CompTIA

RESEARCH REPORT

2021 State of Cybersecurity

September 2021

Introduction

One of the hallmarks of our digital age is the rapid pace of change. The ability to procure core technology components at lower costs and the ability to connect individuals around the globe have dramatically accelerated the capacity for innovation, and there is often a sense that businesses need to constantly adapt or face irrelevance.

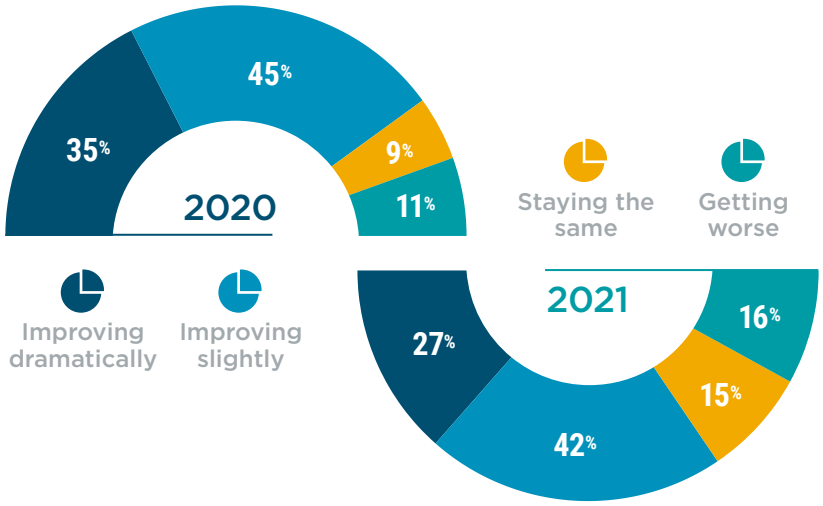
In the middle of all this technological turbulence, it can be easy to miss how slowly many business functions are changing. In short, the capacity for innovation exceeds the capacity for adaptation. New technology can change the world…in theory. In practice, there are decades of business process and learned behavior that must change to take advantage of all the new toys.

Nowhere is this more apparent than the field of cybersecurity. CompTIA's 2020 State of Cybersecurity report described how cybersecurity has become a business imperative, something as important to the long-term success of an organization as finances or legal practices. Given this high priority, a quick response seems appropriate, but instead companies appear to be stuck.

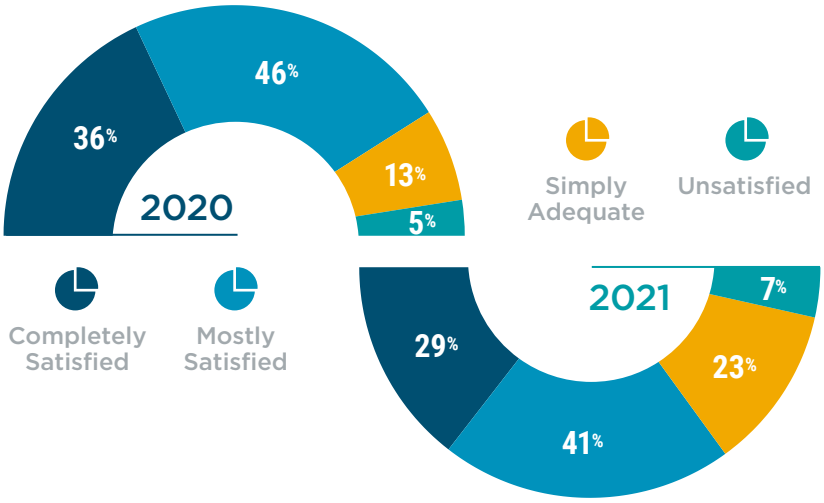
Two pieces of data provide a high-level look at the problem. To start, people feel that the general state of cybersecurity in the economy is getting worse. In 2020, 80% of individuals in CompTIA's study felt like the state of cybersecurity was improving. In 2021, only 69% feel the same. Prolonged pandemic uncertainty, ransomware attacks on critical infrastructure, and supply chain attacks rippling through the business landscape were all likely contributors to a more pessimistic sentiment.

At the same time, there is less satisfaction with corporate strategies. In 2020, 82% of employees felt satisfied with their company's approach to cybersecurity. In 2021, that number dropped to 70%. Given everything happening on the world stage, practices that were previously considered good enough might not be cutting it anymore.

The State of Cybersecurity



Satisfaction with Company's Cybersecurity



There's no question that cybersecurity is a complex problem, so there's no surprise that companies are struggling to build complex solutions. One of the biggest complications is that modern security requires a completely different mindset, with IT taking on strategic significance and cloud computing undoing the traditional notion of a secure perimeter. CompTIA's 2021 State of Cybersecurity study provides a holistic view of cybersecurity strategies and outlines the tactics needed to quickly bring a cybersecurity practice up to speed.

Trends to Watch 2021

1 Policy

Zero trust becomes the guiding principle for cybersecurity

2 Process

Cybersecurity goes both deep and wide

3 People

Companies build expansive cybersecurity teams

4 Product

The cybersecurity toolbox grows to match tactics

Market Overview

Cybersecurity Threat Statistics

$4.24 million

Average cost of a data breach[1]

287

Average number of days to identify and contain a data breach[2]

350K

Number of new malware programs found per day[3]

18K

Number of Solarwinds customers affected by supply chain breach[4]

$1.85 million

Average cost of remediating ransomware attack[5]

74%

U.S. companies experiencing successful phishing attack in 2020[6]

Why has cybersecurity become a top priority for businesses? The numbers tell the tale. To start, the threat landscape continues to grow in the volume of attacks that occur daily and the variety of methods used by cybercriminals. Attacks are coming at a ferocious pace, and a single data breach could cost a company millions of dollars along with massive amounts of time. Of course, the ultimate threat is a ruined reputation that can damage business prospects for years to come.

As much as malware and viruses are still a concern, new types of attacks are exploiting other holes in a defensive strategy. Thanks to the headlines made by Solarwinds in late 2020 and Kaseya more recently, supply chain attacks are now a common part of the cybersecurity lexicon. These attacks, where hackers insert malicious code into software at an early stage before it goes out to customers, are not only difficult to detect since the software is coming from a trusted source but also grow exponentially as the software grants access to the customers of the customers.

While supply chain attacks are the hot new item, ransomware continues its run as a powerful cyberweapon. Ransomware attacks on Colonial Pipeline and JBS Foods have raised awareness that aggressive tactics between nations are no longer limited to planes and tanks. Targeting the IT systems of critical infrastructure is just as effective in doing damage, and the same methods are used by hackers hoping to extort money from corporations.

Finally, the weakest link in cybersecurity continues to be humans. Rather than using purely technical methods to crack into a business, hackers use social engineering tactics such as phishing to get information from unwitting employees. These attacks prey on the soft spots of human psychology, and an event such as a global pandemic makes those soft spots even more pronounced.

The other set of numbers that describes the scope and scale of cybersecurity is the data around spending. For 2020, Gartner originally projected that cybersecurity spending across a range of topics would reach nearly $124 billion by the end of the year, representing a 2.4% increase over 2019. In reality, cybersecurity spending surpassed $133 million, representing a 10.6% increase. For 2021, Gartner clearly expects that momentum to continue.

Cybersecurity Spending Projections[7]

Market	2020	2021	Growth
Application security	3,333	3,738	12.2%
Cloud security	595	841	41.2%
Data security	2,981	3,505	17.5%
Identity access management	12,036	13,917	15.6%
Infrastructure protection	20,462	23,903	16.8%
Integrated risk management	4,859	5,473	12.6%
Network security equipment	15,626	17,020	8.9%
Other security software	2,306	2,527	9.6%
Security services	65,070	72,497	11.4%
Consumer security software	6,507	6,990	7.4%
Total	**133,776**	**150,409**	**12.4%**

To some extent, the increase in spending reflects a post-pandemic reality. The most dramatic growth comes in the area of cloud security. While this is partly due to the fact that cloud security has the smallest 2020 base spending, it is also a sign of companies shifting to a cloud-first mentality for IT architecture.

However, there is more to the spending story than just ripple effects from the pandemic. Spending is significantly higher across the board, including areas such as network security equipment, which does not necessarily fit into the narrative of a shift to remote work. Even areas such as security services and infrastructure protection, which have the largest 2020 base spending amounts, are projected for double digit growth.

Main Issues Driving Cybersecurity

As companies consider their response to the threat landscape and the investments they will make, they are considering a wide range of issues. The volume and variety of attacks are top of mind. Next, they are concerned about guarding their customers' privacy. From there, they are dealing with a growing reliance on data for business operations, the ability to quantify cybersecurity efforts to justify investments, and the different types of skills needed for success. In fact, companies may be underestimating many of these issues—regulatory compliance in particular is likely to be a major challenge moving forward.

The common theme running through the cybersecurity market is complexity. In large part, this is driven by IT systems becoming more complex. The stabilization of the fundamental computing platform has given rise to myriad solutions, many of which are starting to incorporate emerging technology. Beyond IT architecture, cybersecurity now has many additional facets, such as risk management and user education.

A complex problem requires a methodical solution. As companies separate cybersecurity from overall IT operations, they can find success by structuring their approach around four elements: the policies that guide cybersecurity decisions, the processes required to maintain a strong posture, the people responsible for cybersecurity outcomes, and the products that protect digital assets.

1 Policy

In the broadest sense, cybersecurity policy refers to the overall strategy that informs future decisions and investments. In many companies, parts of this policy may be laid out in formal documentation. Beyond any official statements, though, policy is primarily a cultural mindset. This mindset demonstrates understanding of the current business climate, and it drives awareness and action around the best ways to safeguard the organization.

For most of computing history, this mindset centered around two concepts. First, the approach was defensive. Under the assumption that threats were coming from the outside and could be identified, companies took a defensive posture, aiming to keep anything bad from getting in. The second concept was the secure perimeter. Along with the assumption that threats originated outside the company, the concept of the secure perimeter was rooted in logistical infrastructure. For many years, companies operated from defined physical locations, with computing equipment and work tasks rarely leaving the walls of the office.

The secure perimeter was the first concept to start eroding. Over time, organizations equipped their workforce with laptops and other mobile devices for the sake of productivity. The shift to cloud computing accelerated the demise of the secure perimeter, as companies needed to secure applications and data that were hosted on public infrastructure.

The shift away from defense and toward proactive measures has been slower. It has been difficult for businesses to grasp the full nature of cybersecurity threats, where bad actors can attack using a variety of methods and find ways to occupy corporate networks while remaining undetected. Building a strong defense and constantly testing that defense for vulnerabilities sounds like twice as much work, and in fact it is. An increased reliance on digital components implies an increased cost in secure operations.

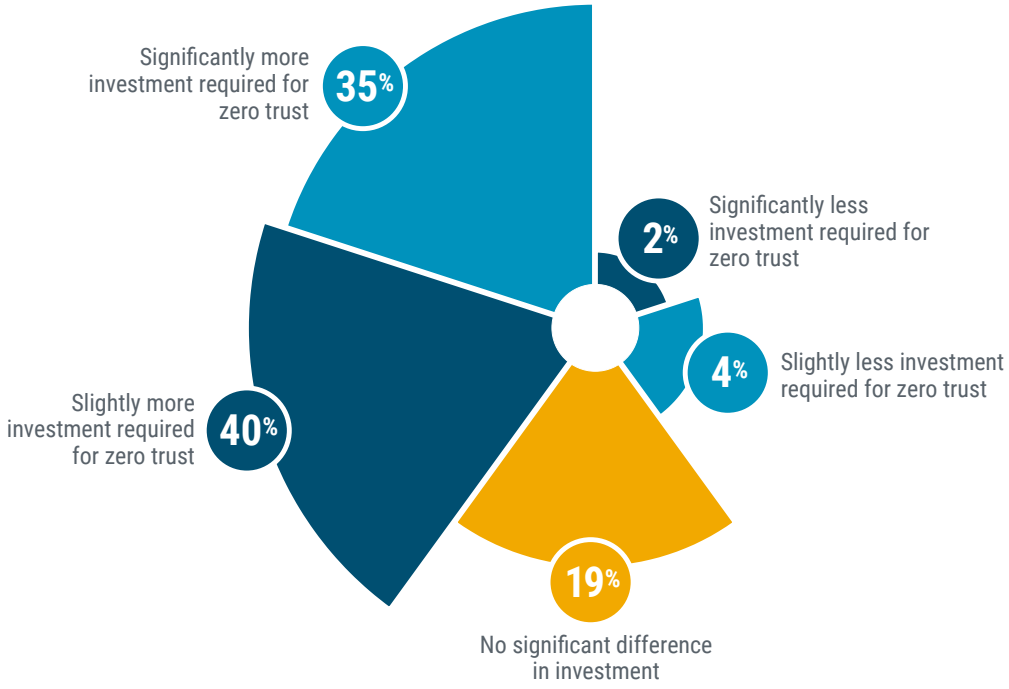
The new mindset that has emerged in response to digital transformation is zero trust. For all the IT trends that have loosely described the underlying solutions, zero trust is exactly what it says it is. Rather than assuming that network traffic or user access is harmless due to origin or credentials, further verification is required at every step.

Components of Zero Trust Framework

The NIST publication on zero trust architecture states that zero trust "is not a single architecture but a set of guiding principles for workflow, system design and operations." (NIST Special Publication 800-207.)[8] These guiding principles are leading organizations toward several common practices. Multifactor authentication reduces reliance on a single set of credentials. Network analytics unearth malicious behavior that may not be apparent. Microsegmentation provides granular control of traffic so that targeted security policies can be applied. None of these stand out as a single best practice for zero trust, but all of them working together provide robust protection.

As with the shift to proactive security measures, a zero trust policy is likely to be a more expensive approach. Among the companies in CompTIA's survey currently pursuing a zero trust architecture, three-fourths have found that more investment is required for zero trust than for their previous initiatives. As the landscape is constantly changing, there is no magic number around proper spend for cybersecurity. In fact, cybersecurity spending may be very difficult for companies to quantify, as security considerations become woven into most operational decisions. The bottom line is that the proper measures require careful investment—not only from a financial perspective, but also from the perspective of internal resources and time.

Investment Required for Zero Trust Framework



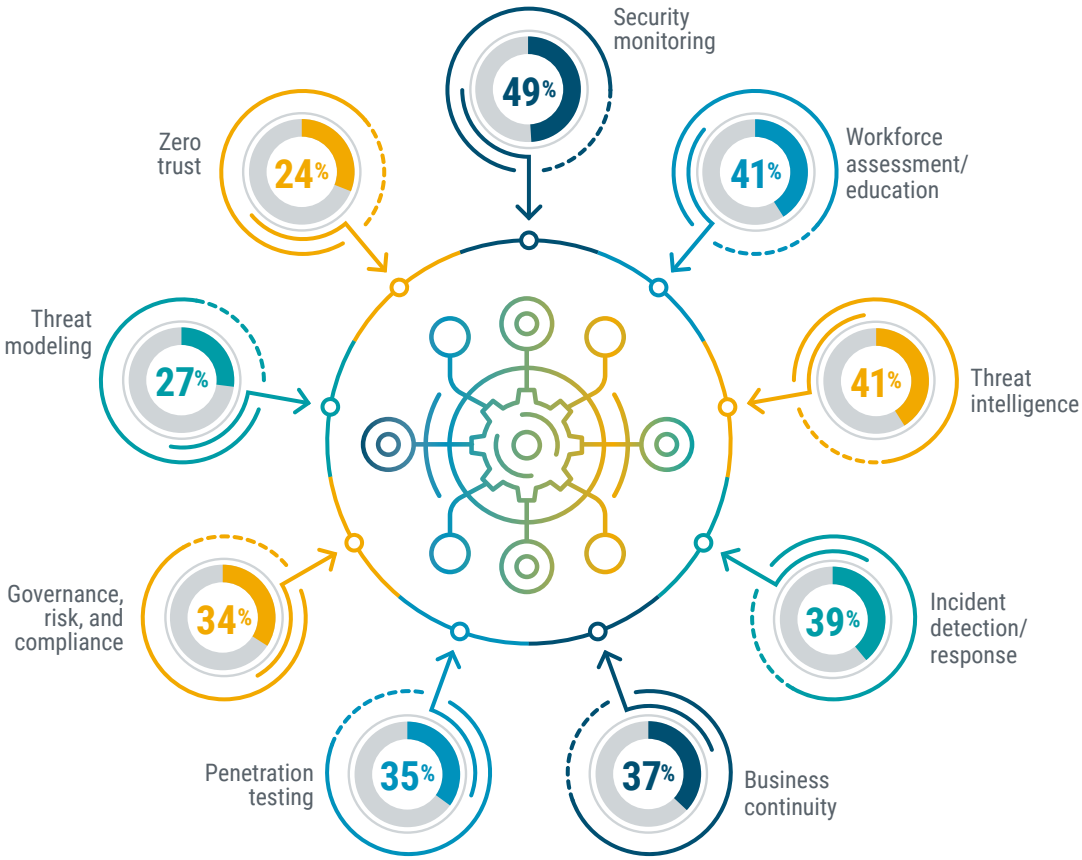
Beyond zero trust, there is another emerging component in modern cybersecurity policy. Edge computing is most often viewed as an alternative to cloud systems for application architecture. Edge systems can store data or perform calculations closer to the source, reducing bandwidth demands or latency issues. From a cybersecurity perspective, edge computing carries a slightly different connotation.

As IT systems grow in complexity, companies are using a broader range of outside firms for their architectural needs. This starts with cloud providers but extends to companies providing services such as content delivery or overlay networking (examples include CloudFlare or NetFoundry). By utilizing these edge companies as part of their architectural stack, organizations are also gaining cybersecurity benefits that are baked into the offerings, such as DDoS mitigation or microsegmentation. The cybersecurity benefits may not be the first reason that businesses use these outside firms, but they end up being part of the overall solution.

2 Process

The process of cybersecurity is where the rubber meets the road. After building an understanding of policy, an organization then has to decide how that policy will be implemented. With cybersecurity now touching so many different areas of a business, there are countless individual practices that go into this implementation phase.

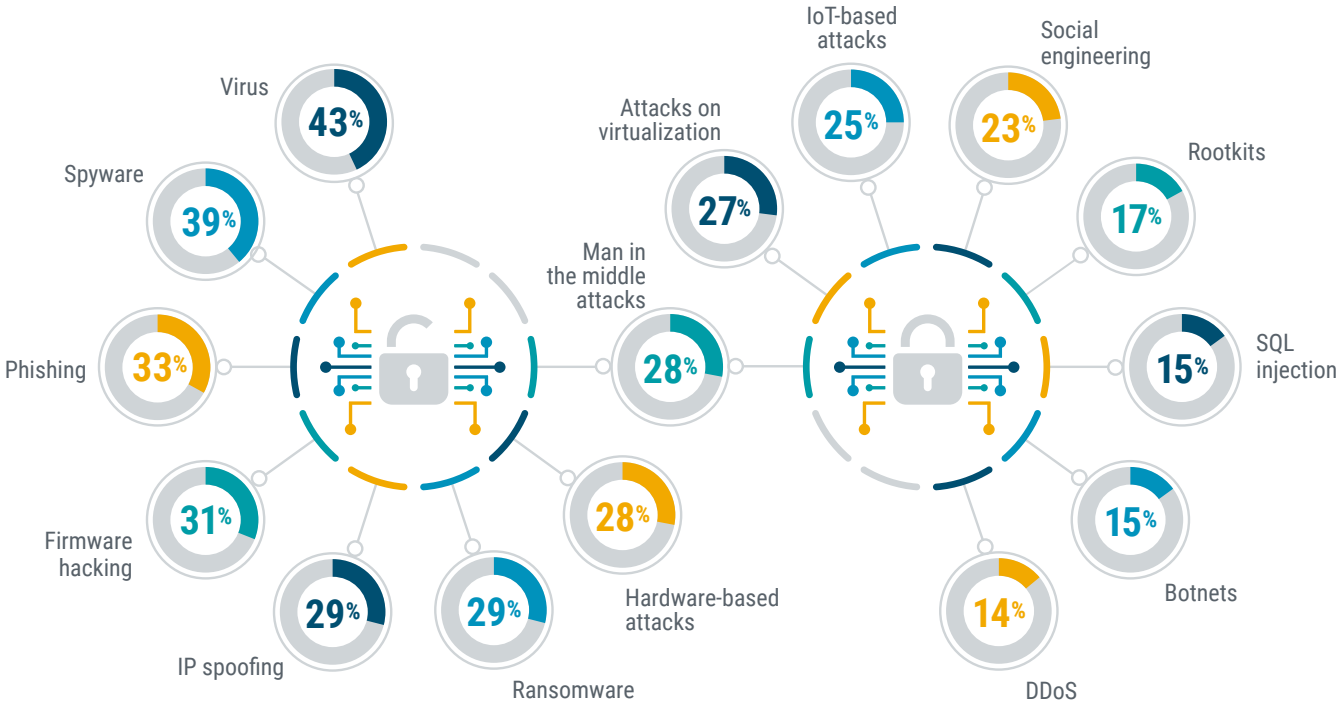
Cybersecurity Practices in Place



The most common cybersecurity practice is monitoring for cybersecurity incidents, which seems self-explanatory. However, this practice also includes analysis of network traffic attack patterns, which is where things get interesting. Simply monitoring for incidents is largely a static activity, where monitoring tools are configured around known attack types and programmed to send notifications when those attacks are detected. Analysis is a more advanced, more proactive initiative. It requires both an understanding of typical network behavior and also an understanding of attack methodology, so that any anomalies can be investigated as potential infections.

Workforce assessment and education has been growing more popular over the past several years. The driver for this practice is the ubiquity of digital tools throughout the entire workforce. In the past, tools such as laptops and smartphones were only used by specific types of workers. Digital transformation has opened the door for most workers to have access to corporate systems or job-specific applications. In addition, the average employee uses technology in their personal life on a daily basis, and consumer-level behavior is typically less aware of security than enterprise-level behavior. Assessments determine the areas having the biggest impact on corporate safety, and targeted education packages with accompanying metrics help improve the situation.

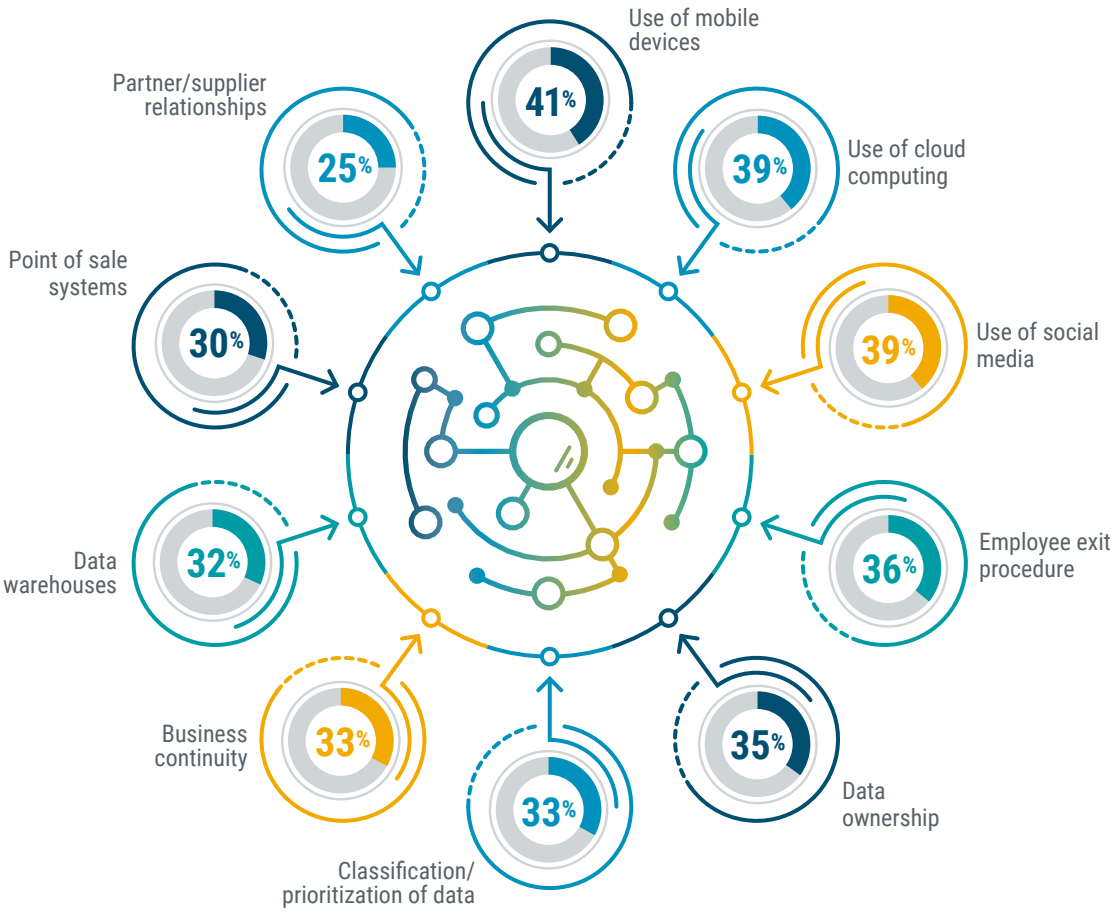
Need to Improve Threat Understanding



Threat intelligence typically refers to a data-driven practice that provides insight into the attacks occurring on corporate systems. As with security monitoring, there are many possible layers to threat intelligence, starting with basic knowledge about the types of attacks occurring across the entire business landscape. As digital business practices have evolved, there has been an explosion in the different ways of disrupting business flow and monetizing this disruption. Most companies still gravitate toward the most traditional threats, wanting to improve knowledge around viruses or malware. While new variants of these attacks can certainly exploit latent vulnerabilities, other attacks target changes in IT practices. Some of these practices are older but growing in popularity (like virtualization), and some practices employ emerging techniques (like internet of things).

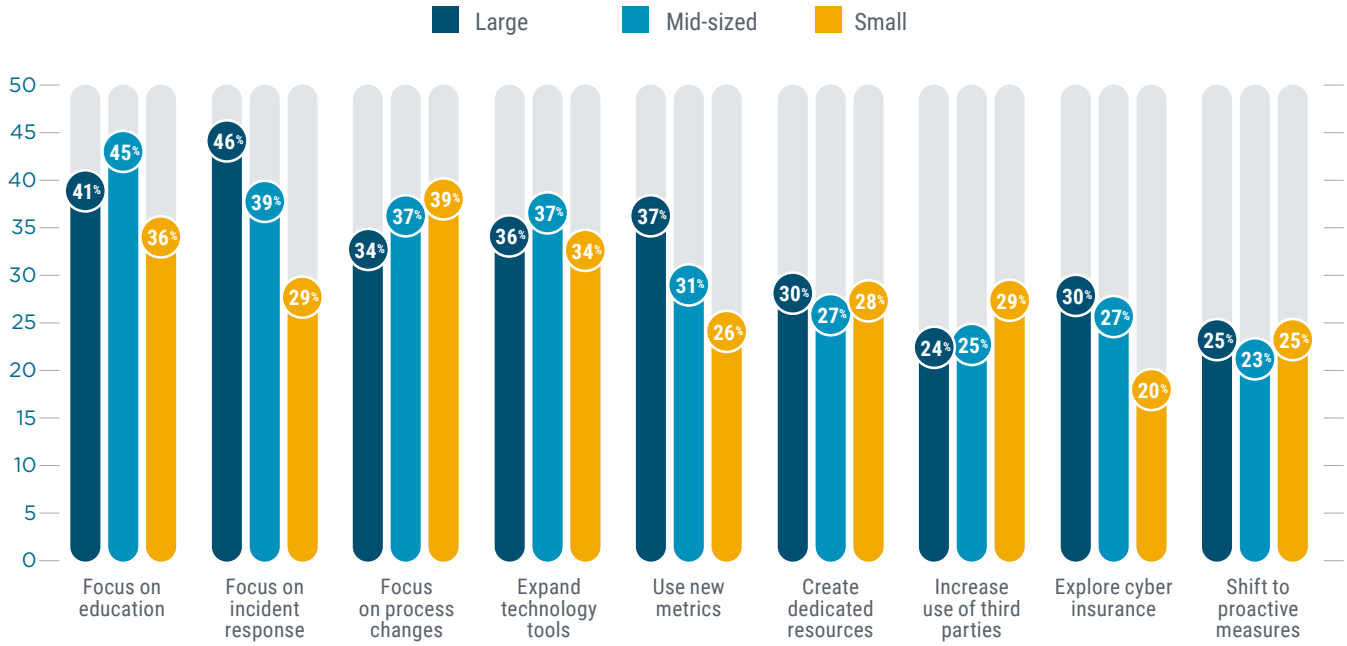
Beyond a broad knowledge of the many different types of attacks, threat intelligence is a leading example of the need to build formal processes in order to manage complexity. A threat intelligence process starts with collecting data—both data from an internal network and data from external sources. This data all needs to be processed just like any other business data flow, placing the information into an organized scheme and filtering out any redundant or unnecessary information. Automation and data analysis techniques help make sense of the processed data, then mitigation plans and feedback loops inform the next set of actions.

Components of Risk Management



Risk management is another example of a process that has become more formal in recent years. Many companies are combining risk management with regulatory awareness, forming teams or specialists in governance, risk, and compliance (GRC). Even companies that are not combining these disciplines should have a structured approach to risk management. In many cases, risk analysis examines the trade-off between convenience and security. For example, mobile devices and cloud computing can greatly enhance productivity, but they also create new vulnerabilities. Perfect security is usually not achievable or affordable, so the level of risk must be assessed before a business decision is even made.

Changes to Cybersecurity Approach



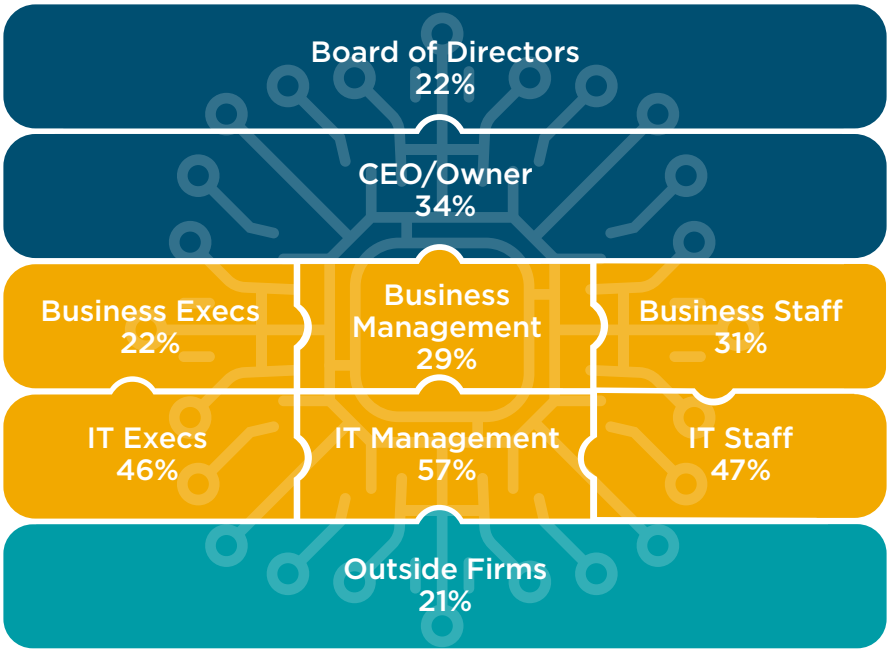
With so many different practices to consider, it is difficult to build depth in every area. This is especially true for small firms (those with less than 100 employees). Small firms lag behind their larger counterparts in four key areas. There is less focus on education, though there are admittedly fewer employees to educate. There is far less focus on incident response, which is likely a holdover from the days of believing that cybersecurity was less of a concern since small companies held fewer assets. Small companies are less likely to apply metrics to the cybersecurity situation, compounding the problem of understanding cybersecurity effectiveness. Finally, cyber insurance is being explored by fewer small companies.

Even for large companies, maintaining both breadth and depth in cybersecurity processes is a major challenge. The old method of a static, secure perimeter was a relatively simple one to maintain, often being treated as a side component of the general IT function. Today's processes require specialization in the technical workforce and security-first thinking in the overall workforce. Unless there is buy-in throughout the organization, the process of security will break down, leaving the business exposed.

3 People

The notion of cybersecurity personnel has expanded along with the processes used for implementation. Just as the process was once a simplistic secure perimeter and now touches every part of the organization, cybersecurity responsibility has grown from isolated skills into company-wide awareness. Obviously not every employee within an organization needs to have deep expertise, but there are key points to consider since so many groups are involved.

Groups Involved in Cybersecurity Chain

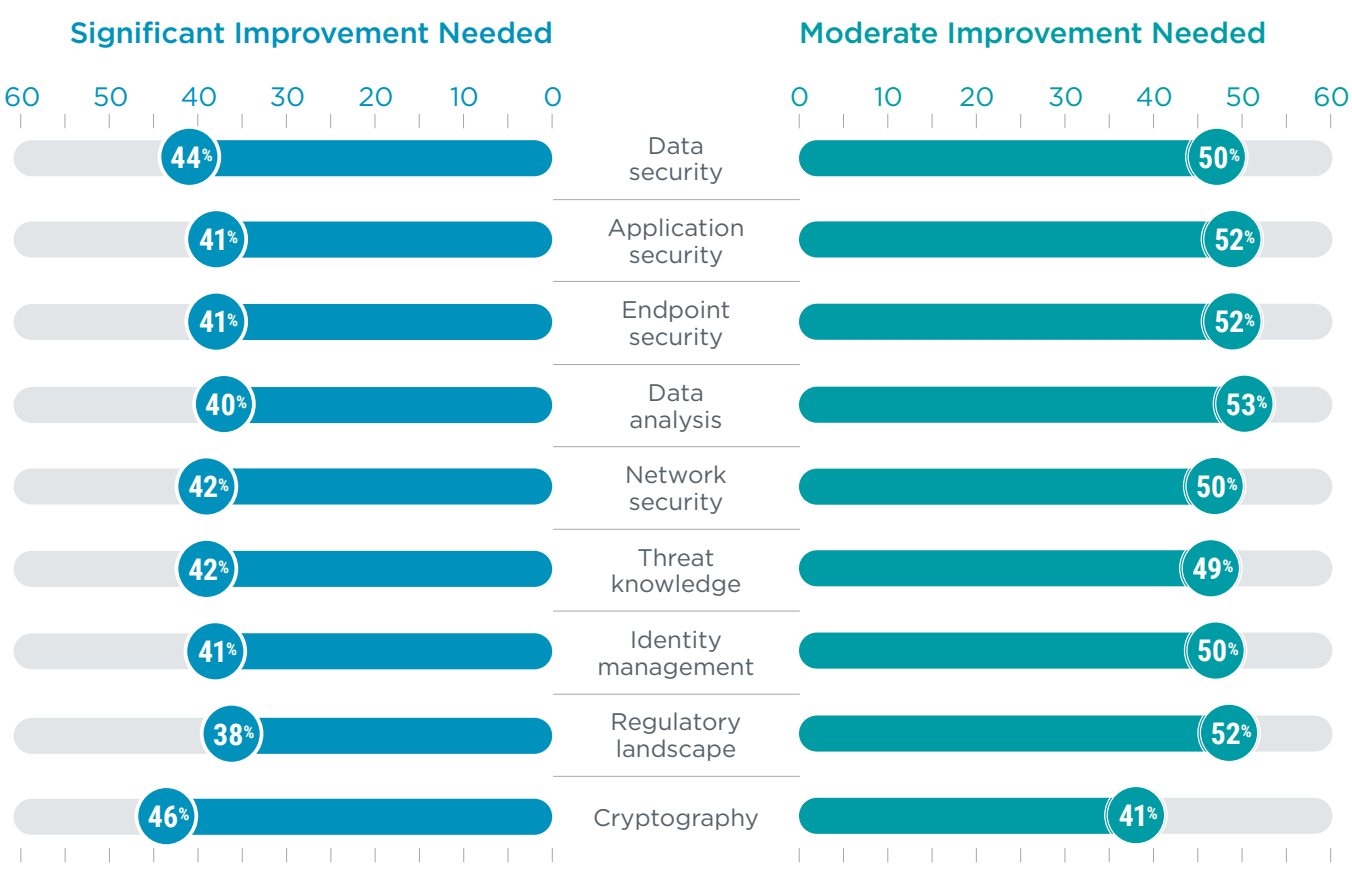


First, the discussions need to be appropriate for the audience. The board of directors is not generally interested in the day-to-day tactics of the IT staff. There needs to be a translation between everyday activity and overall strategy, and it is up to executives and management to define the metrics that align with business interests and then perform the translation. Second, there needs to be a common thread that ties all the discussions together. Improving internal datacenter security may help reduce risk, but it may not address a shift to cloud providers that helps improve flexibility.

Managing the cybersecurity vision is the role of a security operations center (SOC). Since the cybersecurity vision is so closely tied to organizational goals and success, the overwhelming majority of companies choose to locate their SOC internally, whether this is a team within the IT department or something separate. Only 11% of companies have an external SOC, though that number could be growing. In 2020, only 7% of companies reported having an external SOC, and it will be worthwhile tracking this number in the future to see if growth continues or hovers around the same level.

Regardless of how cybersecurity resources are distributed, companies are keenly aware of the need to keep their skills current and relevant. This starts with skill assessment. Like other metrics around security, assessing skill level does not have a long history and is open for interpretation. IT professionals are likely aware of which areas are personal strengths and weaknesses, but there may be no correlation to which skills are critical based on business goals and policy. CompTIA's data shows little differentiation between skills, which likely indicates a lack of knowledge around the actual skill level.

Need to Improve Cybersecurity Skills



The story is similar when it comes to identifying skills to improve. Across the board, approximately four out of ten companies feel that there is a need for significant improvement. Aside from better methods of assessing current skill level, the nature of IT initiatives may help businesses target the correct skills.

- **Data security** may be more important for companies building formal data strategies. Previous CompTIA research has shown that most companies do not have a formal approach to their data, so determining the appropriate investment in data security will be difficult until the approach is more rigorous.
- **Application security** goes hand in hand with cloud migrations, especially if custom applications are being hosted on public cloud infrastructure. These applications, previously protected by a secure perimeter, become more vulnerable since cloud infrastructure providers only secure their offering, leaving anything on top as the responsibility of the client.
- **Endpoint security** is likely being revisited as the post-pandemic workforce opts for more flexibility. Whether employees are choosing full-time remote work or a hybrid approach with occasional days in the office, their equipment may need to be refreshed or reconfigured, and the security scheme needs to match the work style.
- **Identity management** is also imperative in a cloud-first environment with remote workers. The granularity of least-privilege access provides strong security on applications and datasets, and a centrally managed scheme can improve flexibility and reduce overhead across the workforce.
- **Regulatory landscape** expertise has long been a need for highly regulated industries such as healthcare and finance, but it is becoming critical for companies of all shapes and sizes. Increased scrutiny on digital privacy and differing guidelines across state or national borders is driving demand for these skills.

Plans for Improving Cybersecurity Skills

In order to improve skills, companies are turning to range of options. For internal resources, there is obviously the option for new hiring. However, companies trying to hire are facing a constrained labor market, and the supply/demand problem is projected to worsen in coming years. On top of that, bringing in new people always carries the burden of ensuring a cultural fit, and with companies in the midst of determining their cybersecurity policy, this can add complications. Training current staff may be a more feasible option, and adding certification to internal development has been proven to bring benefits for both the company and the employees.

Aside from internal resources, companies are exploring new partnering options, whether this is expanding their current arrangements with outside firms or looking for new specialists. There are many different options in the third party ecosystem, ranging from traditional managed service providers to managed security service providers to cloud providers and other firms that fit into the edge computing category.

When choosing an outside firm, companies are considering several different criteria. For existing partners that may fit a more traditional MSP mold, excellence in core offerings is a signal that security will be handled properly. As organizations target specific facets of cybersecurity, they will clearly be searching for expertise in those areas. Finally, companies are starting to focus on tying cybersecurity to business interests, whether that is performing cost/benefit analysis to understand ROI or using threat intelligence to improve decision making.

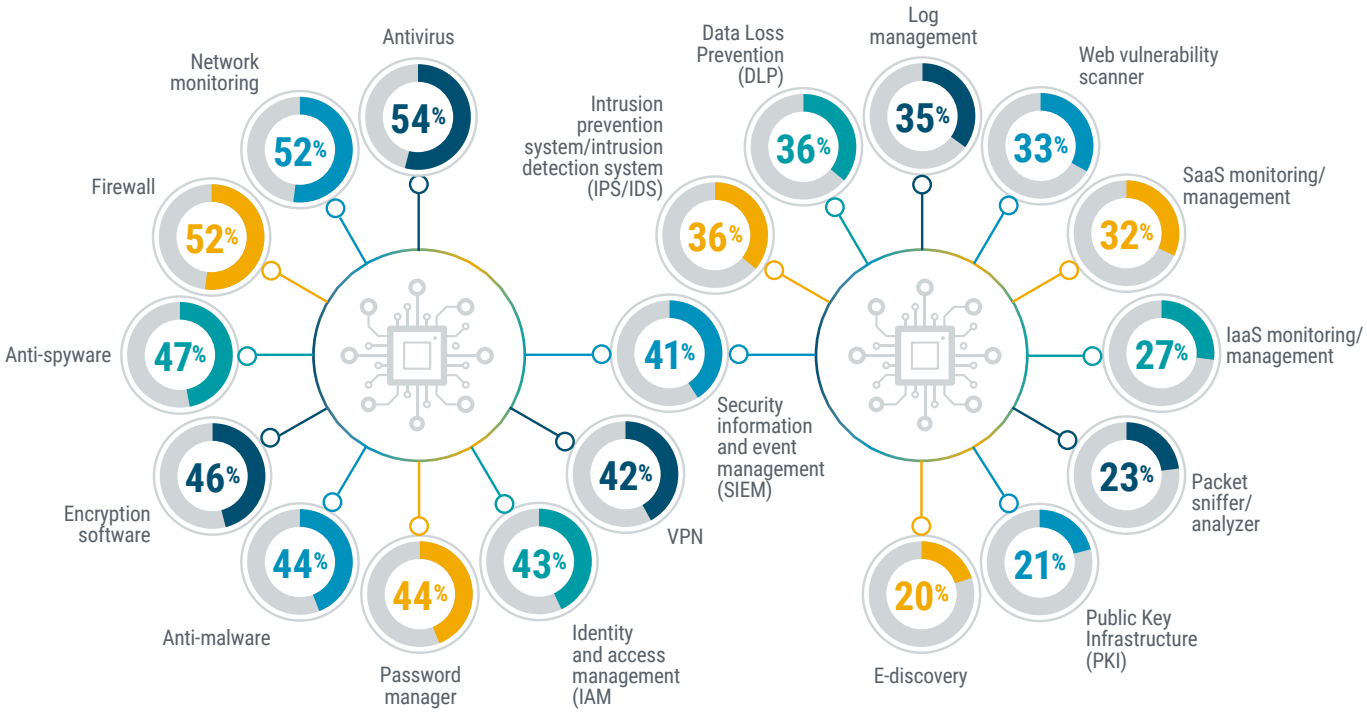
Important Criteria for Third-Party Cybersecurity Firms

4 Product

The final piece of the cybersecurity puzzle is the piece that has traditionally been at the forefront. When cybersecurity was primarily viewed as a byproduct of IT operations, the defensive technology was viewed as the main component of a secure posture. For many companies, this boiled down to two products: firewall and antivirus, forming the secure perimeter that dominated the corporate mindset.

Today, the picture is far more complicated and nuanced. Not only are there far more tools in the toolbox, but they rarely stand alone as self-contained products. Instead, they function within the overarching policy and specific processes that make up the cybersecurity strategy. As with skill assessment, the usage numbers from CompTIA's survey skew lower since the survey includes business respondents that are likely less familiar with their company's IT architecture. Still, the data highlights which tools are well-established and which tools deserve closer consideration.

Cybersecurity Products in Use



Antivirus and firewall hold spots at the top of the list, but these tools are more than just legacy holdovers. Antivirus software is obviously changing constantly to match new strains of malicious code being created, but it has also evolved over time to match the changes in IT operations, including the shift from data centers to cloud, the different combinations of laptops being used, and the adoption of smartphones and tablets. In a similar vein, firewalls have become far more capable, growing from simple packet filtering tools to stateful firewalls to unified threat management.

Since weak passwords are one of the biggest vulnerabilities, many companies are implementing password managers. While there can be a slight learning curve for end users, these tools provide the ability to maintain strong passwords across multiple sites while also allowing for central administration. Companies exploring password managers should be familiar with where credentials are stored and how accounts are recovered.

Data loss prevention (DLP) tools are certainly not new, but they have not yet achieved mass adoption. One of the fundamental attributes of cloud-first IT architecture is that the data itself needs protection. Although the primary storage option may be in one location, data can be fluid as it is being used in applications or potentially getting stored on mobile devices. DLP solutions can help monitor data at rest, in motion and in use so that security professionals are aware of any inconsistencies.

Many other tools target specific operational practices, from cloud monitoring and management to network analyzers. As a business assembles more and more tools, there is a greater need to pull all the information together so that it can be digested. Security information and event management (SIEM) tools provide dashboard capabilities for security teams to monitor complex environments. The challenge with these tools is configuration, making sure that events are flagged properly and that data is collected to enable analysis. The payoff is a simplified method for viewing a wide array of information and responding quickly to potential threats.

The variety of tools speaks to the importance of a disciplined approach to cybersecurity. Simply trying to plug in technology will generally not yield the best results. A modern strategy starts at the very top, ensuring that all key stakeholders understand the corporate policy. From there, implementing processes and bringing in the right people fuel the day-to-day tactics, and investment in the necessary products provides the means for both defense and offense. Companies need to move quickly on cybersecurity, and the fastest way forward is to understand the full scale of the problem in the new world order.

Methodology

This quantitative study consisted of an online survey fielded to workforce professionals during Q3 2021. A total of 400 professionals 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 and Market Intelligence staff at research@comptia.org.

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

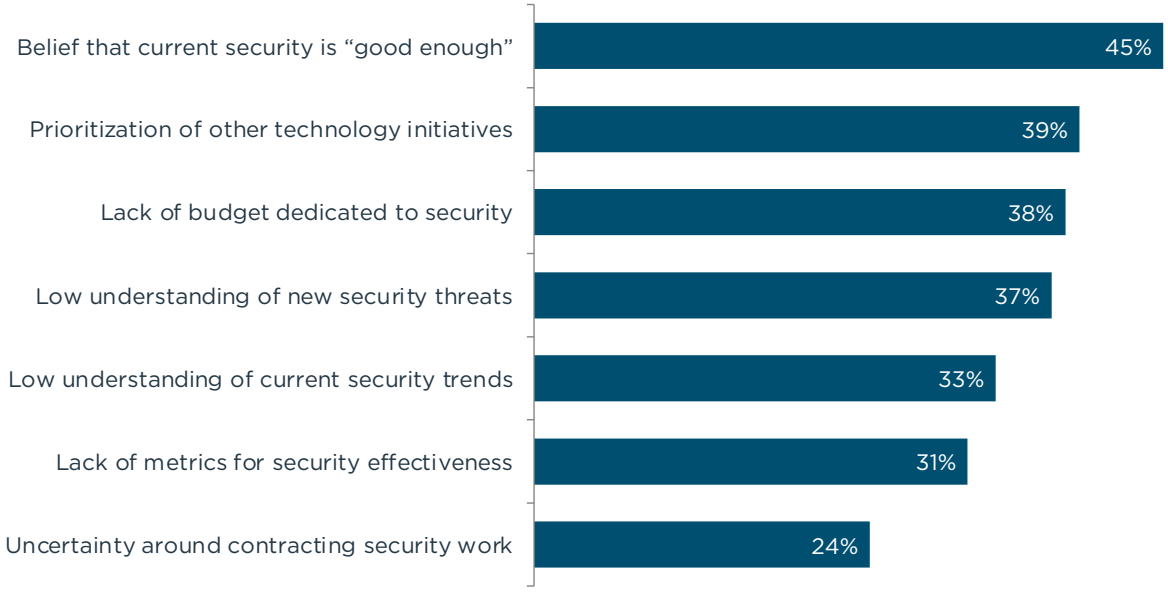
About CompTIA

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5 trillion global information technology ecosystem and the estimated 75 million industry and tech professionals who design, implement, manage and safeguard the technology that powers the world's economy. Through education, training, certifications, advocacy, philanthropy and market research, CompTIA is the hub for advancing the tech industry and its workforce.

CompTIA is the world's leading vendor-neutral IT certifying body with more than 2.8 million certifications earned through rigorous, performance-based exams. CompTIA sets the standard for preparing entry-level candidates through expert-level professionals to succeed at all stages of their career in technology. Through CompTIA's philanthropic arm, CompTIA develops innovative on-ramps and career pathways to expand opportunities to populations that traditionally have been under-represented in the information technology workforce.

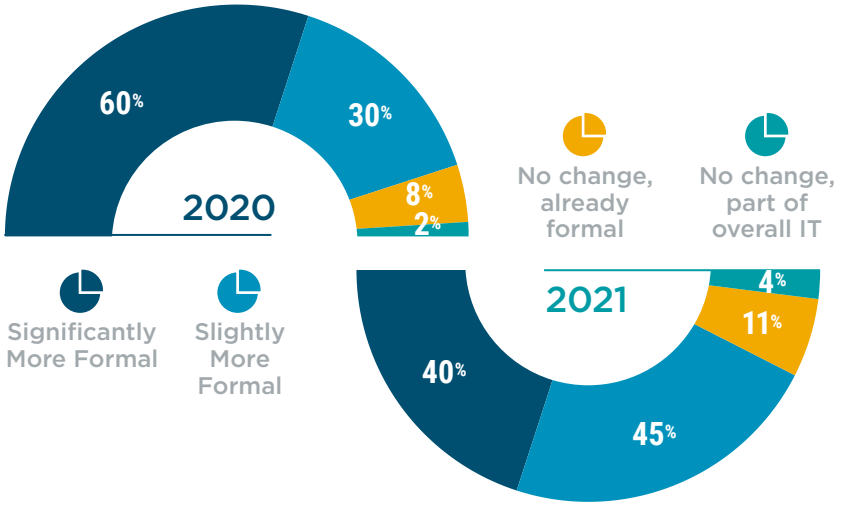
Appendix

Hurdles for Changing Approach to Cybersecurity

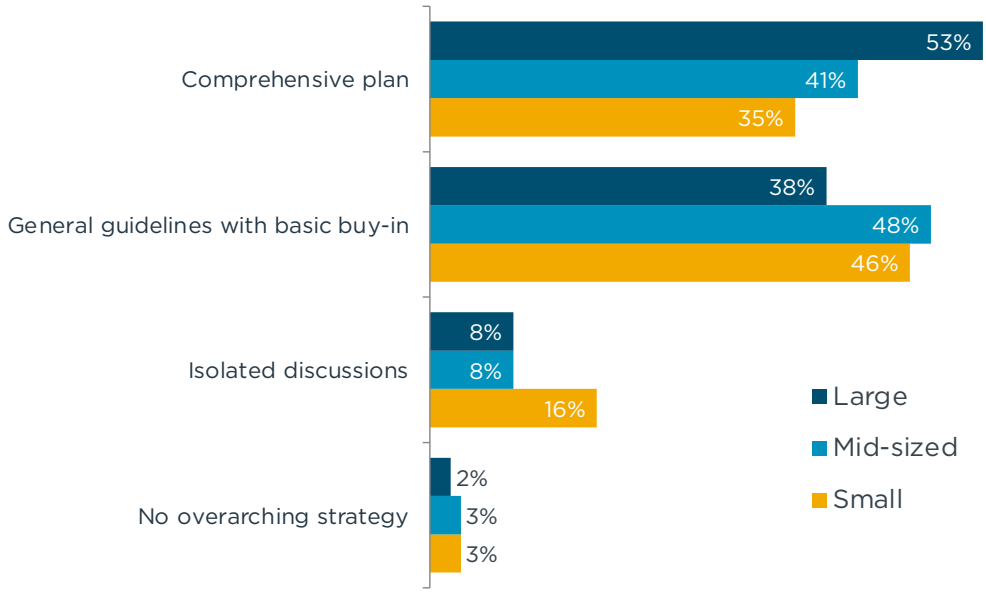


Triggers for Changing Approach to Cybersecurity

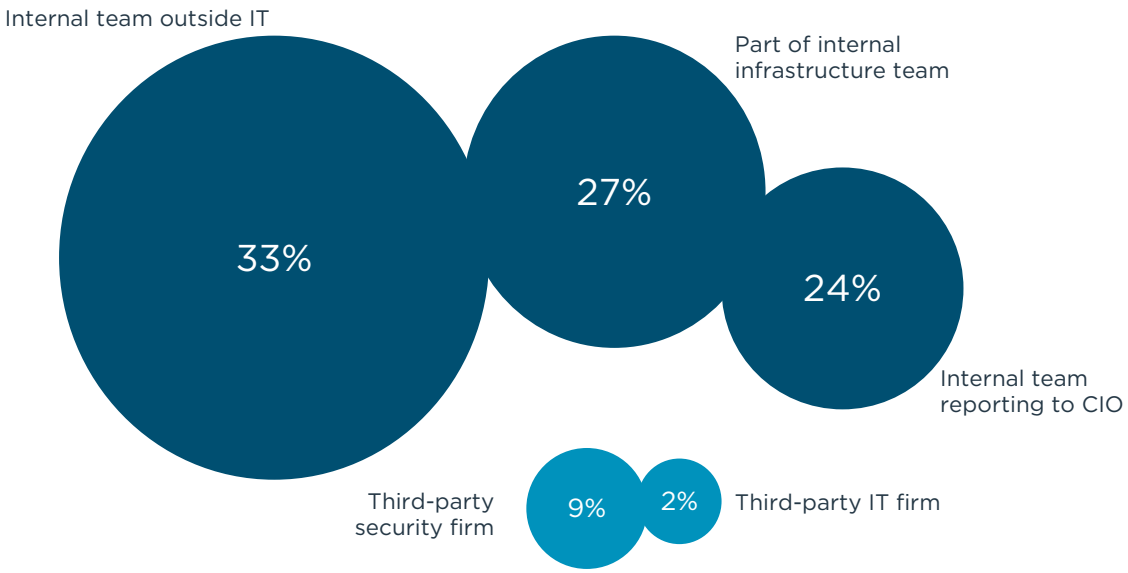
Approach to Cybersecurity Practices



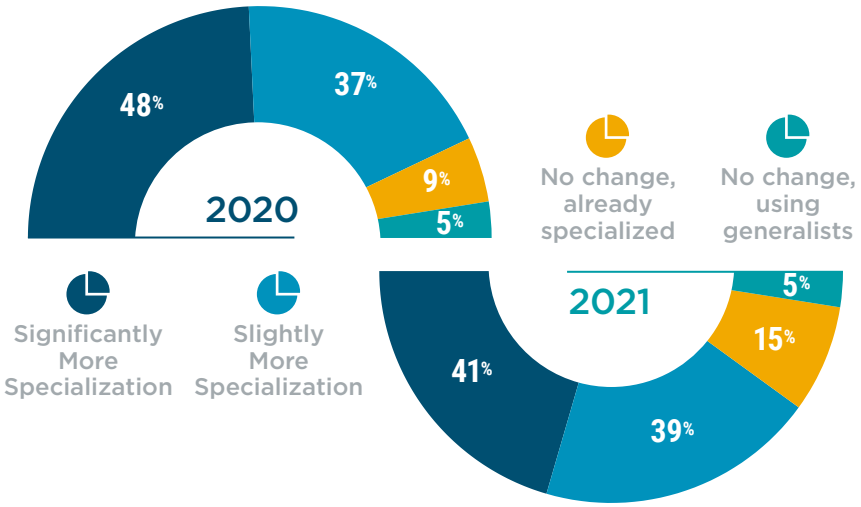
Nature of Discussion in Cybersecurity Chain



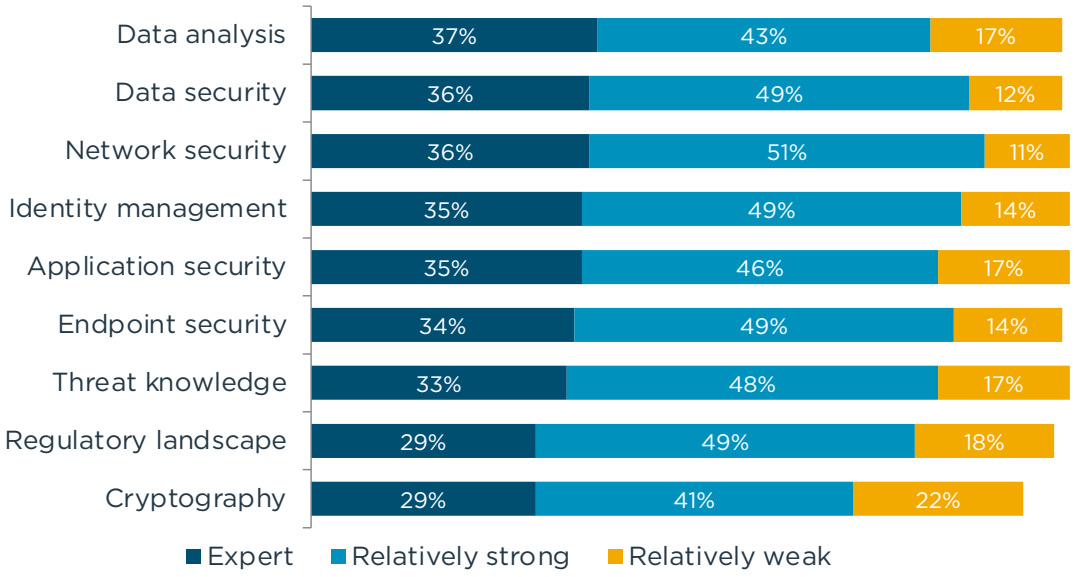
Location of Security Operations Center



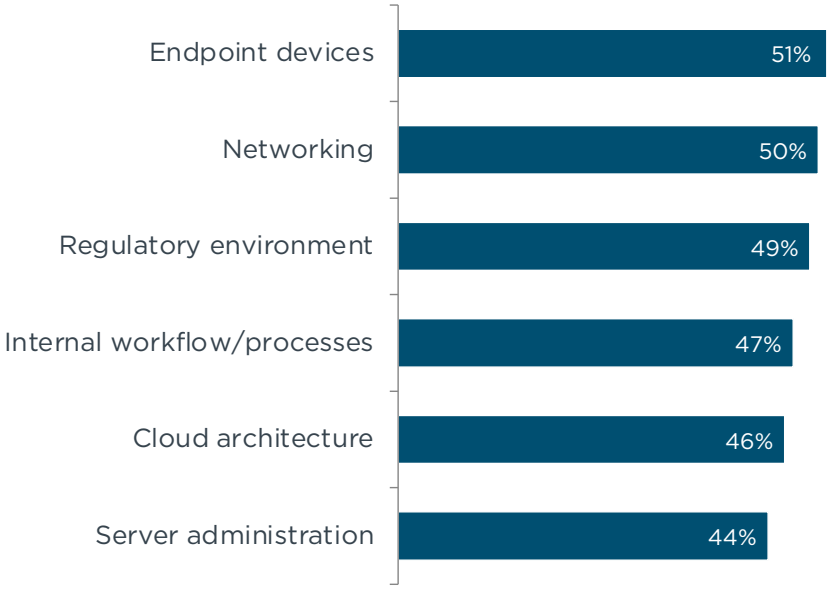
Approach to Cybersecurity Personnel



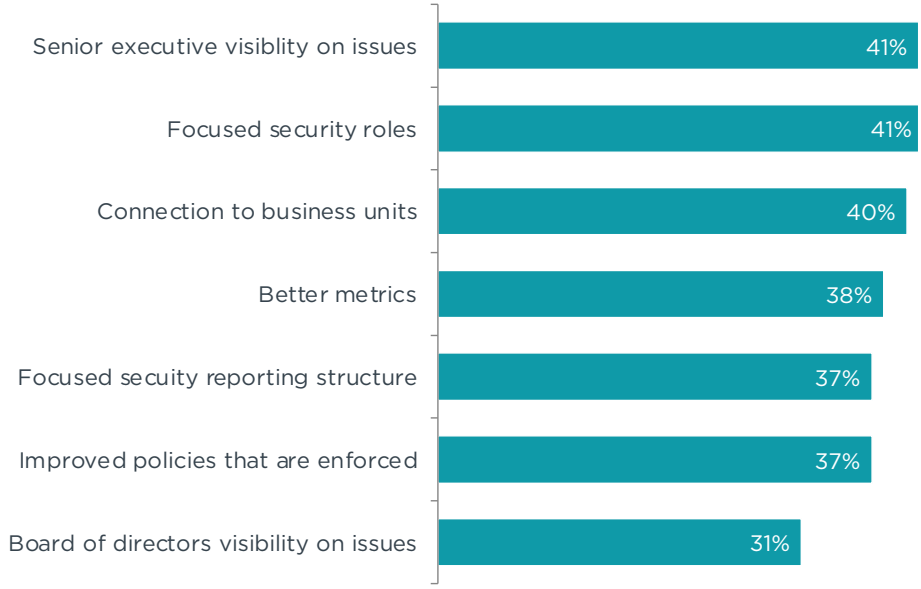
Assessment of Cybersecurity Skills



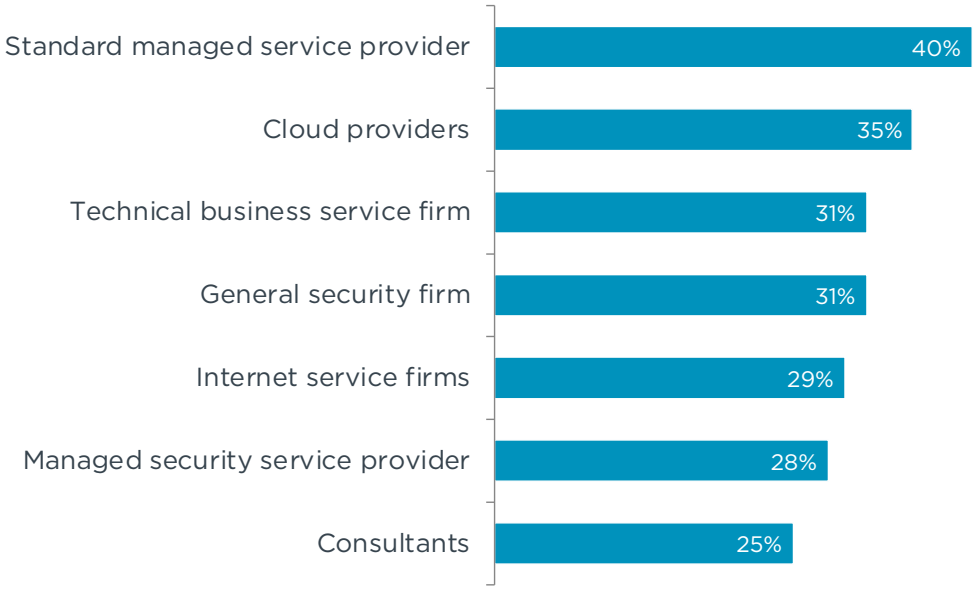
Prerequisite Knowledge for Cybersecurity Roles



Actions to Improve Effectiveness of Security Resources



Types of Third-Party Firms Involved with Cybersecurity



Sources

1 IBM/Ponemon Cost of a Data Breach Report 2021

2 IBM/Ponemon Cost of a Data Breach Report 2021

3 AV-TEST Institute

4 U.S. SEC filing, 12/14/20

5 Sophos State of Ransomware 2021 report

6 Proofpoint 2021 State of the Phish Report

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

8 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

CompTIA.org

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