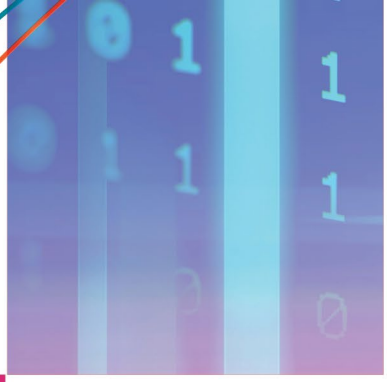


USTELECOM
2021 CYBERSECURITY
SURVEY

Critical Infrastructure Small & Medium-Sized Businesses (SMBs)

USTELECOM
THE BROADBAND ASSOCIATION

USTELECOM
THE BROADBAND ASSOCIATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

USTelecom's 2021 Cybersecurity Survey of Critical Infrastructure Small and Medium-Sized Businesses (SMBs) examines the cybersecurity risks, readiness, and realities SMBs who own, operate, or support U.S. critical infrastructure face in establishing and maintaining cybersecurity in their organizations.

The United States' critical infrastructure, and thus its national security, is dependent on the cybersecurity defensive posture of individual, yet highly interconnected, organizations. Because a SMB cybersecurity failure can impact the broader digital ecosystem leading to financial and reputational loss and service disruption, understanding the organizational behavior of companies of various sizes is imperative.

The importance of requisite security postures was laid bare during the SolarWinds Orion breach when attackers with nation-state capabilities exploited vulnerabilities in the software supply chain of an infrastructure management provider. FireEye, the Department of Treasury, and the Department of Commerce's National Telecommunications and Information Administration (NTIA), among others, were targeted, resulting in the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS/CISA) issuing an emergency order requiring immediate government-wide action to mitigate the impact of the breach.

This survey analyzes Critical Infrastructure SMBs whose cybersecurity programs often struggle to deliver robust and mature security protocols at levels similar to better-resourced and larger sector enterprises, leaving them vulnerable to cyberattacks. This unprecedented survey of Critical Infrastructure SMBs offers new insights into SMB cybersecurity programs and identifies opportunities to address economic, operational, and policy gaps.

In the midst of an escalated cyberattack environment during the COVID-19 pandemic, this survey provides important insights on how SMB cybersecurity practitioners can enhance risk mitigation strategies and practices. According to respondents, 50% of Board, CEO, and C-suite executives indicate cybersecurity is a high priority, while only 26% of employees view cybersecurity similarly. In the accelerated remote work environment spurred by the pandemic, closing this priority gap is essential to enhancing organization security.

50%

of Board CEO, and C-suite executives indicate cybersecurity is a high priority...

...while only

26%

of employees view cybersecurity similarly

Organizations build cybersecurity programs to effectively manage, mitigate, and respond to cybersecurity risks and to protect the confidentiality, integrity, and availability of assets under their control. Accordingly, an effective cybersecurity program may include, among other things:

- Raising employee awareness and training
- Performing regular and comprehensive risk assessments
- Updating policies and procedures
- Evaluating in-house capabilities
- Adopting risk assignment options such as cyber insurance

The survey questions focus primarily on the business implications of cyberattacks and how well SMBs are prepared to defend against, respond to, and recover from a variety of harmful incidents.

The survey's key findings suggest that breaches, and their impact, demonstrate the need for improving awareness, defense, and risk management.

- After a breach, Critical Infrastructure SMBs tend to provide staff with extra training, implement new policies and procedures, change configurations, and communicate breaches to customers, thereby building trust.
- A Critical Infrastructure SMB's use of risk assessments and cybersecurity best practices, policies, and procedures typically results in the increased use of outsourced cybersecurity providers, preparedness, confidence and consumer trust, and the use of government guidance.
- A Critical Infrastructure SMB's use of cybersecurity best practices tends to be more robust as annual revenue increases and leads to increased levels of transparency and trust with customers, cyber prioritization at the board, executive, and director/manager level, use of cyber insurance, communications to customers about breaches, and confidence in an organization's defense capabilities.
- Critical Infrastructure SMBs with $11-20M in annual revenue experienced the most diverse array of attack types and were the most willing to act post-breach.

While improvements made subsequent to an attack are important, the survey findings demonstrate the need for proactive cyber risk assessments calibrated to the uniqueness of individual enterprises so they can best protect against their unique cyber risks. SMB surveys like this one, conducted regularly and on a larger scale, will be critical to actively monitoring the cyber-critical infrastructure landscape as it evolves.

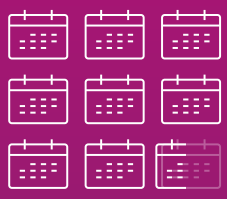
◂ ORGANIZATIONAL IMPACT ▸

BREACH HISTORY

75%
of Critical Infrastructure SMBs experienced a breach **at least once** in company history

45%
experienced a breach within the past year

CONSEQUENCES



On average, it took companies

7.5 MONTHS

to fully recover from a breach

59%
reported the breach stopped daily productivity

46%
LOST CUSTOMERS

Companies spent $170,000
on average to resolve a cyber breach

◂ PREPAREDNESS ▸

CONFIDENCE

72%
of SMBs surveyed believe their organization is prepared to some extent to prevent or recover from a cyberattack

ACTIONS IN SUPPORT OF RESILIENCY

74%
completed a cyber risk assessment within the past 12 months

13%
used government guidance to make cybersecurity decisions

87% have cybersecurity policies and procedures in place

75% have existing cybersecurity insurance policies

52% use an outsourced cybersecurity provider

ON AVERAGE

26%
of IT budgets are used for cybersecurity

RECOMMENDATIONS

Critical Infrastructure SMB and Enterprise Recommendations

Survey findings suggest Critical Infrastructure SMB enterprises are distinctly vulnerable to breaches that can take longer to detect and from which to recover. Heightened vulnerabilities are evident across the following vectors — social media; electronically held customer information; online bank accounts; VPNs; social engineering; and industrial control systems. To improve the cyber defensive postures of Critical Infrastructure SMBs and SMBs more generally, both enterprises and policymakers must take deliberate, focused, and prioritized action. The following recommendations are designed to incentivize organizations to be proactive in cyber defense efforts and dedicate additional budget toward meaningful cybersecurity measures.

RECOMMENDATIONS

TOP RECOMMENDATIONS FOR SMBS

- **Conduct regular cybersecurity training** and test staff based on readily available best practices and controls. The training and testing process should be regularly evaluated to ensure it addresses the most current threat landscape and focuses on what individuals can control (e.g. opening unknown links).
- **Revisit and update policies and procedures** annually, or more often if necessary. Detailed and documented policies and procedures should identify roles and responsibilities and promote organizational accountability.
- **Update system configurations**, as recommended by vendors and experts as appropriate, and have structured protocols in place to patch vulnerabilities.
- **Conduct annual risk assessments** that put cyber risks in empirical and economic terms so mitigation techniques can be calibrated to the unique risks and risk appetite of the organization, and ensure results are known and reviewed by executive management and/or boards.
- **Conduct post-breach assessments** and communicate findings to appropriate management and departments. Update the policies and protocols to reflect risk assessment lessons and insights.
- **Annually evaluate in-house capabilities** and consider retaining outsourced, managed service providers based on a cost-benefit analysis to augment existing cybersecurity staff as needed.
- **Obtain cyber insurance** and review policies annually to ensure the appropriate coverage and alignment with enterprise risk tolerance in light of operational and market changes.
- **Identify and participate in valuable formal and informal information sharing** venues, including sector specific trust pools, that support SMB needs and expectations.
- **Establish regular briefings** for appropriate levels of management and senior executives across all major business units. Implement a process to ensure feedback mechanisms to appropriate personnel within the organization.
- Depending on organization needs and enterprise-level risk tolerance, most organizations should **dedicate at least 10-15% of their IT budget toward cybersecurity**.

These practices will likely require organizations to make additional investments in cybersecurity in the context of their overall business plan, which is highly encouraged.

RECOMMENDATIONS

Policymakers Recommendations

> Based on survey findings and insights into this unique class of Critical Infrastructure SMBs, the following recommendations provide guidance for a focused and well-coordinated national strategy.

TOP 4 RECOMMENDATIONS FOR POLICYMAKERS

- **Ensure expectations for SMB cybersecurity are grounded in an understanding of economics and appropriate incentives are considered.**
  - This involves providing firms with prioritization mechanisms and guidance on how they should spend limited resources to the greatest effect. Resource constrained SMBs need guidance on investment maximization.
  - SMBs may not be able to sustain uneconomic investments in cybersecurity beyond minimum requirements. Consequently, consideration must be given to what incentives may be required.

- **Close the cybersecurity talent gap between Critical Infrastructure SMBs and better-resourced enterprises.**
  - Ideally, cyber talent should be available to companies of all sizes. Both government and privately supported programs should be implemented to address this gap.

- **Undertake a whole-of-nation education effort that begins in K-12 and fulfills the expansion of higher education program offerings.**
  - In the long-term, a much broader and strategic approach that sees the expansion of STEM and cyber-specific pathways in K-12 education and beyond is necessary. Programs that incentivize students to pursue cybersecurity degrees should be expanded. Public-private partnership models can aid in the effort to reduce student debt and subsidize the cost of education in this critical career field.[1] One such example is the National Cyber Education Program (NECP). NECP produces cyber curriculum content for K-12 schools and career opportunities, and is supported by public and private sector partners including the White House and Discovery Education.[2]

RECOMMENDATIONS

- Currently, only 23 U.S. universities offer undergraduate cybersecurity programs.[3] Efforts should be made to increase the number of vocational, undergraduate, and graduate cyber programs.
- Government agencies should leverage their unique capabilities to create educational opportunities.
  - NSA and DHS have co-sponsored centers of academic excellence (CAE) programs in cybersecurity operations (CO) and cyber defense (CD) in an organized response to increasing cybersecurity issues.[4]
  - The Office of Personnel Management launched its Presidential Fellows Program and will accept between 300-600 finalists in 2021.[5]
  - The Department of Energy launched its Operational Technology (OT) Defender Fellowship program, creating a talent pipeline for key U.S. frontline critical infrastructure defenders.[6]

- **Distinguish security from compliance and eschew overly prescriptive or punitive actions.**
  - As the U.S. implements the DoD's Cybersecurity Maturity Model Certification (CMMC) program and other cyber initiatives, the broad stakeholder community must ensure that we don't compromise security for compliance. We need to focus on cybersecurity as opposed to compliance. Government compliance programs could waste scarce cyber resources unless they are implemented based on cost-effectiveness measures as opposed to regulatory mandates.

By following these recommendations, policymakers can dramatically increase the likelihood of effective and sustainable improvements to the cybersecurity of Critical Infrastructure SMBs.

KEY FINDINGS

1. Organizational Impact

> We investigated the frequency of SMB cyber breaches (in company history, within the past year, and after the onset of the coronavirus pandemic), actions taken post-breach, disruptions to staff's daily work, costs to resolve breaches, and how many months companies would continue to operate if they experienced a significant breach.

Criminals are incentivized to steal data from large and small businesses alike. As such, breaches targeting SMBs are increasing in frequency, impact, and size. [7]

75%
of SMBs surveyed experienced a breach at least once in their company history,

and…

45%
experienced a breach within the past year

According to the Verizon 2020 Data Breach Investigation Report, most cyber breaches are web application- and cloud-based. The COVID-19 pandemic and the consequent mass transition to remote work has amplified the problem. Malware and phishing attacks are escalating as attackers try to exploit remote workers who operate beyond their company network perimeter and may not have adequate security at home.

Fifty-three percent of our survey respondents reported an increase in phishing since the start of the coronavirus pandemic and 37% have experienced a cyber breach in the same timeframe. In our interviews with executives, it was noted that the expectation for SMBs to follow the example of large players and leaders in the industry fails to acknowledge vastly different resources and capabilities. The organizational impact of cyber breaches on SMBs may require unique solutions that recognize this disparity.

COMMON EXPERIENCES OF CRITICAL INFRASTRUCTURE SMBS

SMBs that experienced a cyber breach in the past year are significantly more likely, across nearly all survey measures, to take actions to repair the breach and improve cybersecurity. This trend held true across all organization sizes, levels of annual revenue, and critical infrastructure sectors. Those who experienced cyber breaches in the past year report:

- Heightened awareness of vulnerability across the following vectors — social media, electronically held customer information, online bank accounts, VPNs, social engineering, and industrial control systems.
- Difficulty managing the increasing complexity of cybersecurity, sophistication of attacks, volume of attacks, and struggle to retain practitioners to respond to attacks.
- Higher percentages of annual IT spending directed to cybersecurity (31% average) compared to other organizations (22% average).

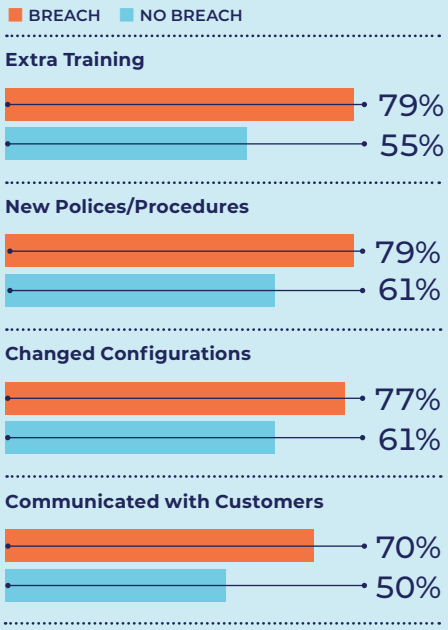
- Higher volumes of cyberattacks and, as a result, significantly higher likelihood to have cybersecurity insurance, outsource cybersecurity, revisit policies and procedures, and complete cyber risk assessments.
- Taking actions such as conducting trainings, communicating breaches to customers, changing system configurations, and creating new policies and procedures.

Companies with 50 or fewer employees, however, are less likely to take action after experiencing a cyberattack. The lack of action within organizations of this size may stem from a lack of experience, economic constraints, limited solution set knowledge, and a lack of confidence about defending against specific types of attacks.

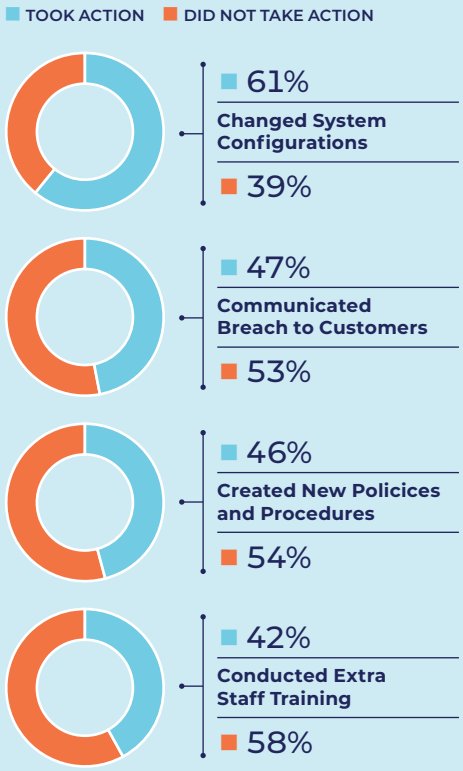
During interviews with executives, it was noted that building and delivering appropriate education and training to SMBs presents opportunities to signal the value of investment and an ability to demonstrate progress at increasing levels of practitioner capabilities.

SMBs that experienced a cyber breach in the past year are significantly more likely to take actions to repair the breach and improve cybersecurity

ACTION TAKEN POST BREACH



LACK OF ACTION ORGANIZATION SIZE 1-50



KEY FINDINGS

SMB BREACH DETECTION, COSTS, AND RECOVERY

Since no cybersecurity panacea exists, it is inevitable that business will sometimes be compromised, especially if it's a nation-state actor engaged in an Advanced *Persistent* Threat. Once an attack is successful, the focus shifts from prevention to mitigation, which requires a breach be detected. Verizon found "the number of breaches that take months or years to discover is greater in large organizations than in small organizations." Similarly, IBM's 2020 Cost of a Data Breach report found that it takes companies, on average, about 197 days to identify and 69 days to contain a breach.[8] Our survey indicates that Critical Infrastructure SMBs did not fare as well. On average, it took organizations **7.5 months to operate following a significant breach.** To put this figure in context, of the 4,644 executives surveyed in a 2020 study, the longest it took for an organization to recover from a breach was 90 days or less, with most being able to remediate within 15 days or less.[9] This suggests that SMBs may be more debilitated by cyber breaches. Fifty-nine percent reported the breach stopped staff from carrying out daily work and 46% lost customers. **Organizations spent $170,000 on average to resolve a cyber breach.**

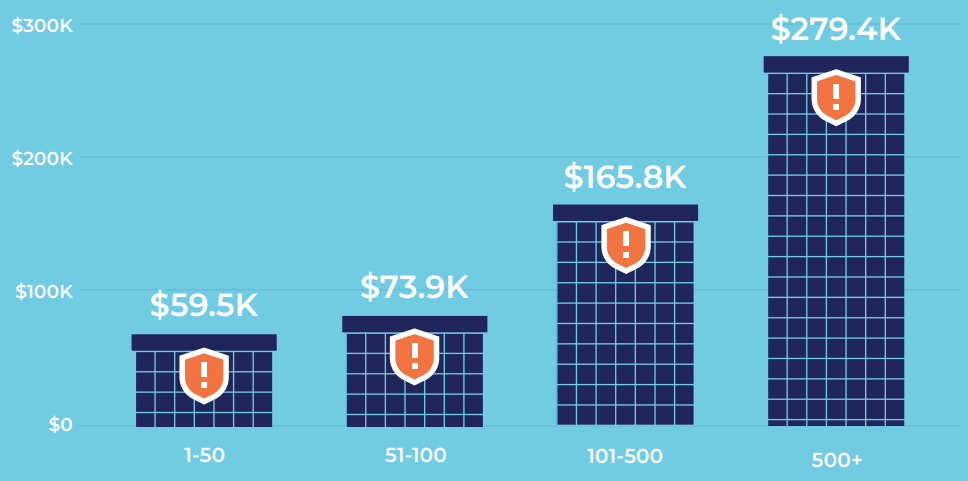
It takes 7.5 months for organizations to fully recover from a breach.

59%
reported the breach stopped staff from carrying out daily work, and...

46%
lost customers

The chart below shows the cost of breaches varied significantly by number of employees.

AVERAGE COST OF BREACH BY ORGANIZATION SIZE



2. Preparedness

We investigated the cyber defensive posture of SMBs, including their confidence defending against attacks, use of cybersecurity providers, policies and procedures, risk assessments, cybersecurity insurance, and use of government guidance to make decisions.

MEASURING PREPAREDNESS IN THE CONTEXT OF CYBERSECURITY

Preparedness against cyber breaches is highly contextual. Certain behaviors, however, can be indicative of cyber breach preparedness, including an organization's use of cybersecurity providers, policies and procedures, risk assessments, cybersecurity insurance, and government guidance to make decisions. Although engaging in these preparedness activities does not completely eliminate or prevent cyber threats, it can increase an organization's confidence and ability to respond and recover.

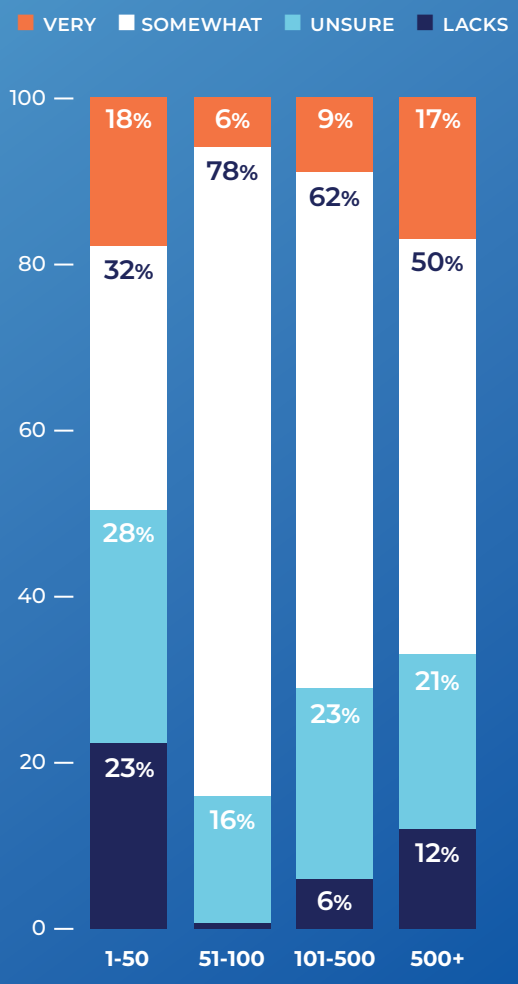
Seventy-two percent of survey participants believe their organization is prepared to some extent to prevent or recover from a cyberattack. However, confidence to defend against attacks varied considerably based on organization size. More than half of organizations with 50 or less employees lacked confidence or were unsure about their ability to defend against attacks. Even among the larger SMBs, only 6–17% (depending on size of organization) reported being very confident.

The chart at right shows the reported confidence of SMBs to defend against attacks by number of employees.

72%

of SMBs surveyed believe their organization is prepared to some extent to prevent or recover from a cyberattack

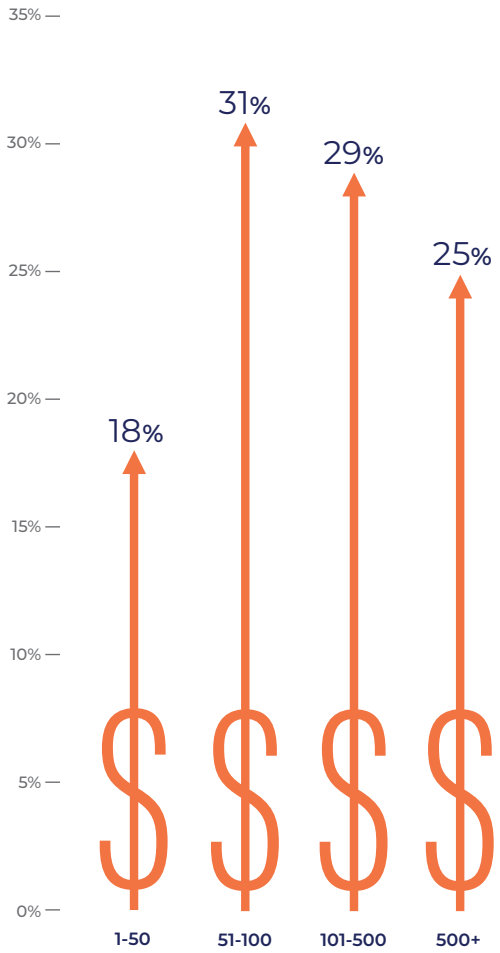
CONFIDENCE DEFENDING BY ORGANIZATION SIZE



KEY FINDINGS

Prudent cybersecurity risk management calls for all organizations to **evaluate their in-house cyber capabilities**. Since SMBs in many cases have limited budgets and staff, finding the properly trained professional can be difficult, forcing many to rely on service providers to manage their IT and cybersecurity needs to keep workflows and systems secure. The survey found that 52% use an outsourced cybersecurity provider. Moreover, companies are more likely to outsource cybersecurity if they conduct cyber risk assessments. This may be due to increased awareness of the threats that require expert knowledge and resources to defend against them. In addition, executives shared that the scarce talent available in an already tight cyber labor market is being absorbed by larger organizations. As such, outsourcing is becoming the only viable solution to the current cyber talent gap for many smaller businesses struggling to manage their cybersecurity programs. In the short-term, outsourced dependence may be expected and welcomed. In the longer-term, in-house capability may grow in tandem with a growing cyber workforce.

PERCENT OF IT BUDGET SPENT ON CYBERSECURITY BY ORGANIZATION SIZE



Appropriately funding a firm's cybersecurity program can mean the difference between a minor incident and a major catastrophe. As such, **cyber budgets are a top-of-mind concern** for frontline practitioners and executives alike. The proportion a business invests in cybersecurity relative to its IT budget can signal how seriously they view the cybersecurity threat and, therefore, how prepared they will be to recover in the event they are breached. Since cyber budgets may consist of, among other things, internal staff, consultants, software, hardware, trainings, and insurance, it is difficult to capture this proportion with any accounting precision. With varied consistency in mind, the survey found that the average percent of IT budget related to cybersecurity across all size organizations was 26%. Although companies with fewer than 50 employees spent a considerably lower percentage of their IT budget on cybersecurity compared to other groups surveyed, they still spent above industry averages, which are in the 10-15% range.[10]

Because cyber threats are constantly evolving, routinized and **annual cyber risk assessments help** determine whether a company is actually prepared to prevent or recover from an attack. Fortunately, 74%

of survey respondents reported they had completed a cyber risk assessment within the past 12 months. Reasons for conducting risk assessments were influenced by a variety of factors, including regulatory requirements, coronavirus concerns, executive prioritization within companies, and experiences with breaches. The survey also found that assessing risk improves preparedness, confidence, and customer trust. Organizations that conducted risk assessments assert they are better prepared to respond and are confident defending against cyberattacks and cyber breaches. Organizations conducting risk assessments also report higher communication with customers resulting in higher customer trust. They are also more likely to report:

- Outsourcing cybersecurity.
- Experiencing all types of attacks included in the survey: phishing, social engineering, malware, ransomware, viruses, spyware, email frauds, unauthorized use of computers from outside the organization, unauthorized use of computers from someone inside the organization, and denial of service attacks.
- Health, customer, and personally identifiable information stolen during a cyber breach.
- Using government programs assisting with cybersecurity; sharing best practices learned from cyberattacks with other companies; and participating in trainings hosted by the government or private organizations.

Cybersecurity **policies and procedures play a significant role in setting behavioral norms**, especially when employees are the weakest links in an enterprise security chain. It is, therefore, encouraging that 87% of survey respondents reported they have cybersecurity policies and procedures in place. Cybersecurity policies and procedures increase in robustness and breadth of coverage as annual revenue increases. Critical infrastructure SMBs with $50M+ in revenue indicated they use and place a great deal of importance on nearly all best practices assessed in the survey. Conversely, organizations with less than $1M in revenue are more likely to report placing a lower level of importance for a majority of the best practices than SMBs with more than $1M in revenue. These practices include multi-factor authentication (MFA); training; policies and procedures; risk assessments; insurance; and software updates. Organizations with policies and procedures are more likely to:

Organizations with $50M+ in revenue use best practices.

Organizations with <$1M in revenue are more likely to report using very few best practices

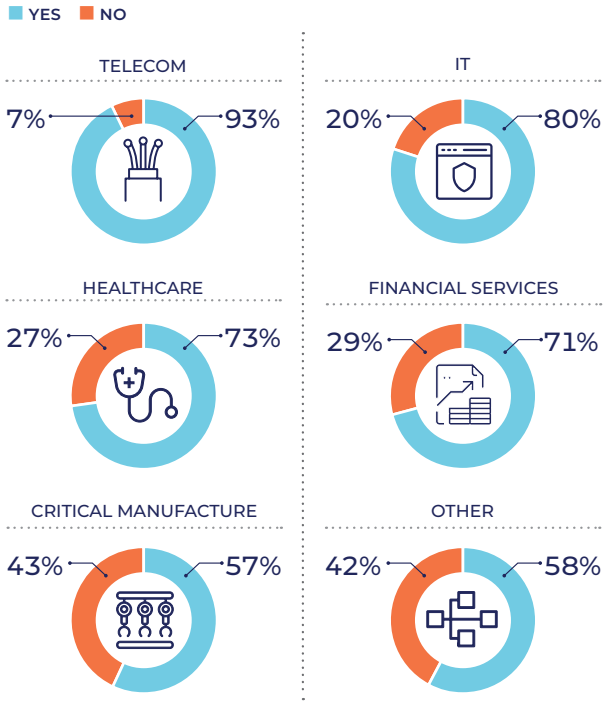
- Take actions resulting from a cyber breach by conducting extra training, communicating with customers, changing system configurations, and creating new policies and procedures.
- Report being very confident defending against cyberattacks.
- Prioritize cybersecurity at the board member, executive, and director/manager level.
- Report having cybersecurity insurance.
- Report having more open and transparent relationships with customers based on more frequent communication. However, the strength of the relationship is not a free pass for losing data in cyber breaches, as most reported they would lose customers if they lost data in a breach.

KEY FINDINGS

13%

of SMBs use guidance issued by DHS/CISA to make cybersecurity decisions

CYBERSECURITY INSURANCE BY SECTOR



A company can only do so much to prevent a cyber breach. At a certain point, cyberattacks are out of the victim's control, becoming an inevitable and unavoidable cost of doing business in the digital age. It is not a matter of "if" you'll be attacked, but "when," as well as "how" you will prepare and respond. Fortunately, **cyber insurance gives organizations the option to transfer that risk to other entities**. The survey found that 75% of participants have existing cybersecurity insurance policies. In interviews with executives, it was noted that there is some skepticism around the value of cyber insurance. One CEO admitted that, although they are considering cyber insurance, they do not currently have it due to a lack of research. Another revealed the heavy focus on cost reduction has resulted in their organization struggling to understand the strategic aspect of investing in cybersecurity insurance.

The U.S. government continuously issues cyber guidance, adapting and updating its publications, as the cyber landscape changes. As new information is gathered and understood, researchers work tirelessly to issue alerts and distill and organize best practices for other organizations to implement. Uptake of these education and awareness tools, or lack thereof, is important to understanding the effectiveness of government efforts to support organizations in their management and prioritization. On average, 13% on average of the SMBs indicated they used guidance issued by the Department of Homeland Security Cybersecurity & Infrastructure Security Agency (DHS/CISA) to make cybersecurity decisions. It is worth noting this percentage reflects that companies are not only aware of government guidance, but also use the material to enhance security posture. The effective uptake of government guidance, or lack thereof, is important for government and industry practitioners to understand, and collaborative efforts should be undertaken to expand awareness and use of thoughtfully curated material. Government guidance that is accompanied by cost-effective analyses likely would expand adoption by helping companies prioritize security investments based on traditional business analyses.

SURVEY METHODOLOGY AND PARAMETERS

1. **QUALITATIVE:** Fourteen in-depth surveys with SMB Chief Executive Officers (CEOs) and C-Level executives to identify and better understand where cybersecurity gaps and barriers exist and explore steps that should be taken to enhance the cybersecurity of the organizations they represent.

2. **QUANTITATIVE:** An online survey of employees, directors/managers, and executives of SMBs with up to 2,500 employees. A total of 323 people completed the survey with responses that could be included in the analysis.

ACKNOWLEDGEMENTS

EXECUTIVE SPONSOR

USTelecom

Robert H. Mayer
Senior Vice President, Cybersecurity & Innovation

CONTRIBUTORS

Mike Saperstein
VP, Strategic Initiatives & Partnerships

Paul Eisler
Senior Director, Cybersecurity

Michael Steckler
Research Analyst

USTELECOM SURVEY PARTNER

SURVEY LEAD

Dr. Dustin Williams
Research Psychologist, CyberRx

CONTRIBUTOR

Ola Sage
CEO, CyberRx

ENDNOTES

1 https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

2 https://www.google.com/url?q=https://www.natcybergroup.com/&sa=D&ust=1609917197829000&usg=AOvVaw0UlFN7fBOVri0Yu8CrXTa4

3 https://www.usnews.com/best-colleges/rankings/computer-science/cybersecurity

4 https://www.cyberdegrees.org/listings/top-schools/

5 https://federalnewsnetwork.com/workforce/2020/09/presidential-management-fellows-plan-to-enter-the-cyber-reskilling-game/

6 https://www.energy.gov/articles/us-department-energy-launches-program-enhance-partnerships-between-government-and-critical

7 https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

8 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

9 https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf

10 https://www.darkreading.com/operations/cybersecurity-budget-rose-in-2019-uncertainty-prevails-in-2020/d/d-id/1338580#:~:text=As%20a%20percentage%20of%20the,a%20share%20of%20employee%20cost; https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html; https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget#:~:text=Finally%2C%20it's%20worth%20noting%20that,fiscal%20budget%20(%244.746%20trillion)


USTELECOM
THE BROADBAND ASSOCIATION
USTelecom.org