practices



2. Formal practices are bringing definition to a modern security approach. For years, there has been an understanding in the industry that security has moved away from a secure-perimeter mindset. The modern security approach has generally been defined by more advanced technology, more detailed processes, and more comprehensive education. Now, companies are formalizing their approach to areas like risk management and threat intelligence, with new frameworks emerging to structure best practices.

3. Cybersecurity personnel are becoming much more specialized. Continuing a trend that has been in place since businesses started installing CISOs, there is a major push for specialization in the field of cybersecurity. Whether companies are focusing on internal resources or outside partnerships, there is much more demand for targeted skill in threat management, proactive testing, and regulatory compliance.

Approach to Cybersecurity Personnel



Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

MARKET OVERVIEW

In 2020, digital operations took on significantly more importance as the world adjusted to the COVID-19 pandemic. At a minimum, companies sent workers home when they could and scrambled to make sure that their day-to-day workflow could continue. In many cases, there was a complete reimagining of business offerings and customer experience, and these new efforts relied on the modern paradigm of cloud and mobile infrastructure.

From a technology perspective, there were not many new innovations that companies took advantage of as they shifted into pandemic operations. The mobile technology that enabled remote work and the cloud systems that provided resiliency had been available for years. What changed was the degree of reliance on these components and the strategic shift towards using them for future strategy. This type of shift is a prime driver for new security activity, even without the underlying technology models changing dramatically.

The COVID pandemic certainly introduced new elements to the security equation. Remote work exposed vulnerabilities in workforce knowledge and connectivity. Phishing emails preyed on new health concerns rather than previous financial tactics. These elements, though, only added complexity to a fundamental problem: the nature of modern cybersecurity.

Over the past decade, CompTIA has described modern cybersecurity as a three-part problem. First, there is the traditional piece of technology, which has evolved from basic firewall and antivirus to a full toolbox of options. Second, there are processes that help maintain secure operations. Risk analysis and compliance management are examples of processes that have become more critical for most firms. Finally, there is workforce education. Human error remains the primary component of most security breaches, and the level of knowledge needed by employees has greatly increased as a result of broader technology usage.

The level of detail for each one of these areas leads to a highly complex security landscape. What was once treated as a component of IT operations has now become its own industry. One place where this is reflected is in revenue projections. While Gartner estimates that total global spending on cybersecurity will reach $123.8 billion in 2020, they break that spending down into multiple areas. Capital expense on equipment will take a hit this year due to COVID cutbacks and shifts in strategy, but other areas are set to grow, especially the area of cloud security as more companies accelerate their cloud adoption. It's also noteworthy that security services account for nearly half the total, and there are certainly a number of activities that fall into this bucket.

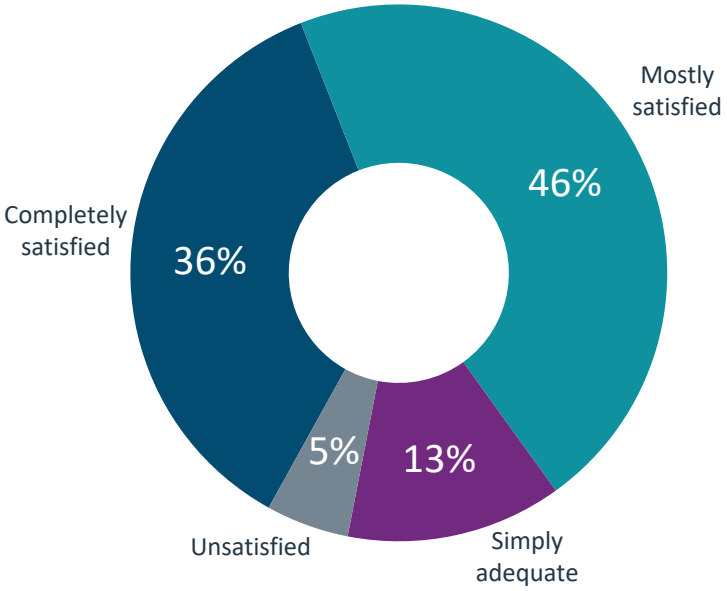
Ultimately, the question at hand is how organizations are dealing with this degree of complexity in order to protect their interests and their customers. Overall, most survey respondents feel satisfied with their company's approach, with 72% overall feeling completely satisfied or mostly satisfied. Those at the top level of a company tend to have a more positive outlook—51% of executives felt completely satisfied with their security posture, compared to 32% of IT staff and 28% of business staff. This disparity can lead to issues when it comes to attacking the problem, which will be explored in more detail later in this report.

Market	2019	2020	Growth
Application security	3,095	3,287	6.2%
Cloud security	439	585	33.3%
Data security	2,662	2,852	7.2%
Identity access management	9,837	10,409	5.8%
Infrastructure protection	16,520	17,483	5.8%
Integrated risk management	4,555	4,731	3.8%
Network security equipment	13,387	11,694	-12.6%
Other security software	2,206	2,273	3.1%
Security services	61,979	64,270	3.7%
Consumer security software	6,254	6,235	-0.3%
Total	**120,934**	**123,818**	**2.4%**

Source: Gartner | Spending amounts shown in millions of U.S. dollars

To understand the true scale of the problem, consider the importance of cybersecurity. The topic is no longer an ancillary topic within IT operations. It is a critical business function, on par with a company's financial procedures. In that light, even "mostly satisfied" is likely insufficient. As the pandemic has accelerated many technology adoption plans, it has also accelerated the tactics needed for modern security.

Satisfaction with Company's Security Posture

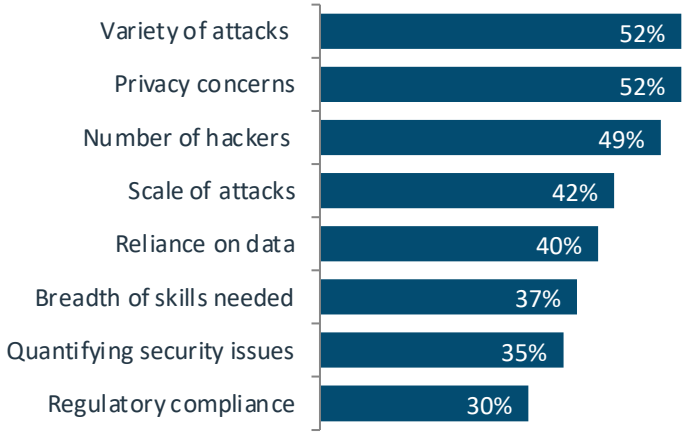


Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

THE DRIVING FORCES FOR CYBERSECURITY

When considering the overall state of cybersecurity, there are many factors that come into play. Companies may feel like things are getting worse because the number of attacks is growing, while other companies may feel like things are getting better because the ability to respond to attacks is improving. Given the complex nature of cybersecurity, it is no surprise that the list of driving factors covers a wide range of topics.

Main Issues Driving Cybersecurity



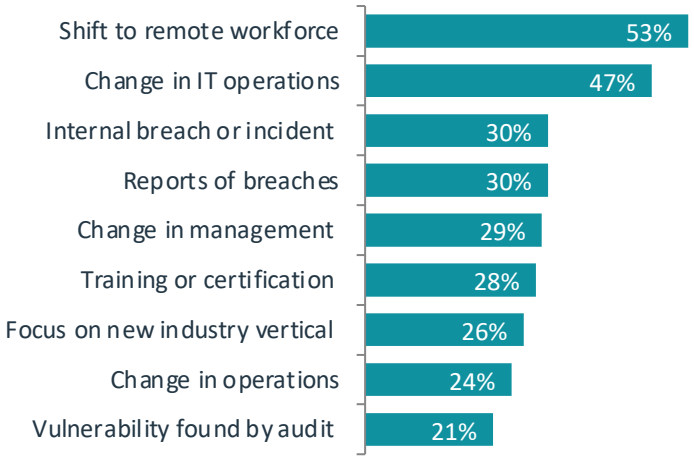
The attack landscape is certainly top of mind, with attack-related concerns taking three of the top four spots. The variety of attacks has exploded from earlier days when malware and viruses were dominant. With more opportunity for financial gain and the addition of other motivations, the number of cybercriminals has also exploded. Finally, the potential scale of cybersecurity breaches has gone from minor disruption to major threat to the business.

Privacy takes the remaining spot in the top four. There is a clear tension between protecting data and using that data to provide innovative services, and companies have to carefully consider the real needs of their business model before making decisions around privacy. Privacy concerns are likely to be a focal point of regulatory activity in the future, an area which many companies may be underestimating.

One final issue to note is the problem of quantifying security issues in relation to the overall business. Previous CompTIA research has examined the use of security metrics. When IT was a tactical activity and security was primary a defensive component, most companies used the simple metric of whether a breach had happened or not. Today, the strategic nature of cybersecurity demands more measurement, and there are several different metrics being explored by security teams, such as the number of systems with current patching, the percentage of employees that have been through training, or the number of flaws found by external audits.

Beyond the use of metrics, the strategic nature of cybersecurity is driving new approaches. As with any shift in thinking, there are barriers in the way of adopting a new mindset around cybersecurity. The top two hurdles are the belief that current cybersecurity efforts are sufficient and the prioritization of other technology initiatives. Whether by using metrics or by collaborative discussion, the goal is to get decision makers to recognize that a modern cybersecurity approach is needed in order to secure a business for the future.

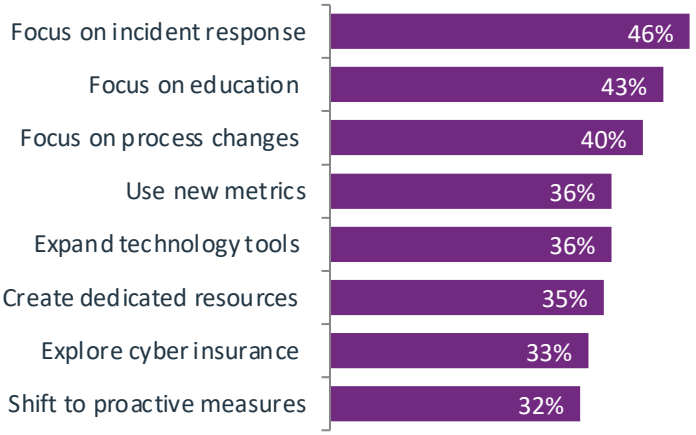
Triggers for Changing the Cybersecurity Approach



As expected, the recent shift to a remote workforce during the COVID-19 pandemic has been the primary trigger for revisiting security. While there are real security issues to consider with a remote workforce, those are only the starting point for issues created by a change in IT operations. After companies begin evaluating cybersecurity based on a remote workforce, they should be sure to continue the work by evaluating broader changes needed for expanded cloud adoption or exploration of emerging technology.

With remote workers as the primary driver, one of the primary changes to cybersecurity is naturally a focus on education. This is a continuation of the trend from the past several years of ensuring a higher level of cybersecurity awareness among the workforce. Other changes are more in line with new IT tactics, such as focusing on incident response rather than assuming incidents are being blocked and shifting to proactive measures since there is no secure perimeter. Two specific areas—process changes and dedicated resources—deserve a closer look.

Changes to the Cybersecurity Approach



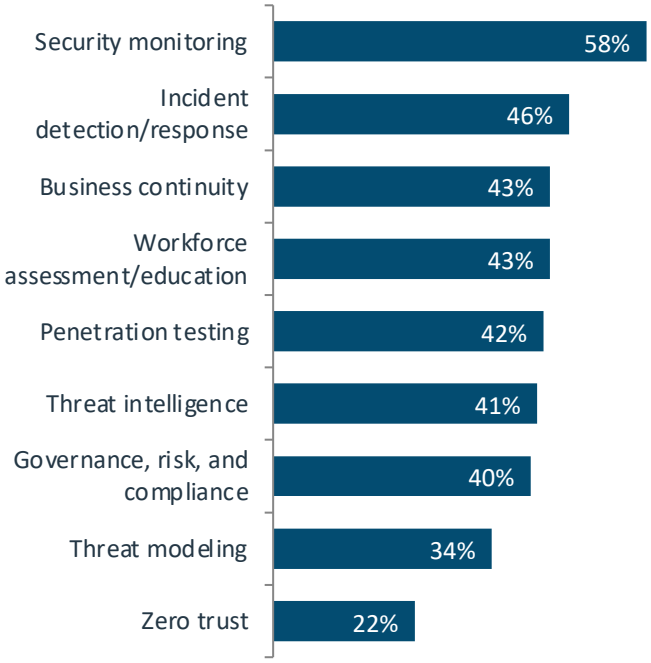
Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

BUILDING BETTER CYBERSECURITY PROCESSES

One takeaway from the main trends listed at the beginning of this report is that companies are taking cybersecurity more seriously. However, this doesn't mean that they now have security as a higher priority. For most companies, security has been a high priority for years, with cloud adoption highlighting the fact that a new approach is necessary. The recent change is that companies are starting to understand what to do about cybersecurity and are building more formal practices around this critical area.

Before diving into the most popular practices, it is worth mentioning the least popular one. A zero-trust framework is based on the concept of verifying every single access request rather than assuming that anything is safe. In a way, it adds a new twist to the secure perimeter problem; not only are activities taking place outside the perimeter, but companies should also not trust what is inside. Although comprehensive zero-trust architectures are not yet common, the framework provides an overarching approach that captures the tenets of modern security.

Cybersecurity Practices in Place



As far as individual practices go, security monitoring and analysis is definitely gaining momentum. The analysis part of the equation is the more recent addition, and companies are ramping up their efforts to analyze network behavior for anomalies, including threat hunting and the use of artificial intelligence.

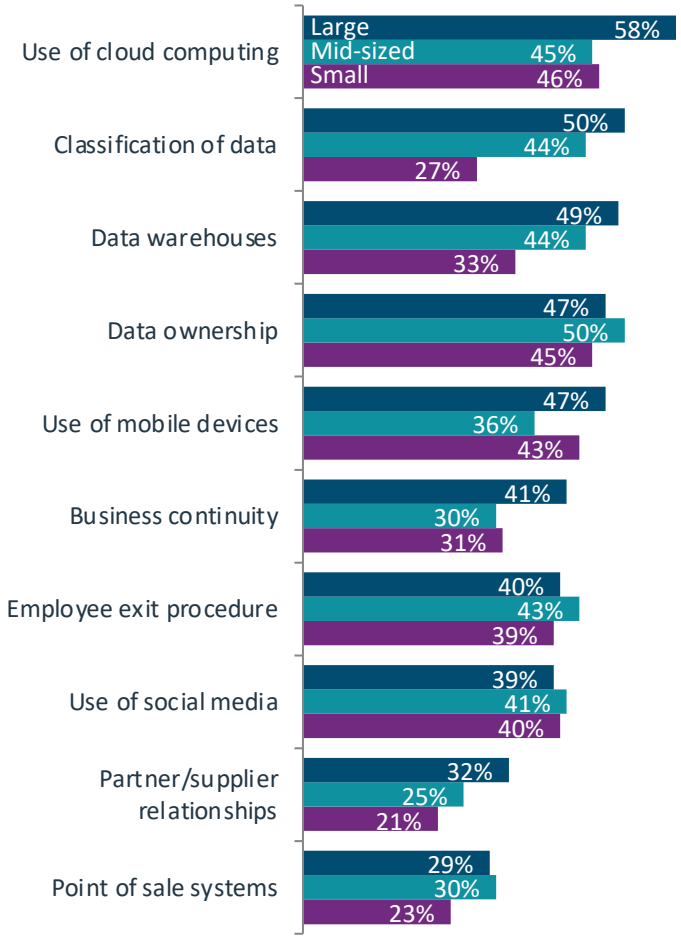
Penetration testing represents the other side of the coin. Security analytics is a more advanced take on the traditional defensive mindset, and penetration testing is the prime example of a more proactive approach. Generally speaking, companies are finding more balance between defense and offense, and penetration testing is gaining steam as a method for assessing and improving network resiliency.

Moving forward, one practice that will likely see increased adoption is governance, risk management and compliance (GRC). This is a less technical area, relying more on process knowledge and an understanding of the regulatory environment. With debate over digital regulations set to spike in the near future, it will be important to stay up to speed on the changing requirements for doing business in the future.

The risk management part of GRC is an area that is new for many businesses. Back in the secure perimeter days, companies didn't have to worry about which data carried the most risk. Everything was placed inside the secure perimeter and treated equally. Today, applications and data are essentially secured on an individual basis, and the costs of premium security for every component are prohibitive. Companies need to take a more granular approach and quantify specific risks against the costs of protection and mitigation.

Small companies are lagging their larger counterparts in several areas of risk management, but most notably in the area of data classification. This continues a historic trend of small companies underestimating the value of their data, and there is ample opportunity here for an outside expert to guide a firm through the exercise of data classification.

Areas of Focus for Risk Management



Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

THE CYBERSECURITY CHAIN

As cybersecurity becomes an organizational imperative, the burden of responsibility spreads from the IT professionals to everyone in the company. Even more so than other critical business functions, everyone has a role to play in cybersecurity since everyone is using technology to some degree in their work. The personnel involved in cybersecurity discussions now include business units, upper management, and outside firms.

Groups Involved in the Cybersecurity Chain

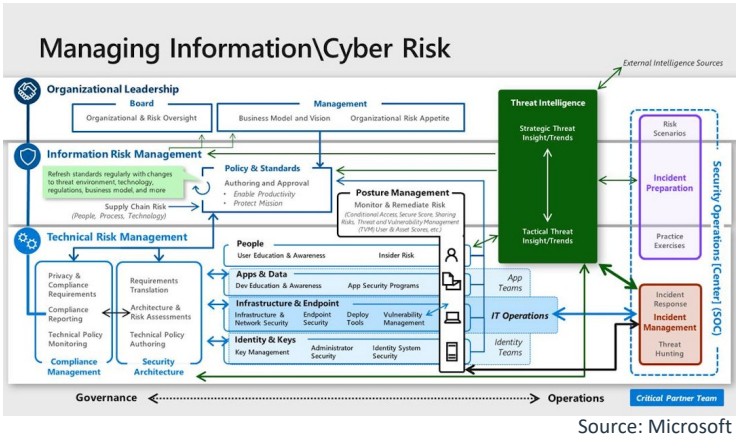
Board of Directors 20%	
CEO/Owner 37%	
Business Execs 21%	IT Execs 52%
Business Mgmt 23%	IT Mgmt 64%
Business Staff 20%	IT Staff 55%
Outside Firms 17%	

As more groups get involved with cybersecurity discussion, it is important that the discussion matches the function of each group. For example, the board of directors should not be concerned with the specific tools being used for cybersecurity. Creating the appropriate discussion throughout the organization is a prime factor in building an appropriate cybersecurity posture. Among those companies who felt completely satisfied with their security posture, 75% said that their cybersecurity discussions took the form of a comprehensive plan with clear objectives and measurable outcomes. In contrast, this view was held by only 53% of companies that were mostly satisfied with their security posture and a mere 22% of companies that felt their security posture was adequate or unsatisfactory.

Building a comprehensive plan has several challenges. For the top levels of an organization to move past the belief that "security is good enough," they must be properly educated on the nature of cybersecurity and the appropriate strategy and metrics. This requires security professionals to connect the security landscape to business objectives, including the risk of attacks, the impact of attacks, and the tradeoffs involved with mitigation.

Another challenge occurs at the lower levels, where the work is getting done. Cybersecurity has clearly moved away from being a side concern of the overall IT infrastructure plan. There is an incredible amount of complexity introduced by the shift to more proactive tactics, the changing regulatory environment, and the need to educate the entire workforce.

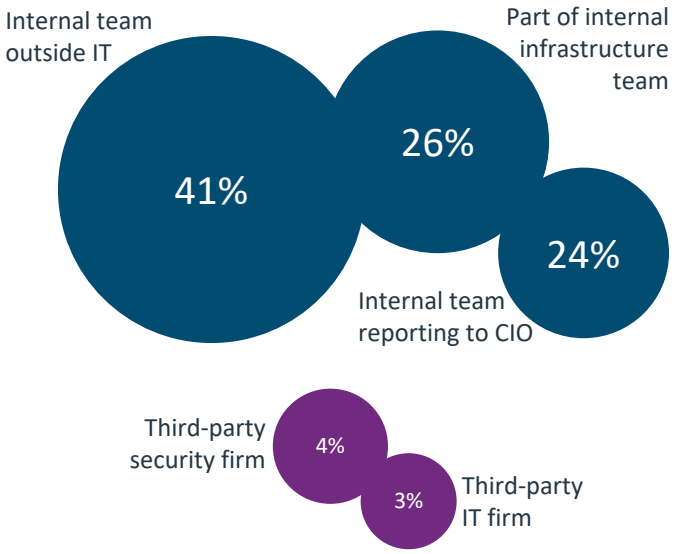
The Wide Range of Cybersecurity Functions



Source: Microsoft

With all this complexity, it is important to define a security operations center (SOC). In larger organizations, the SOC may be a robust team with many skills led by a CISO. In small organizations, it may be a single person responsible for coordinating discussions and activities with internal resources and outside partners. In rare cases, a company will use an outside firm as their SOC.

Location of Security Operations Center



Although outside firms are not common as the focal point for all security activity, they are a key component of overall security operations. Eight out of ten companies with an internal SOC also utilize external resources as part of their cybersecurity strategy. In fact, 79% of all firms that use outside resources use more than one firm for their security needs. This speaks to the high degree of specialization taking place in the security industry. Few companies have the means or the desire to build a comprehensive set of security resources. For CIOs, CISOs, and other individuals in charge of a SOC, the first order of business is determining which skills should be included in the SOC and which skills will be outsourced.

Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

BUILDING CYBERSECURITY SKILLS

With so many cybersecurity skills needed for robust operations, companies need to be methodical in their approach to skill building. The process starts with foundational knowledge. Cybersecurity specialists have traditionally come from an IT infrastructure background; while there are now direct paths into cybersecurity job roles, those paths still feature training in basic areas. Networking, server administration and endpoint devices are the top three areas that companies cite as prerequisites before pursuing specific security skills.

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 and endpoint security are examples of skills that have long been part of a security strategy. Correspondingly, most companies view those skills as relatively current among their internal resources.

Moving up the skill stack, there are some skills that have become more important as cloud and mobility have become ingrained into IT operations. Consider the examples of identity management and application security. These fall in the middle of the pack, and even then the level of skill may be overstated. In the case of identity management, a company may be handling identity on their firewall but not utilizing a comprehensive identity and access management (IAM) tool to verify identity across multiple environments.

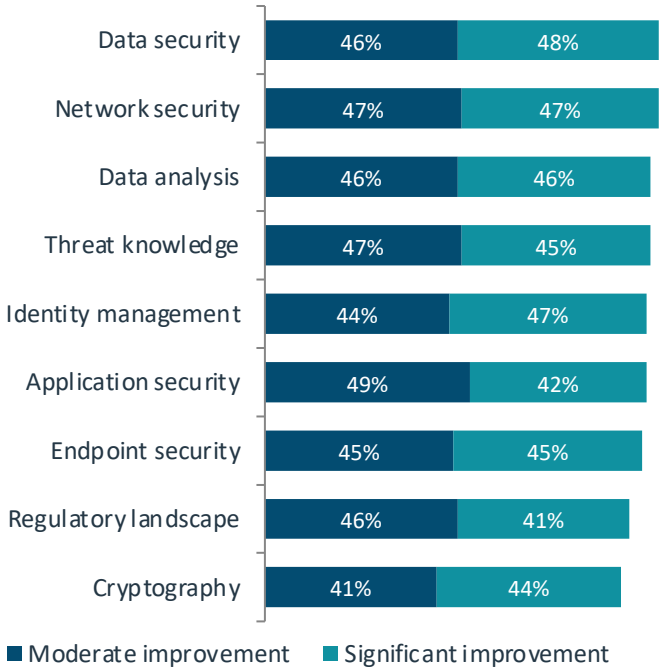
Finally, there are skills that are emerging as important parts of security monitoring and proactive tactics. Examples include data analysis, threat knowledge and the regulatory landscape. In the case of data analysis, companies are likely thinking only about more basic practices that have been in place for some time, rather than more advanced practices using massive data sets or machine learning algorithms. The other two skills fall to the bottom of the list.

Skills Viewed as Current within Internal Resources

	Small	Mid-size	Large
Data security	66%	73%	80%
Network security	68%	75%	76%
Data analysis	64%	67%	77%
Endpoint security	59%	62%	79%
Identity management	63%	68%	73%
Application security	56%	63%	74%
Threat knowledge	59%	66%	72%
Regulatory landscape	56%	67%	68%
Cryptography	43%	51%	57%

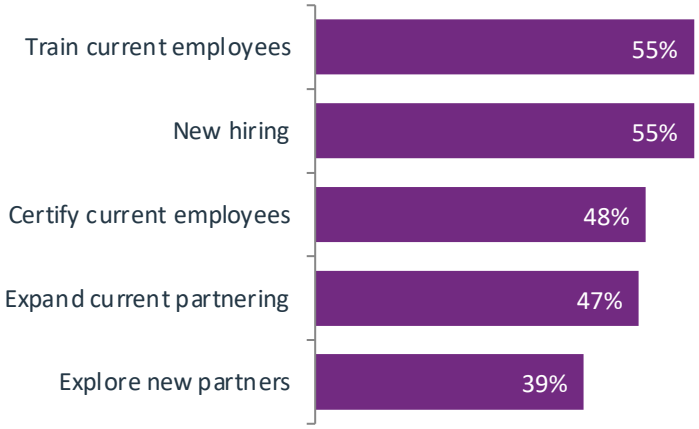
Even when companies believe that certain skills are relatively strong, there is a desire for further improvement. The consistency in the number of companies looking for significant improvement does not necessarily correlate to the current strength of that skill; rather, it is likely a statement of familiarity. Companies know more about network security, so they know exactly which areas need improvement. They know less about application security, so they simply know there's a long way to go. Across the board, the number of companies looking for significant improvement has risen substantially since CompTIA's similar research in 2018.

Improvement Needed across a Broad Set of Skills



In order to expand their skill set, companies are turning to several different tactics. The primary focus is internal, whether it is training employees, bringing new specialists on board, or certifying the current workforce. Outside partnering is a less common option, but nearly four out of ten companies still say they are exploring the use of new partners, likely expecting those partnerships to fill a specific niche.

Plans for Expanding Skills



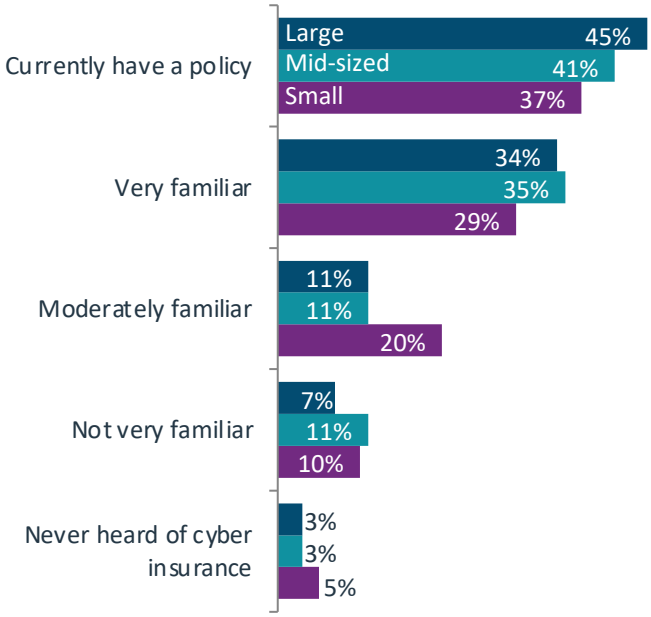
Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

CYBERSECURITY INSURANCE

One of the more recent additions to the cybersecurity toolbox is cybersecurity insurance. Cyber insurance as a concept is relatively straightforward—as with other forms of insurance, companies pay premiums to ensure protection against the downside of cyber attacks. What makes cyber insurance interesting are the circumstances driving adoption and the details of the policies.

There has always been a tangible risk to cyber attacks. What has changed recently is the inevitability of an attack. In the old way of thinking, companies felt comfortable investing in their defenses with the hope that they could keep a breach from occurring. Now, it is widely accepted that breaches cannot be avoided. The fact that breaches are commonplace takes cyber insurance past the tipping point for adoption.

Familiarity with Cyber Insurance

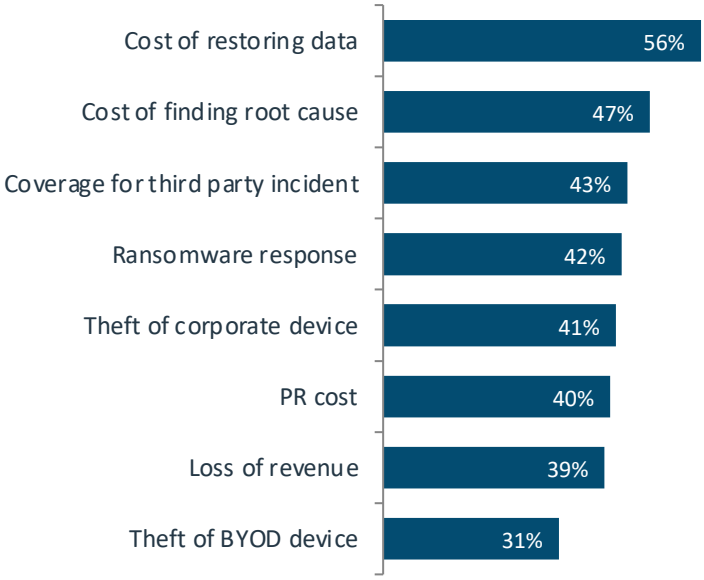


Indeed, the adoption numbers appear to be remarkably healthy. CompTIA does not have historic data on cyber insurance to provide a direct trend line, but the number of companies that currently hold a cyber insurance policy is quite high for an offering that has not been in the market very long. What's more interesting is the relative lack of disparity between companies of different sizes. Small companies used to view cybersecurity as a lower priority under the assumption that they were not a primary target. That situation has changed, and small companies appear to be taking the issue more seriously.

Deciding to procure a policy is just the first step in the journey, though. As with other types of insurance, there is no one size fits all approach, and the situation is made more confusing by the fact that cyber insurance is a relatively new field. Companies have to be prepared for an in-depth discovery phase, and they will also have to work hard to quantify an area that does not have a long history of measurements.

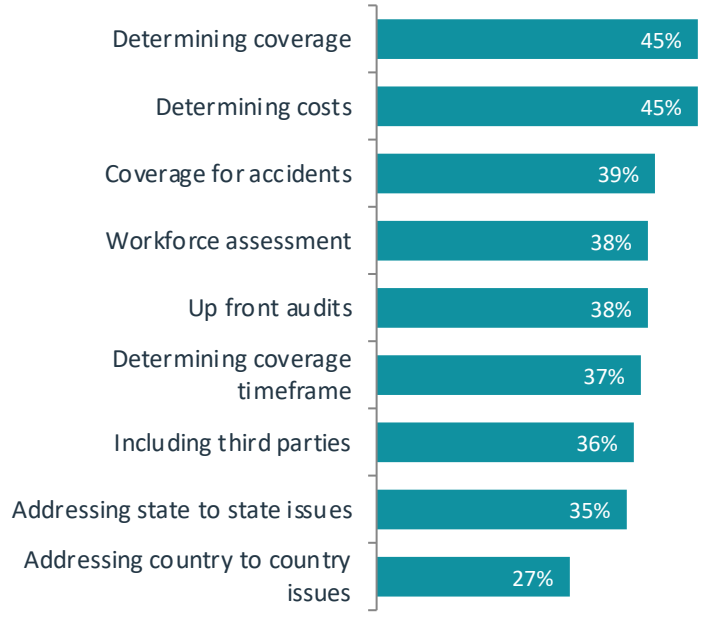
The most common coverage areas that companies consider in a policy are the areas most closely related to a security breach: restoring the data and determining what went wrong. From there, policy details depend on a holistic understanding of cybersecurity, such as knowing how third parties could lead to a security breach, or deep knowledge of breach impact, such as the loss of revenue while a breach is being repaired.

Common Areas of Cyber Insurance Coverage



Determining the specifics on coverage is only one challenge involved in building a cyber insurance policy. Another issue is the up front work of performing an audit or a workforce assessment to determine the baseline of vulnerability or awareness. Then there is also the issue of understanding the regulatory environment across state or country borders. The bottom line is that cybersecurity has become critical to business and has also grown very complicated, and new insurance policies that exist to protect against the business risk must also deal with the high degree of complexity.

Challenges in Building Cyber Insurance Policies



Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

RESEARCH METHODOLOGY

This quantitative study consisted of an online survey fielded to workforce professionals during August/September 2020. A total of 425 businesses based in the United States participated in the survey, yielding an overall margin of sampling error proxy at 95% confidence of +/- 4.9 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

LEARNING | CERTIFICATION

CompTIA is the leading provider of vendor-neutral education and skills certifications for 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 technology trends covered in this report.

CompTIA Communities

PHILANTHROPY

As the leading charity of CompTIA, Creating IT Futures is taking on the tech workforce challenge through research, program development and partnering. The foundation creates on-ramps for more people to prepare for, secure and succeed in IT careers.

Creating IT Futures

Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

APPENDIX

Hurdles for changing approach to IT security

CompTIA

Desire to Improve Threat Understanding Differs Depending on Security Satisfaction

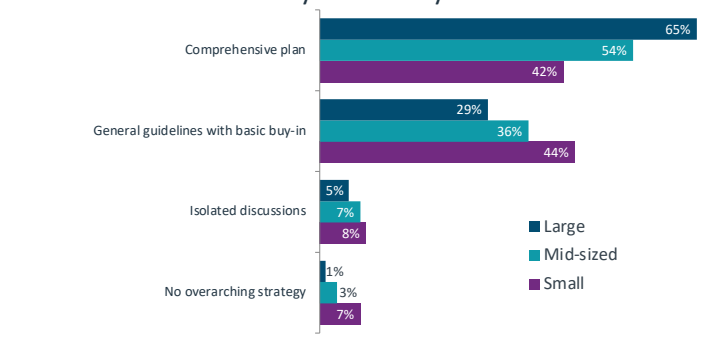
	Completely satisfactory	Mostly satisfactory	Adequate/ unsatisfactory
Viruses	47%	43%	44%
Spyware	42%	41%	47%
IP spoofing	47%	33%	35%
Firmware attacks	41%	37%	30%
Ransomware	30%	39%	39%
Phishing	29%	37%	37%
Virtualization attacks	37%	36%	28%

	Completely satisfactory	Mostly satisfactory	Adequate/ unsatisfactory
Hardware attacks	40%	28%	29%
IoT attacks	32%	27%	28%
Social engineering	32%	28%	24%
Man in the middle	32%	25%	22%
SQL injection	23%	23%	16%
DDoS	17%	18%	22%
Botnets	19%	17%	19%

Some common threats like viruses and spyware are constantly changing and require updated knowledge. Otherwise, firms that are completely satisfied may have built solid plans for threats such as ransomware or phishing, while firms that are less satisfied are feeling less prepared. With plans in place for known threats, firms that are completely satisfied can then turn their attention to more advanced threats, such as IP spoofing or hardware-based attacks.

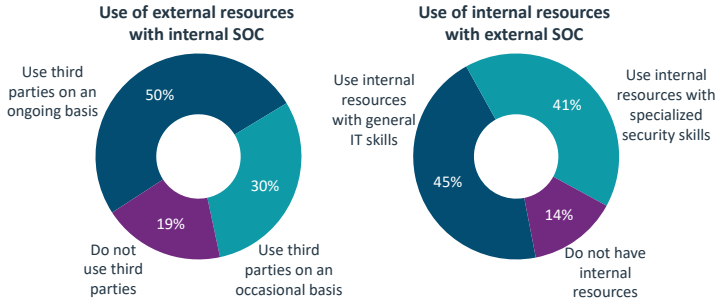
CompTIA

Nature of Discussion in Cybersecurity Chain



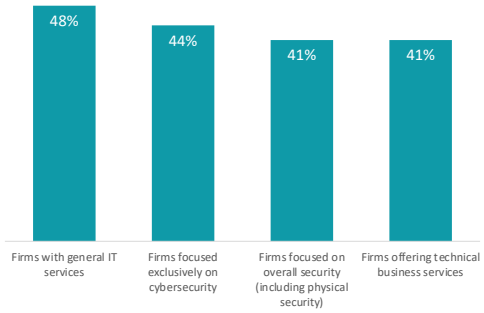
CompTIA

Most Firms Blend Internal and External Resources



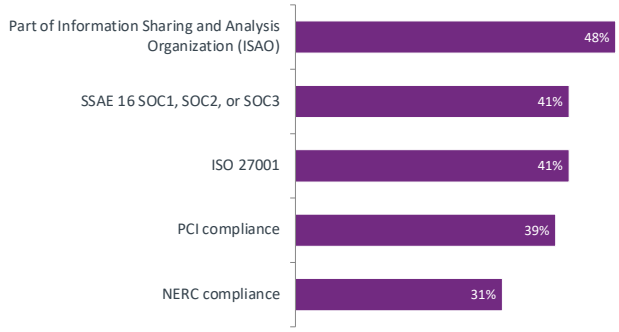
CompTIA

Types of Third Party Firms Used for Cybersecurity



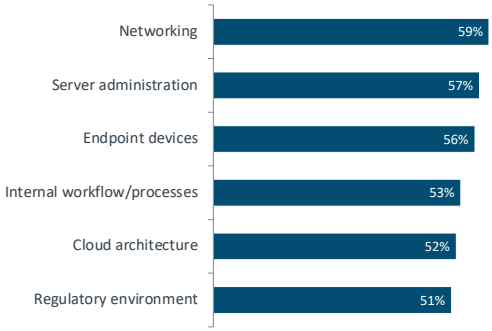
CompTIA

Typical Third Party Credentials/Affiliations



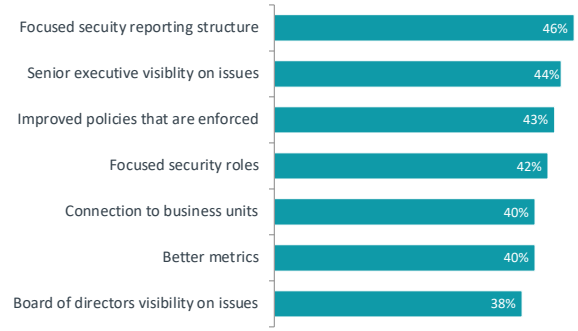
CompTIA

Prerequisite Knowledge for Cybersecurity Roles



CompTIA

Actions to Improve Effectiveness of Security Resources



CompTIA

Copyright (c) 2020 CompTIA Properties, LLC, All Rights Reserved | CompTIA.org | research@comptia.org

CompTIA