State of Hoosier Cybersecurity

2025

JANUARY
2025

PREPARED FOR
Indiana Executive Council on Cybersecurity

BY
Kelley School of Business, Indiana University
Indiana Business Research Center

Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University), Christos A. Makridis, PhD (Arizona State University)

Special thanks to Tanner Wilburn and Madelyn Gamble for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Lubin and Angie Raymond for their helpful comments and suggestions.

Table of Contents

Contact Information

For more information about this report, contact Indiana Business Research Center at (812) 855-5507 or email ibrc@iu.edu. Professor Shackelford may be reached at sjshacke@iu.edu

Executive Summary

Cyber attacks have become a widespread challenge for organizations across Indiana. From county governments in Clay and Monroe to healthcare providers, universities, small businesses, utilities, and school corporations—no sector has been immune to digital threats. Recognizing the need for a comprehensive understanding of these risks, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council partnered with researchers from Indiana University and the University of Arizona to conduct an in-depth study to help explore how Indiana organizations perceive and manage cyber risks.

Building on the initial 2020 research and report, this study examines how approaches to cybersecurity have evolved since the COVID-19 pandemic.

1

Understanding Cyber Risk

Section 1 provides background on cyber threats, organizational challenges, and recent state-level policy efforts.

2

Research Methodology

Section 2 explains the study's research methodology, including its approach to data collection and analysis.

3

Survey Results

Section 3 presents survey results on risk perceptions, management strategies, and cyber insurance trends.

4

Policy Recommendations

Section 4 offers actionable recommendations to address cybersecurity vulnerabilities and governance gaps effectively.

This report aims to equip business leaders, policymakers, law enforcement, and all Hoosiers with critical insights into the state of cybersecurity in Indiana. As the report emphasizes, cybersecurity is a collaborative effort—*we're all in this together.*

Key Findings

1. Cyber Risk Perceptions

Over 95% of respondents expressed significant concern about cybersecurity incidents, particularly phishing and ransomware attacks. These threats are viewed as the most pressing and reflect a heightened awareness of cyber risks since 2020.

2. Cybersecurity Incidents

Only 11% of organizations reported experiencing a successful cyber attack since spring 2021 which suggests a marked improvement from the prior three years. This decrease in successful attacks could indicate progress in threat mitigation efforts across Indiana.

3. Preventive Measures

Organizations are increasingly adopting essential cybersecurity practices, including antivirus software, remote backups, software updates and patching, and multifactor authentication. When asked about how their cybersecurity practices had changed since 2021, organizations most frequently reported adopting multi factor authentication, remote backups, and antivirus software.

4. Incident Response

In 2023, 34% of respondents reported revising their incident response plans since 2021. This shows organizations are becoming more proactive in preparing for and addressing emerging cybersecurity threats.

5. Training and Personnel

While 63% of organizations provide cybersecurity awareness training, many still lack dedicated cybersecurity professionals. This indicates a persistent skills gap that undermines efforts to build robust cybersecurity defenses.

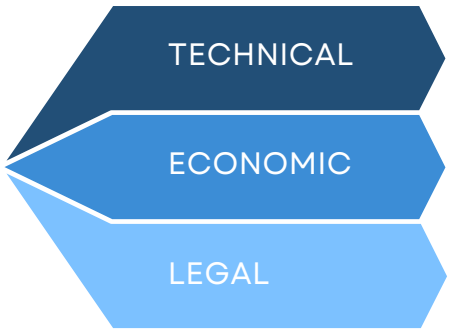
6. Cyber Risk Insurance

Cyber risk insurance coverage increased to 64% in 2023, up from 50% in 2020. However, 58% of insured organizations reported rising premiums, posing financial challenges, especially for smaller entities.

Understanding Cyber Risk

Understanding cyber risk requires moving beyond traditional notions of individual data breaches or isolated technical failures. While these threats remain important, they are only part of a larger, more dynamic landscape shaped by technological innovation, economic pressures, and evolving legal frameworks. Cyber risk now encompasses systemic vulnerabilities that impact critical infrastructure, disrupt global supply chains, and challenge regulatory compliance. The growing interconnectedness of devices, fueled by the Internet of Things (IoT), and the widespread shift to digital operations during the COVID-19 pandemic have accelerated this evolution.

This section explores cyber risk through three key dimensions—technical, economic, and legal—to provide a comprehensive understanding of its multifaceted nature. It then offers actionable steps to manage these risks, framed around the principles of being aware, being organized, and being proactive. Lastly, it examines emerging trends reshaping the cyber risk landscape, including the rise of cyber insurance, the integration of artificial intelligence, and shifts in security strategies in a post-pandemic world.



A. Cyber Threat Dimensions

Organizations currently face cyber risks across multiple dimensions: the myriad technical threats to information and systems pose serious economic threats across many sectors. Furthermore, the complex, patchwork legal landscape governing cybersecurity and privacy in the United States poses a challenge to businesses seeking to understand the protections that apply to them and the regulations they must comply with.

1. Technical

Technical vulnerabilities pervade modern business, and society. Smart phones can be compromised to be used as microphones even when they appear to be turned off.[1] Internet-connected lights and kitchen appliances can be hijacked to launch cyber attacks.[2] Internet traffic can be rerouted to servers around the world without the user's awareness.[3] Supply chain vulnerabilities and weak encryption can lead to a cascade of failures, yet are hard to identify and address.[4] Each of these cyber risks, as with so many others, require a suite of corporate governance and policy responses. The problem is vexing given both the complexity and scale of the issue, with reports of novel cyber attacks being launched every thirty-nine seconds.[5]

2. Economic

Successful cyber attacks can cause serious and long-lasting impacts on organizations, including but not limited to financial damages, compromised personally identifiable information, breaches of critical infrastructure, tarnished reputations, and a loss of consumer confidence.[6] Managing the fallout from a data breach can be a challenging and costly endeavor. While this pertains to most organizations, it is especially true for small and midsize businesses (SMBs).

Cybercrime has become a significant cost center for these firms, with one survey revealing that 58% of executives thought that data breaches were a more significant concern than incidents like fires, floods, and physical break-ins combined.[7]

This is both true of midmarket firms, as well as larger organizations; indeed, perhaps counterintuitively the bigger the company, the less it spends per employee for cybersecurity owing to economies of scale combined with a lack of focus on cybersecurity issues.[8]

In addition to businesses, attacks on local governments are more salient than ever. Governments often misperceive the potential complexity of a cyber attack, which can cause sensitive data like bank information, government processes, municipal employee records to become vulnerable. Just like businesses, local governments have to work within the lack of financial resources to tackle cybersecurity challenges, with average state or local government agencies spending less than 5% of their IT budget on cybersecurity.[9]

Despite these risks, and with a few notable exceptions such as the financial industry where cybersecurity spending is high due to the alignment of incentives through the imposition of liability for breaches, the overall growth in cybersecurity spending remains relatively low according to Gartner Research. Spending on cybersecurity grew at 12% compound annual growth rate (CAGR) in 2018, and it was projected to decline to 7% CAGR by 2023.[10]

However, more recent reporting from Gartner has noted that in fact global cybersecurity spending was now projected to reach $215 billion in 2024, reflecting a 14.3% increase from $188.1 billion in 2023. The growth is driven by increasing cyber threats, cloud adoption, and data privacy regulations. Notably, cloud security spending is expected to grow by 24.7%, and data privacy investments are projected to rise by over 24% as organizations prioritize compliance with stringent data protection rules.[11]

3. Legal

Unlike other jurisdictions such as the European Union, the U.S. government has no comprehensive federal law that regulates information security, cybersecurity, and privacy throughout the country. Instead, sector-specific laws have been prioritized with a special focus on healthcare and financial firms.

As a result, many states have passed laws to address these governance gaps. This creates a unique challenge for organizations that conduct business across state lines, as these areas are currently regulated by a piecemeal of sector-specific federal laws and state legislation. Some states have been more active in adopting cybersecurity laws than others, although some categories of cybersecurity have been commonly adopted. Some of the areas seeing the most recent legislative activity include:

- **Increasing** penalties for cybercrimes.
- **Auditing** cybersecurity within the insurance industry.
- **Regulating** government agencies to implement training and security policies and practices to better improve incidence response and preparedness.
- **Creating** task forces and commissions to study or advise on cybersecurity issues.
- **Supporting** programs and incentives for cybersecurity training and education.
- **Expanding** enforcement of privacy violations.

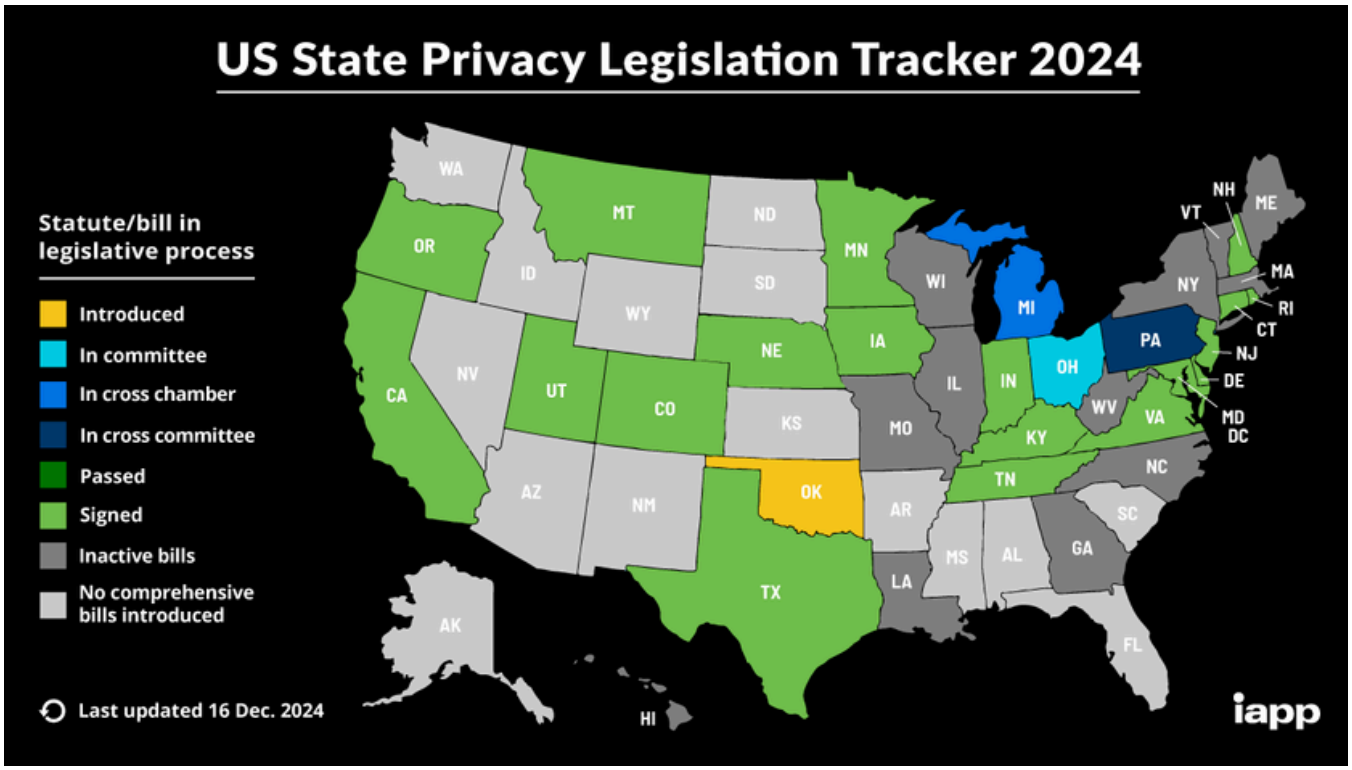


Figure 1: U.S. Privacy Legislation Tracker 2024

It is also worth noting that new, state-level, comprehensive data privacy laws also have important cybersecurity components. The current state of such privacy laws is encapsulated in Figure 1, courtesy of the International Association of Privacy Professionals (IAPP).

State privacy laws in the U.S. are enacted to regulate how businesses and other entities collect, use, store, and share personal information. These laws vary widely by state, both in scope and in specific requirements. Some states, like California with its California Consumer Privacy Act (CCPA) and subsequent California Privacy Rights Act (CPRA), provide robust rights to individuals, such as the right to access, delete, and correct personal data, as well as to opt out of data sales. Other states, like Virginia and Colorado, have enacted comprehensive frameworks that focus on consumer rights, data controller responsibilities, and data processing requirements.

Certain states have implemented laws defining "reasonable cybersecurity" with varying approaches. States like California and Ohio define "reasonable" by referencing widely accepted frameworks such as NIST and CIS Top 20, providing clear guidance for compliance. See Figure 2.[12]

These definitions often include additional safeguards, such as specifying protective measures businesses must adopt, and sometimes offer safe harbor protections for those adhering to recognized standards.

Figure 2: "Reasonable" Cybersecurity Summary Table

B. Steps to Managing Cyber Risks

Analysts have recommended that organizations of all sizes manage cyber risk by **(1) being aware**, **(2) being organized**, and **(3) being proactive**.[13] As we discuss below, each of these steps can potentially include a wide range of technical and business activities.

1. Be Aware

Managers and policymakers need to keep up to date on the growing variety of cyber threats facing their organizations, especially as an increasing number of workers are working remotely. Phishing and ransomware campaigns are especially prevalent during the pandemic.[14] Cybercriminals have taken advantage of the current global health crisis, for example, and the new technical configurations that result from a remote workforce to multiply the number of attacks.[15] In response, organizations of all sizes need to be aware of the variety of cyber threats facing their organizations. A range of cybersecurity best practices can help firms better understand their vulnerabilities, including network traffic analysis using deep packet inspection. [16]

2. Be Organized

Protecting an organizations' physical infrastructure is only the first step in safeguarding its assets; in many ways, digital assets and information is increasingly the lifeblood of both government entities and private firms. One example of this fact is the extent to which the intangible assets comprising the S&P 500 flipped from the 1970s to 2018, at which point intangibles such as intellectual property and reputation comprised 84% of corporate value.[17] Organization is vital to protect such invaluable digital assets, yet even a computer that is "air gapped," or unplugged from the public Internet may still be accessible via flash drive or rewritable CD introduced by an insider threat. Large companies like Sony did not even have a Chief Information Security Officer until relatively recently. It hired one in the aftermath of its 2011 breach, but that did not save them from being breached again in 2014.[18] Still in 202, both leadership structures and accountability remains muddy in too many organizations across Indiana.

3. Be Proactive

In general, the best cyber defense is a healthy skepticism and proactive vigilance backed up by a robust program of cyber hygiene and an updated incident response plan. Employees who do not have appropriate cybersecurity skills can unintentionally create vulnerabilities in a network. For example, it has been reported that 91% of cyber-attacks start with a phishing email – an issue that may be addressable by training.[19] Network security policies ensure that employees have access to the correct and appropriate information, and play a key role in preventing breaches from occurring.

However, designing security policies to strike the correct balance between security and convenience is not an easy undertaking. For example, consider the difficulty of monitoring employees who are working remotely. One study found that 78% of IT specialists reported that their end users had set up unapproved services and applications, which increased the chance of a potential unmanaged risk.[20] Hiring qualified personnel is another source of concern, as demonstrated by the fact that there are currently more than 3.5 million unfilled cybersecurity jobs.[21]

In general, it is essential that organizations have resources and tools in place that allow them to adhere to and manage security policies. Anything that forces people to drastically change the way they work or results in an organization's lack of agility is counterproductive. An ideal solution should offer increased security entwined with business agility, which is an arena where cyber risk insurance can help.

C. Current Trends in Addressing Cyber Risk

Cyber risk evolves as quickly as the technology, social context, and policies underlying information systems. Although this evolution occurs in myriad ways, in this section we focus on three of the most prominent issues in cyber risk management today: the continuing importance of cyber risk insurance, the emergence of Artificial Intelligence (AI) as a tool for identifying and responding to cyber incidents, and the impact of the COVID-19 pandemic on technology practices and risks.

1. Cyber Risk Insurance

Cyber risk insurance has long been thought of as an integral component to managing cyber risk. Insurance firms have been experimenting with cyber risk insurance policies for decades.[22] By some estimates the market was worth more than $2.5 billion in 2020, with projections that it could triple by 2030,[23] a trend that could be reinforced by regulatory developments such as the California Consumer Privacy Act (CCPA) or the EU's General Data Protection Regulation (GDPR).[24] Indeed, U.S. companies are increasingly eyeing cyber insurance as they potentially face millions of dollars in liability under CCPA, under which state residents can seek up to $750 per data security incident. The CCPA also directs the California Attorney General to take enforcement actions for privacy violations.[25]

In addition to protecting organizations against financial fallout from cyber incidents, organizations can use cyber risk insurance to inform their security practices in other ways. For example, insurers can use tactics like cyber-meteorology to audit companies against cyber risks and help them prioritize their security efforts.[26] The insurance industry has also focused extensively on their own cybersecurity practices. Model laws like the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law seek to establish data security standards for regulators and insurers in order to mitigate the potential damage of future data breaches. This Model Law, which has been enacted in at least 11 states as of September 2020, requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program based on a recognized risk assessment tool, with a designated employee in charge of the information security program. The model does not create a private cause of action, nor does it limit an already-existing private right of action. As such, it is less a new approach to regulating cyber risk insurance than an encouragement for covered insurance providers to adopt an approved set of cybersecurity tools and frameworks.

However, with 49 states still not mandating cyber insurance, adoption has been slow. Deloitte's 2019 Middle Market Cyber Insurance Survey reported cost and coverage limits being the main deterrent from purchasing cyber risk insurance.[27] However, much is still unknown about how companies decide whether to adopt cyber risk insurance, and the broader role that cyber risk insurance plays in cyber risk mitigation practices, which is a key topic on which this survey focuses.

Moreover, cyber risk insurance does not protect companies against all types of cyber risks. The full impact of some potential risks may be difficult to quantify and thus difficult to fully insure. Insurance policies may exclude coverage of incidents that happen under certain circumstances, such as a cyber-attack that is attributed back to a foreign nation that may be defined as an act of war. Businesses must carefully review policies to ensure that their expectations about what types of incidents are covered aligns with their policies, which can create barriers to adopting policies.

2. Artificial Intelligence

Artificial intelligence (AI) has been sought as the next frontier for protection against cyber threats.[28] An automated, zero-time prevention platform can reduce the array of duties typically carried out by a cybersecurity team, which helps mitigate the prevailing cybersecurity workforce shortage, though no piece of software however advanced can replace a well-trained and well-rounded cybersecurity professional. Automated systems can, though, create alerts about anomalous activities that need to be investigated by human analysts, which can turn out to be benign. Moreover, as new threats arise, security solutions that use AI must be re-trained to keep up.[29] Deep learning prediction models can produce a far lower level of false positives than traditional AI systems, which typically experience an approximately 1% false positive rate.[30] It is designed to automatically identify the relevant features of a malicious file or vector without engineering from a cybersecurity expert. Already, AI tools are being used by the insurance industry to assess the cyber risks facing organizations.[31]

3. Cybersecurity During the Pandemic

CIOs and CISOs have been under intense pressure to meet the needs of homebound workers, while concurrently needing to take added steps to safeguard their enterprise networks. Organizations recognize the new risks associated with new types of employees working from home that have not done so prior to the pandemic. Mitigating the risks of a remote workforce largely comes down to ensuring the business is using the right security and that IT leaders are educating their employees on best practices around security as we navigate this crisis.

From an organizational standpoint, it is now more critical than ever to have the right technology in place and to make sure equipment is up to date and secure.

It is also crucial for remote employees to exercise good cyber-hygiene. Organizations attempting to decide how to change their cybersecurity practices in light of COVID-19-related changed to work practices may find it helpful to consult decision-making frameworks such as the NIST Cybersecurity Framework or the Indiana University Center for Applied Cybersecurity Research Information Security Practice Principles.

In our 2020 report, we predicted that COVID-19 may also change the planned use of cyber risk insurance, potentially for many years to come. The Cowbell Economic Impact of Cyber Insurance reported 65% of small and mid-Size Enterprises in the U.S plan to spend more on cybersecurity insurance over the next two years. More than half believe the cost of insurance is well worth the protection, on average, firms opt for cybersecurity insurance coverage limits of about 0.14% of revenue. By comparison, only 58% of large US-based enterprises plan to spend more on cyber-insurance over the next two years.[32]

In actuality, what we witnessed was a surge in ransomware attacks during the pandemic, along with expanding attack surfaces due to the continued prevalence of remote work and IoT products. Insurance premiums also increased over 22% in the United States according to NAIC, with a 2022 Marsh report finding that premiums had doubled in some regions due to the prevalence of ransomware campaigns.[33]

Methods

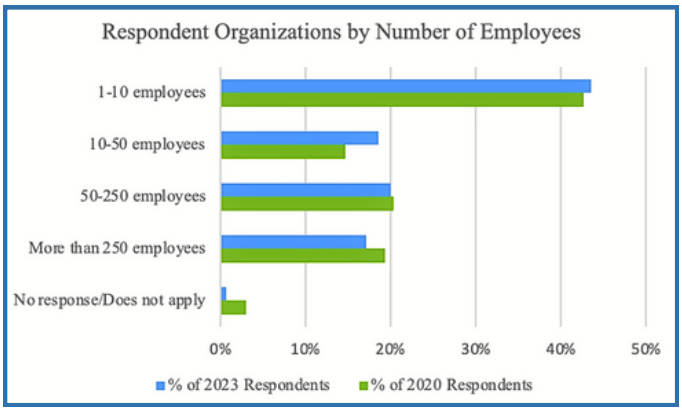
A. Aims of this Study

The goal of this project was to explore cybersecurity practices amongst Indiana organizations and understand how those practices may have changed since 2020. To answer these questions, we conducted a survey of Indiana organizations to elicit information about their cyber risk perceptions, cyber risk management and planning, and use of cyber risk insurance.

This survey built on our prior experience surveying Indiana organizations about their cybersecurity practices in 2020 (Boustead et al. 2020). To design our 2023 survey instrument, we began with the questions asked in our 2020 survey instrument, which had been developed through extensive discussion with subject matter experts and consultation with key informants. However, we revised some questions to streamline the survey based on feedback from our 2020 respondents and added additional questions asking about changes in cybersecurity practices since spring 2021 (representing the end of remote work due to the COVID pandemic). The completed survey is available in Appendix A.

B. Survey Development and Distribution

The goal of this project was to explore cybersecurity practices amongst Indiana organizations and understand how those practices may have changed since 2020. To answer these questions, we conducted a survey of Indiana organizations to elicit information about their cyber risk perceptions, cyber risk management and planning, and use of cyber risk insurance. This survey built on our prior experience surveying Indiana organizations about their cybersecurity practices in 2020 (Boustead et al. 2020). To design our 2023 survey instrument, we began with the questions asked in our 2020 survey instrument, which had been developed through extensive discussion with subject matter experts and consultation with key informants. However, we revised some questions to streamline the survey based on feedback from our 2020 respondents and added additional questions asking about changes in cybersecurity practices since spring 2021 (representing the end of remote work due to the COVID pandemic). The completed survey protocol is available in Appendix A.



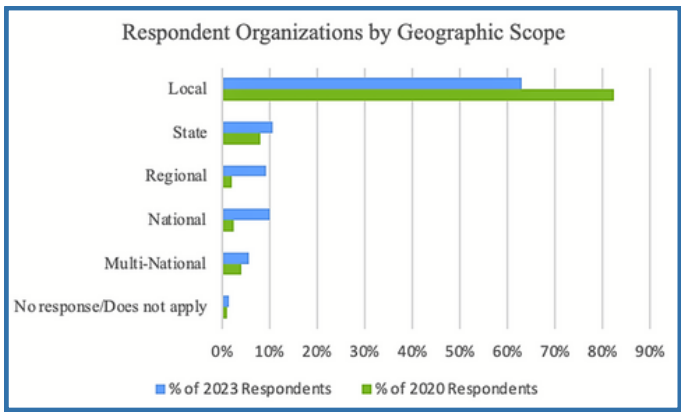


Figure 3: Description of Respondent Organizations

Almost a third of 2023 respondents were from government sector organizations; educational services (11%) and health care/social assistance (10%) were the next most represented sectors. Because organizations may account for the sensitivity of the information they encounter in their cybersecurity planning, we also asked respondents about the types of information handled by their organization.

Eighty-two percent of respondents reported handling some form of personal data, underscoring the critical need for strong data protection practices. Figure 4 illustrates the types of data most commonly processed by these organizations. Respondents indicated that personally identifiable information (PII)—such as home addresses, email addresses, and Social Security numbers—was the most frequently handled type of data.

This was followed by personal financial information, including credit card numbers, banking details, and credit scores, and then by personal health information, such as allergy histories, blood pressure readings, and records of past medications. The prevalence of these sensitive data types highlights the importance of cybersecurity frameworks tailored to the specific risks associated with each category, particularly in sectors that routinely handle large quantities of such information.

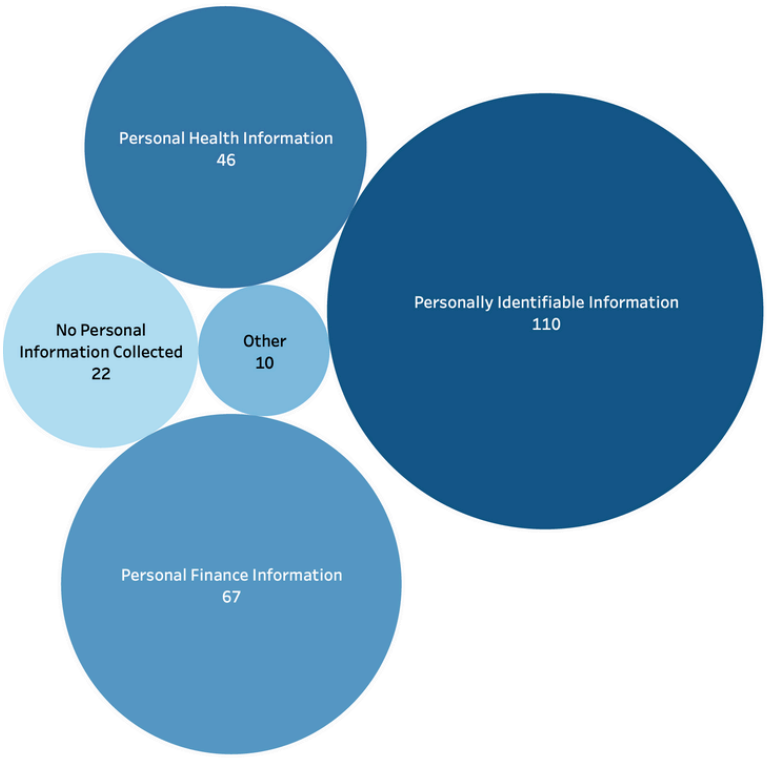


Figure 4: Types of Data Handled by Respondent Organization

C. Limitations

There are several notable limitations to this research. Most importantly, our survey was conducted using a convenience sample of respondents, meaning that our results cannot be generalized to all organizations in Indiana (or to US organizations in general). Our results should therefore be understood to be exploratory in nature, providing insights about the behavior of a particular group of respondents. Additionally, for privacy reasons our survey is distributed in a way that does not enable us to match respondents from our 2023 survey with respondents from our 2020 survey.

Although we compare our 2020 and 2023 results where possible, it cannot be determined whether observed differences are due to changes in behavior within respondents or differences in our 2020 and 2023 respondent pool. To address this limitation, we added a number of questions asking respondents about how their organization's cybersecurity practices have changed since 2021, providing insights about changes over time.

Nevertheless, this analysis can provide key insights to inform cybersecurity policymaking in Indiana today. It provides a description of mechanisms used by organizations to protect their information and mitigate potential attacks, which can be used to identify practices currently employed by organizations in the state. It explores the reasons why these practices have not been adopted, which can provide insights about barriers that governmental organizations may seek to address.

Results

In this section, we summarize and discuss the responses provided by the Indiana organizations that participated in our survey. We focus specifically on describing cyber risk **perceptions**, **planning**, and **responses**. When possible, we contextualize these responses with reference to other sources of data.

A. Risk Perceptions & Experiences

1. Potential Events & Consequences

The overwhelming majority - over 95% - of respondents indicated that their organization was somewhat concerned or very concerned about the risk of a cyber security incident. Respondents were divided on whether their organization had become more concerned about cybersecurity threats over time, with slightly less than half of respondents indicating that their organization was as more concerned more much more concerned about the risk of a cyber security incident than they were in spring 2021, and slightly less than half of respondents indicating that their organization had about the same level of concern.

Respondents were then asked about the types of cybersecurity incidents that their organization was concerned about. As can be seen by Figure 5, respondents to our 2023 survey most frequently reported that their organization that their organization was concerned about phishing attacks (reported by 82% of 2023 respondents), ransomware attacks (reported by 78% of 2023 respondents), and malware attacks (reported by 76% of 2023 respondents). These findings are similar but slightly different to the concerns reported by our 2020 respondents–who were most concerned about malware (reported by 87% of 2020 respondents), phishing (reported by 76% of 2020 respondents, and ransomware (reported by 75% of 2020 respondents).

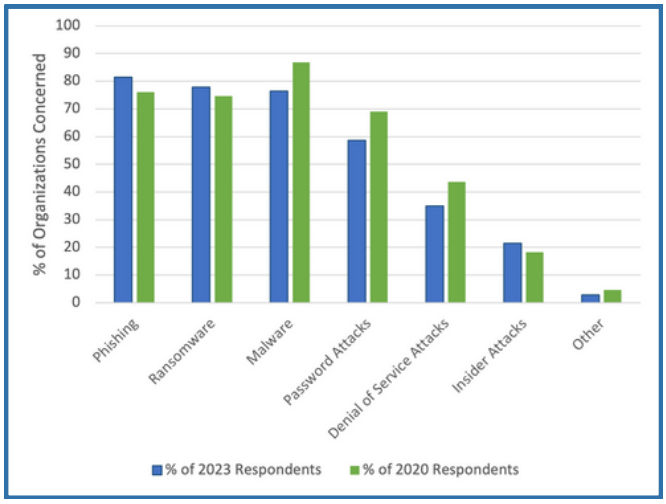


Figure 5: Proportion of Respondents Concerned About Cyber Incidents, By Type

The survey responses regarding cybersecurity concerns show some alignment with actual incident data, but also reveal some discrepancies between perception and reality. According to a 2021 analysis of the most common types of cyber incidents by the Government Accountability Office, business email compromises (which are generally the target of phishing) were by far the most common type of incident, aligning with respondents' high level of concern about phishing attacks.[34] In 2021, business email incidents accounted for 77% of the reported most common attacks. This validates the 82% of respondents who

expressed concern about phishing attacks. However, the survey results indicate that ransomware was perceived as the most concerning threat by 30% of respondents, with 78% expressing concern about it overall. This perception appears somewhat misaligned with the actual incident data. While ransomware attacks did represent 14% of reported cyber incidents in 2021, they were still far less common than business email compromises or data breaches.

It is important to note that phishing attacks and ransomware incidents are often closely linked. Phishing serves as the initial attack vector for more than 90% of cyber attacks, including ransomware deployment.[35] This connection between phishing and ransomware may partly explain why ransomware is perceived as such a significant threat. While ransomware incidents themselves may be less frequent, the prevalence of phishing attacks means that the potential for ransomware deployment is constantly present.

Organizations may anticipate a broad range of potential consequences from cyber incidents. Respondents reported concerns about data breaches leading to loss or theft of sensitive information, which could result in reputational damage, financial losses, and legal liability. Operational disruptions were another key concern, with many organizations fearing that cyber attacks could halt critical business processes and cause significant downtime and lost productivity. Financial impacts were also considered, including direct costs from ransom payments, recovery efforts, and potential fines for non-compliance with data protection regulations. Additionally, respondents expressed worry about long-term effects on customer trust and business relationships, which could have lasting impacts on an organization's market position and overall viability.

As can be seen by Figure 6 below, respondents to our 2023 survey most frequently indicated that their organization was concerned about data being deleted or lost (reported by 76% of 2023 respondents), data being exposed to outsiders (as reported by 68% of 2023 respondents), and identity theft (as reported by 58% of 2023 respondents). These findings are similar to the concerns reported by our 2020 respondents, although identity theft was more commonly reported by our 2020 respondents. When asked to rank the potential consequences they identified as concerning, about 24% of respondents indicated that their organization was most concerned about data being deleted or lost while about 18% of respondents identified data being exposed to outsiders as most concerning.

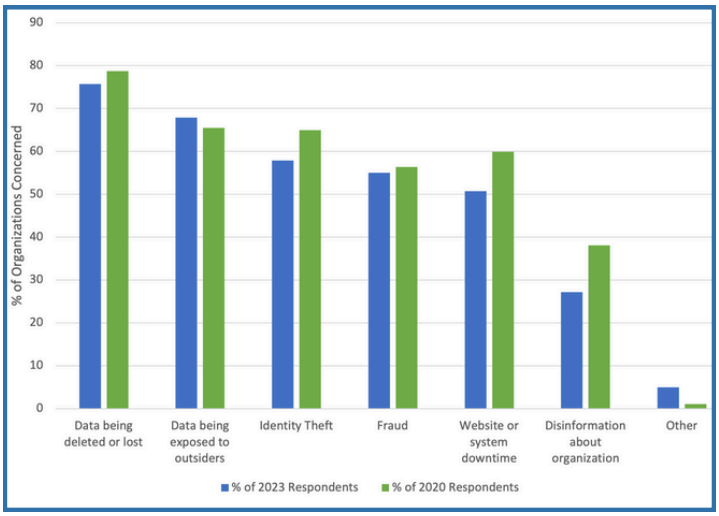


Figure 6: Proportion of Respondents Concerned About Consequence of Cyber Incidents, By Type

To assess the alignment between perceived risks and actual financial impacts, we can compare the survey results on organizational concerns with the small and medium-sized business (SMB) data from CISA's Cost of a Cyber Incident report. While survey respondents were most concerned about data being deleted or lost (76%), data exposure (68%), and identity theft (58%), the cost data suggests that these concerns may not align perfectly with the most significant financial impacts of cyber incidents.

For SMBs, the highest mean costs were associated with total incident costs ($178,000), total payouts ($136,000), and crisis services costs ($112,000).

Notably, forensics costs, which could be related to investigating data loss or exposure, had a mean cost of $72,000. Credit/ID monitoring costs, which might be implemented in response to identity theft concerns, had a relatively lower mean cost of $45,000. For larger entities, while the sample size is smaller, the costs are significantly higher across all categories, with total incident costs averaging $5.55 million and crisis services costs averaging $3.84 million.

Interestingly, while data exposure was a top concern in the survey, the specific costs related to notification ($75,000 mean for SMBs) and credit/ID monitoring ($45,000 mean for SMBs) were not the highest cost categories. This suggests that while these are valid concerns, they may not represent the most significant financial risks. The data also highlights substantial costs in areas that may not have been top-of-mind for survey respondents, such as legal damages and lost business income, which for SMBs had mean costs of $264,000 and $343,000 respectively. This discrepancy between perceived risks and actual costs underscores the importance of comprehensive risk assessment and mitigation strategies that address both the most concerning and the most costly aspects of cyber incidents.

B. Managing Cyber Risk

1. Prevention and Mitigation of Cyber Incidents

Eleven percent (N=16) of respondents reported that their organization had experienced a successful cyber attack since spring 2021.This is comparable to the findings of our prior report, in which 19% of respondents indicated that their organization had experienced a successful cyber incident in the past three years.

As is shown in Figure 7 below, respondents reported that their organization engages in a broad range of cybersecurity practices.Use of antivirus software was the most commonly reported cybersecurity practice, followed by use of remote backups, updating and patching software, and automatic updating of operating systems and software. In order to gauge how cybersecurity practices have changed since the move to remote work during the pandemic, we also asked respondents whether their organizations had adopted any of the practices they reported since spring 2021. Respondents most commonly described multifactor authentication (40% of respondents) as being adopted since spring 2021, followed by remote backups (26% of respondents) and antivirus software (21% of respondents).

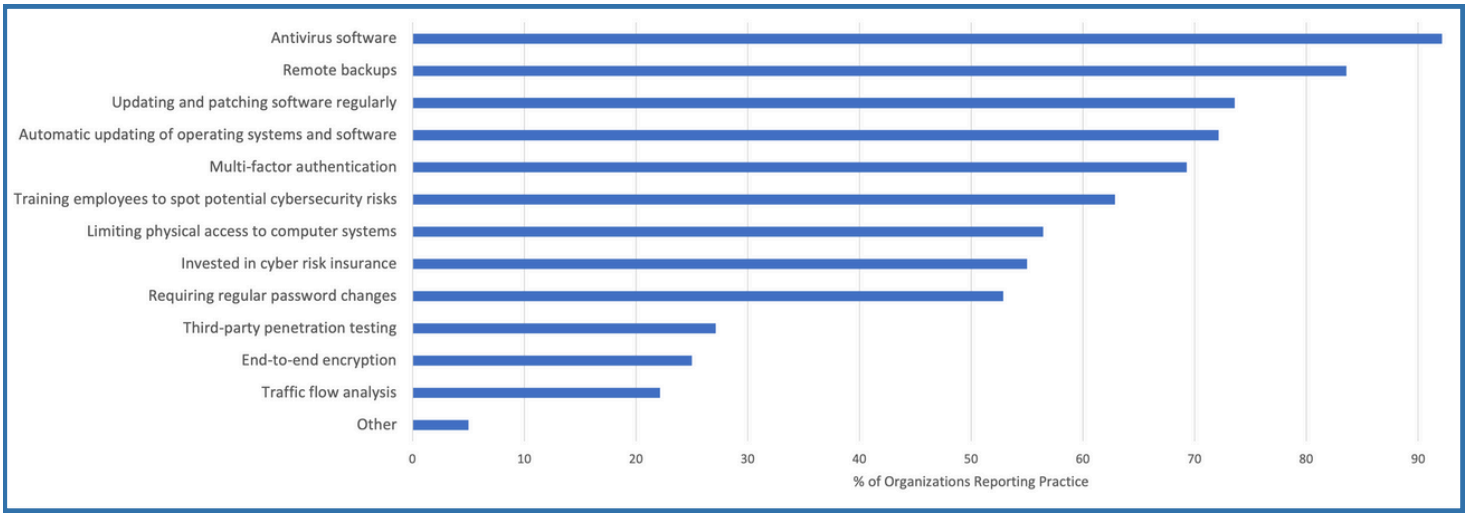


Figure 7: Cybersecurity Practices Adopted by Responding Organizations

There are a broad range of external and internal cybersecurity tools available for use by organizations. As is shown by Figure 8 below, respondents most frequently reported that their organization had revised or updated their incident response plan to ensure that cyber threat information as getting where it was needed (34% of 2023 respondents), consulted news reports (33% of 2023 respondents) and joined an information sharing group such as an ISAC (17% of 2023 respondents).

These findings were largely similar to those reported by our 2020 respondents, although a higher proportion of 2020 respondents reported that their organization had joined an information sharing group (21% of 2020 respondents compared with 17% of 2023 respondents), a higher proportion of 2023 respondents reported that they relied on government data (26% of 2023 respondents compared with 21% of 2020 respondents) and a higher proportion of 2023 respondents reported that their organization had launched a cyber hygiene campaign (18% of 2023 respondents compared with 11% of 2020 respondents).

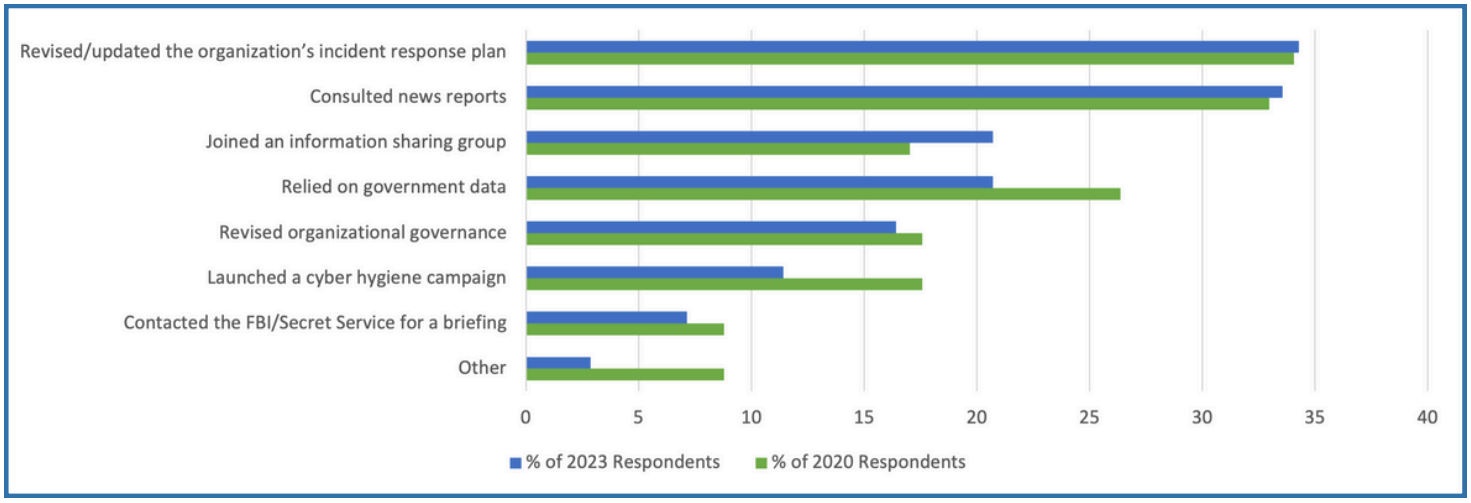


Figure 8: Cybersecurity Tools Used by Responding Organizations

2. Management, Training, & Documentation

Organizations must make critical but difficult decisions about how to allocate responsibility for managing cyber risk. As is shown in Figure 9 below, there was a substantial amount of variation in who respondents indicated was ultimately responsible for managing cyber risks at their organization. A plurality of respondents (29%) indicated that their organization's Chief Executive Officer was ultimately responsible for managing cyber risks, with other executive figures (such as a town manager or clerk-treasurer) and other staff members (such as an office manager) as the next most common responses. Most of our respondents reported that few if any cybersecurity professionals were employed at their organization, with the majority of respondents (67%) indicating that there were no cybersecurity professionals currently employed and 26% indicated that their organization employed 1-5 cybersecurity professionals.

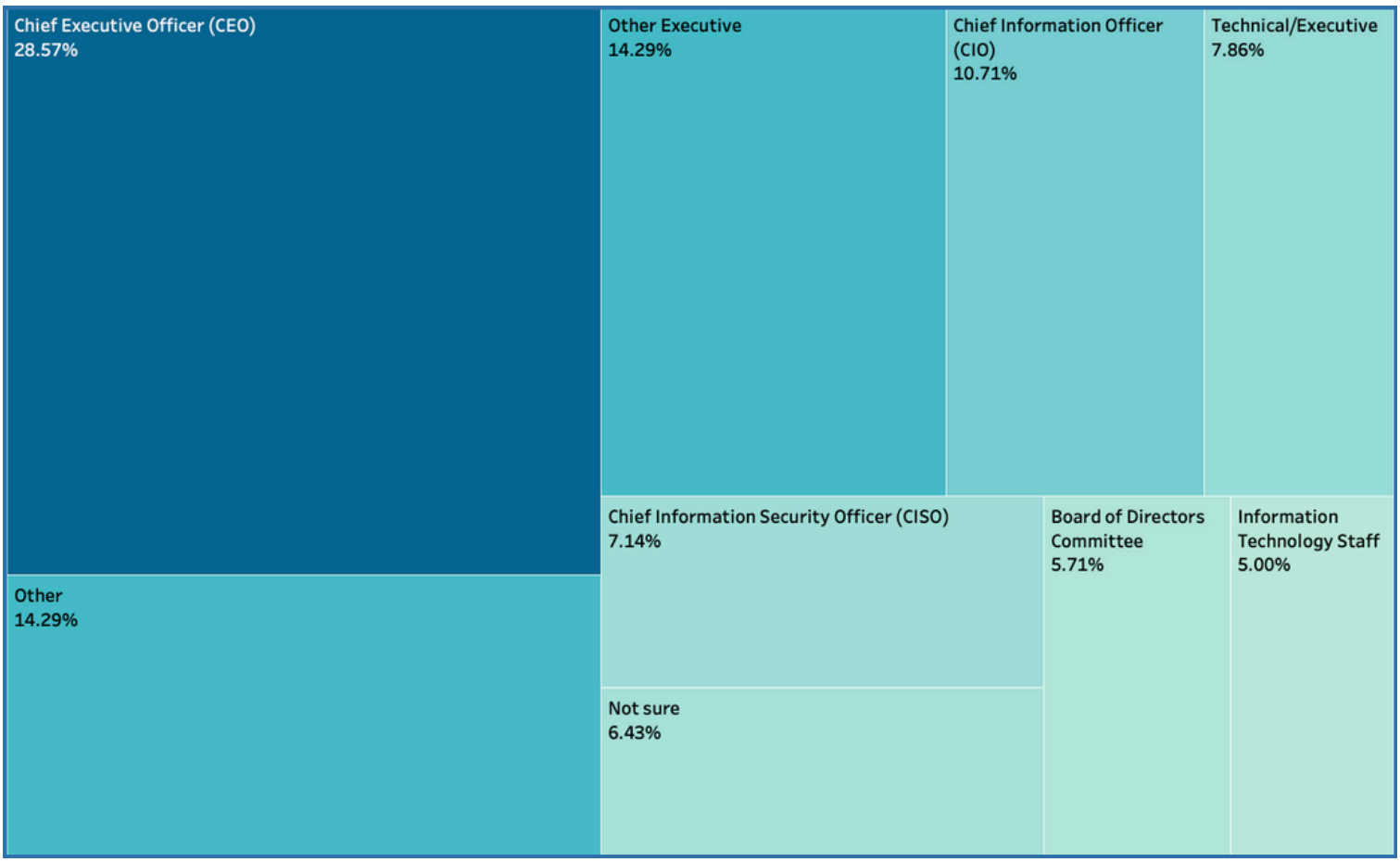


Figure 9: Person Ultimately Responsible for Managing Cyber Risks at Responding Organizations

Almost 63% of respondents reported that their organization had provided any training intended to raise awareness of the potential for cybersecurity threats like hacking, phishing, spamming, or other threats related to stealing or compromising digital data. Slightly more than half (52%) of those who indicated that their organization had provided any training indicated that they had received formal cybersecurity training from their organization. Among respondents who had received cyber security training, 43% indicated that their received such training once a year and 39% indicated that they received it once a quarter, with remaining respondents receiving less frequent training. Forty-seven percent of respondents who indicated that their organization provided any training reported that others in their organization had received formal cybersecurity training.

Effective planning is the foundation of a strong cybersecurity strategy. It enables organizations to proactively defend against threats and respond quickly to incidents. Documentation plays a crucial role in this planning process. Through proper planning, organizations can anticipate potential threats, efficiently allocate their resources, and react promptly to security breaches.[36] Forty-six percent of respondents indicated that their organization did not have written documentation related to cybersecurity planning and response, 41% indicated that their organization did have such documentation, while 13% of respondents were unsure. Furthermore, respondents that reported that their organization did have cybersecurity documentation generally did not have strong feelings about the quality and timeliness of this documentation.

C. Role of Cyber Risk Insurance

Cybersecurity insurance is a specialized form of coverage designed to protect organizations from financial losses resulting from cyber attacks or data breaches, and it has become more important as such incidents are increasingly common and costly. Sixty-four percent of respondents indicated that their organization had insurance specifically tailored to cover cyber incidents, 21% indicated that their organization did not have such insurance, and the remainder of respondents were unsure. This represents a higher rate of cyber risk insurance uptake than observed in our prior survey, where about half of respondents reported that their organization had cyber risk insurance.

According to our survey, the price of cyber risk insurance appears to be increasing: 58% of respondents whose organizations had cyber risk insurance reported that the price of this insurance had increased since spring 2021, compared with only 6% of these respondents indicated that the price of this insurance had decreased since spring 2021. Cyber risk insurance plans may provide coverage for a range of losses to the insured (also known as first party losses) stemming from a cyber incident. Figure 10 below shows the types of first party losses reported by our respondents as covered by their cyber risk insurance plan (amongst respondents who indicated that their organization had cyber risk insurance). As can be seen, our respondents most commonly indicated that their organization's cyber risk insurance plan included coverage for damages to computer or information systems (69%), followed by coverage for business interruptions related to denial of service or other downtime (58%) and cost of notifying affected customers or others whose data was exposed in a breach (57%).

Cyber risk insurance plans may also provide coverage for a range of losses to entities other than the insured (also known as third party losses) stemming from a cyber incident. Amongst respondents who indicated that their organization had cyber risk insurance, our respondents most commonly indicated that their organization's cyber risk insurance plan included costs for legal defenses related to the data breach (51%), claims for damages from customers or others whose information was exposed in the breach (40%), and fines and penalties (33%).

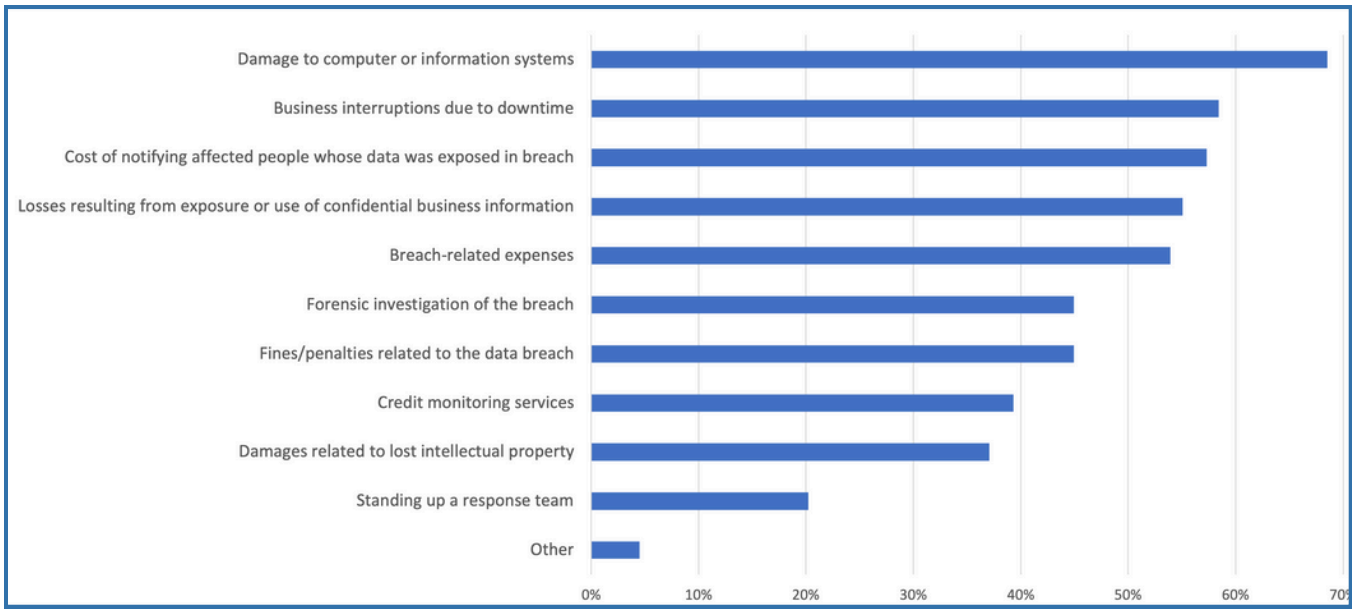


Figure 10: First Party Losses Covered by Respondent Organization's Cyber Risk Insurance

In addition to reimbursing organizations for harms suffered during a cyber incident, cyber risk insurance may also improve cybersecurity by requiring insured organizations to undertake certain protective measures. About 67% of respondents whose organizations had cyber risk insurance indicated that this policy requires their organizations to undertake certain security measures. As can be seen by Figure 11 , employee training/cyber hygiene and mandatory, automatic patching were the most frequently mandated security practices; more than 50% of respondents who indicated that their organizations cyber risk insurance policy mandated security practices reported that these where amongst the practices were required.

Respondents were able to indicate that their organization's cyber risk insurance practice mandated a security practice not mentioned by the survey; respondents who selected this "other" option most often reported that their organization's cyber risk insurance mandated two factor or multi-factor authentication.

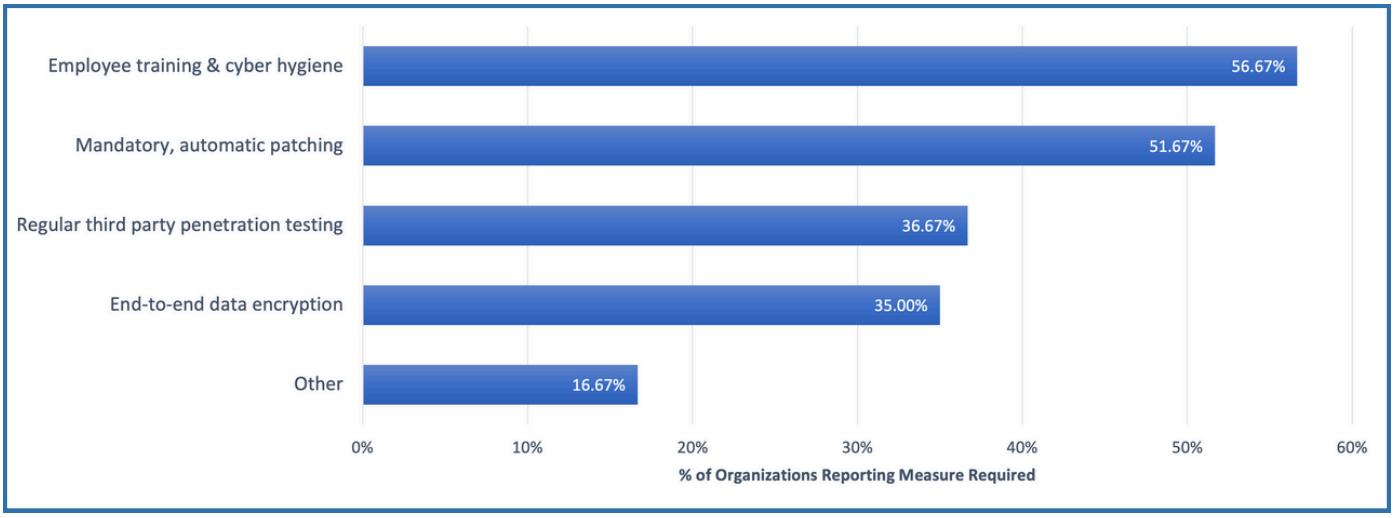


Figure 11: Cyber Risk Mitigation Measures

Discussion

A. Shifts in Cyber Threat Perceptions

The 2023 survey results reveal both encouraging progress and persistent gaps in cybersecurity practices among Indiana organizations when compared to the 2020 survey. While awareness of cyber risks has increased, the findings also expose a disconnect between the perceived importance of cybersecurity and the actual adoption of protective measures. These insights have profound implications for businesses, policymakers, and stakeholders, particularly regarding resource allocation, regulatory priorities, and the need for more targeted support.

One of the most informative findings is the shift in organizations' perceived cyber threats and their understanding of the broader risk landscape. In 2023, phishing attacks emerged as the most concerning cyber threat, surpassing malware, which had been the primary concern in 2020. This shift aligns with broader trends in cybersecurity, as discussed above. The rise in ransomware concerns—identified by 78% of respondents and ranked as the most concerning threat by 30%—also more accurately reflects the reality of cyber risks.

The survey highlights a potential misalignment between perceived threats and actual incident data in other areas. While ransomware incidents are highly visible and costly, they represent a smaller proportion of reported cyber incidents compared to phishing-based attacks, which accounted for most incidents nationally in recent years. This discrepancy suggests that organizations still overestimate the likelihood of certain high-profile attacks while underestimating the prevalence of other risks.

B. Adoption of Cybersecurity Practices

Another important area of change is the adoption of cybersecurity best practices. The survey indicates that organizations have increasingly implemented measures such as multifactor authentication, remote backups, and regular software updates since 2021. These practices are critical, particularly in the context of remote and hybrid work environments. Despite these positive developments, significant gaps remain. Many organizations still lack basic protections that are relatively simple to implement, such as antivirus software or documented cybersecurity plans. Additionally, the survey found that nearly half of responding organizations did not provide formal cybersecurity training to employees, leaving them vulnerable to social engineering attacks.

1. The Disconnect Between Awareness and Action

The highlight a persistent disconnect between organizations' expressed concern about cybersecurity and their actual adoption of protective measures. While over 95% of respondents indicated that their organization was somewhat or very concerned about cyber risks, only a small subset reported engaging in comprehensive cybersecurity planning and all best practices. Several factors contribute to this disconnect. Resource constraints are a major issue, particularly for smaller organizations, which often lack the financial and human capital to invest in

advanced cybersecurity measures. Limited expertise within organizations further compounds the problem, as many respondents indicated that they had no dedicated cybersecurity professionals on staff. Moreover, some organizations may perceive themselves as less attractive targets for cyber attacks due to their size or sector, leading to complacency.

2. Cyber Insurance

The survey also highlights the importance of cyber risk insurance as a tool for managing financial exposure to cyber incidents. The proportion of respondents reporting that their organization had cyber risk insurance increased from approximately 50% in 2020 to 64% in 2022. This growth reflects a growing recognition of the financial risks posed by cyber attacks and the value of insurance in mitigating those risks. However, the rising cost of cyber risk insurance—reported by 58% of respondents with coverage—presents a challenge for smaller organizations. Policymakers could explore ways to address this issue, such as creating state-supported risk pools or offering subsidies to make cyber insurance more accessible.

Cyber risk insurance also has the potential to drive improvements in organizational cybersecurity. Many insurers now require policyholders to implement certain protective measures as a condition of coverage. The survey found that employee training and automatic software patching were among the most frequently mandated practices under cyber insurance policies. These requirements not only reduce the likelihood of successful attacks but also encourage organizations to adopt a proactive approach to cybersecurity. Expanding the use of such conditional coverage requirements could further enhance the cybersecurity posture of insured organizations.

3. Bipartisan Support for Cybersecurity

The survey also provides a foundation for fostering bipartisan support for cybersecurity initiatives. Cybersecurity transcends political divides, making it an area where stakeholders from across the spectrum can collaborate to address shared challenges. Investments in cybersecurity infrastructure, training, and awareness campaigns have the potential to yield broad benefits, strengthening the resilience of organizations and communities against evolving cyber threats.

Policy Opportunities

A. Awareness Training

The survey findings show a positive trend in need of support. Indiana organizations have demonstrated increased awareness of cyber risks and taken meaningful steps toward adopting essential protections. However, substantial gaps persist, particularly among smaller organizations and sectors constrained by limited resources. These gaps—manifesting as incomplete cybersecurity planning, insufficient employee training, or a lack of best practice adoption—create vulnerabilities that could lead to severe financial and operational consequences. The policy recommendations below aim to address these challenges, empower organizations, and enhance Indiana's overall cybersecurity posture.

B. Increase Access to Financial Support for Cybersecurity Measures

A prominent obstacle to implementing robust cybersecurity measures is cost, especially for small and medium-sized organizations. Many respondents reported that resource limitations prevented them from adopting critical practices, such as conducting employee training or maintaining up-to-date incident response plans. To overcome these challenges, state and local governments should establish grant programs specifically designed to support smaller organizations. These grants could offset the cost of essential cybersecurity tools, including antivirus software, firewalls, and secure backup systems. Additionally, policymakers could incentivize investment through tax credits for organizations that undertake training, risk assessments, or other cybersecurity enhancements.

Policymakers should also explore public-private partnerships to deliver cost-effective, scalable solutions. For example, collaborating with technology providers could enable discounted access to managed cybersecurity services or cloud-based security solutions tailored for small businesses and nonprofits.

C. Expand Cybersecurity Education and Training Programs

The survey revealed significant room for improvement in formal cybersecurity training, with nearly half of respondents indicating that their employees lacked such training. This shortfall highlights the urgent need for accessible, statewide education and training initiatives. Policymakers should prioritize developing free or low-cost programs aimed at improving cybersecurity literacy for employees and organizational leaders alike.

These initiatives could be interactive workshops, webinars, and self-paced online courses addressing common threats, such as phishing and ransomware. Industry-specific training programs would be particularly beneficial for sectors like healthcare and education, which have unique regulatory and operational challenges. Partnering with industry associations, universities, and community colleges to deliver these programs could also enhance accessibility and impact of these initiatives.

Expanding mandatory cybersecurity awareness training for government employees and contractors could set a strong example for the private sector. Policymakers might also consider requiring state-funded organizations or grant recipients to demonstrate baseline cybersecurity practices, such as conducting regular employee training.

D. Promote Cyber Risk Insurance Accessibility

Cyber risk insurance is becoming a critical tool for managing financial exposure to cyber incidents. However, the rising cost of coverage presents challenges, particularly for smaller organizations. While 64% of respondents reported having cyber insurance, smaller organizations were less likely to carry such policies, often citing cost as the primary deterrent. To encourage broader adoption, policymakers could establish state-sponsored cyber insurance pools to provide affordable coverage for small and medium-sized businesses. Alternatively, subsidies for first-time cyber insurance purchasers could help organizations overcome the financial barriers to securing coverage. Insurers frequently require policyholders to implement specific security measures, such as multifactor authentication or regular patching, as conditions for coverage. Policymakers could collaborate with insurers to standardize these requirements, ensuring alignment with broader cybersecurity best practices. This approach would yield dual benefits: increased adoption of insurance and improved organizational security.

E. Encourage Development and Implementation of Cybersecurity Documentation

The survey revealed a concerning lack of documented cybersecurity plans, with nearly half of respondents reporting the absence of written protocols for cybersecurity planning or incident response. This deficiency leaves organizations ill-prepared to manage and recover from attacks. Policymakers should develop model frameworks or templates for cybersecurity plans that organizations can adapt to meet their specific needs. These templates should include detailed incident response protocols, tools for risk assessment, and reporting requirements. Policymakers should also consider mandating basic cybersecurity documentation for certain sectors, particularly those that handle sensitive personal or financial data. Compliance could be incentivized through grants or recognition programs, such as cybersecurity certifications for compliant organizations.

F. Strengthen Information Sharing and Threat Intelligence Networks

Effective cybersecurity demands collaboration. The survey indicated low participation in information-sharing networks, such as Information Sharing and Analysis Centers (ISACs). Policymakers should focus on increasing awareness and accessibility of these networks, particularly for small and local organizations. Creating regional or sector-specific ISACs could make these resources more relevant and attractive to organizations that currently do not participate. Additionally, state and local governments should facilitate regular cybersecurity briefings, workshops, and simulations to share best practices and prepare organizations for potential attack scenarios. Encouraging real-time reporting of incidents and threats would enhance the collective defense of businesses and institutions across the state.

G. Support Statewide Cybersecurity Workforce Development

The lack of dedicated cybersecurity professionals within many organizations is a critical barrier to improving security practices. Policymakers should prioritize initiatives to expand the cybersecurity workforce, such as scholarship programs for students pursuing cybersecurity degrees and apprenticeships offering hands-on training. Partnerships between industry and educational institutions can ensure that training programs align with the needs of employers, producing graduates equipped to address modern cybersecurity challenges. Expanding opportunities for reskilling and upskilling current employees is equally important. For example, targeted programs could help IT professionals transition into cybersecurity roles, addressing critical talent shortages.

H. Defining *"Reasonable"* Cybersecurity

As this survey underscores, many organizations are rightly confused about what 'reasonable' cybersecurity entails. To date, that varies across the more than one dozen states with such laws on the books. Under Californian law, for example, organizations are required to implement "reasonable security procedures and practices . . . to protect personal information from unauthorized, access, destruction, use, modification, or disclosure."[37] The California Attorney General's Office defined "reasonable" to include the following list of Center for Internet and Security controls as the minimum threshold, which include requiring multi-factor authentication, and end-to-end encryption on portable devices.

IU's Center for Applied Cybersecurity Research, in collaboration with Purdue cyberTAP and the Indiana Office of Technology, rolled out the CyberTrack program that has begun to answer this question at least for local governments and critical infrastructure providers. This research resulted in an evidence-based, prioritized list of the CIS Safeguards, with 12 safeguards making up the top-scoring group that are now the major focus of the tactical-level standard for the Cybertrack assessment. We validated this ranking and highest-scoring "Transformative Twelve" safeguards via independent Indiana University and Purdue University subject matter expert analysis, confirmed the very high presence of these safeguards in other standards (for example, NIST's).[38]

2.3	Address Unauthorized Software
3.3	Configure Data Access Control lists
3.4	Enforce Data Retention
4.1	Establish and Maintain a Secure Configuration Process
4.7	Manage Default Accounts on Enterprise Assets and Software
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
6.3	Require MFA for Externally-Exposed Applications
6.4	Require MFA for Remote Network Access
6.5	Require MFA for Administrative Access
10.1	Deploy and Maintain Anti-Malware Software
10.2	Configure Automatic Anti-Malware Signature Updates
11.4	Establish and Maintain an Isolated Instance of Recovery Data

**The numbering system corresponds to specific Safeguards from the CIS Controls v8.0*

Figure 12: The Transformative Twelve

This is not to say that these are the only controls worth implementing. Moreover, much-needed future research may result in a somewhat different top-scoring group. However, in the context of a cybersecurity landscape where some "standards" include hundreds of controls, and most lack prioritization or evidentiary grounding, we see building real confidence in any subset as a victory for practicality. The Indiana state government can be a helpful ally in helping small businesses and local governments navigate this complexity.

I. Cyber Risk Insurance

As is evident from this survey, there remains significant barriers for Indiana organizations accessing this tool, including cost, awareness, and confusion over coverage for both first and third-party losses. Given that only a minority of the survey respondents likewise were aware of exclusions in their policies, it seems clear that the State has a role to play in helping Indiana organizations navigate what types of cyber risks insurance can, and cannot, help mitigate. One tool to help in this regard, which could be folded into Indiana's Cybersecurity Hub offerings, could take the form of a guide modeled after Citizen Lab's Security Planner but focused not just on cybersecurity best practices, but also on the navigating cyber risk insurance questions across markets, and sectors. We plan follow-up surveys to periodically assess how Indiana is improving along these metrics, and hope that these results help convince other states to follow Indiana's example in this regard.

Conclusion

Indiana organizations face an expanding array of cyber threats. Although progress has been made, significant challenges remain. Policymakers must take a leading role in empowering organizations to strengthen their cybersecurity posture. By addressing resource limitations, broadening access to education and training, enhancing the availability of cyber insurance, and fostering collaboration through information sharing and workforce development, Indiana can cultivate a more secure and resilient digital environment. Implementing these strategies will not only protect individual organizations but also reinforce the economic and social stability of the state.

Appendix A: Indiana Cybersecurity Survey Protocol

Appendix A: Survey Protocol

Hoosier Cybersecurity 2024

Start of Block: Consent

Q62 University of Arizona Consent to Participate in Research Study Title: *Examining Cybersecurity Practices Amongst Indiana Organizations: 2022 Update* Principal Investigator: Anne Boustead.

You are being asked to participate in a research study. Your participation in this research study is voluntary and you do not have to participate. This document contains important information about this study and what to expect if you decide to participate. Please consider the information carefully. Feel free to ask questions before making your decision whether to participate. The goal of this study is to elicit information about the cybersecurity risk perceptions, cybersecurity risk management and planning, and cybersecurity insurance use practices of public and private organizations in Indiana. To participate in this study, you will be asked to complete a survey describing your organization's cybersecurity practices, how your organization decided to engage in those practices, and your role in your organization's cybersecurity. We anticipate that this survey will take 25-35 minutes to complete. If you choose to participate in this survey, you could face risks from your employer if they find out you have shared information they do not want shared. To minimize these risks, we will not share information that could identify you publicly, and will not publish information about the data that could lead someone to be able to identify you. You will not benefit directly from participating in this study, and you will not be paid for the time you spend participating in this study. The information that you give in the survey will be anonymous, and we will not collect identifiable information from you about either you or your organization during the course of the survey. Any information we do collect will be stored on an encrypted hard drive or in a secure cloud storage location, and password protected. Your name or your organization's name will not be collected or linked to your answers, and will not be used in any reports. The data you provide will be shared with external research team members. In addition, data you provide may be used in future research. The information that you provide in the study will be handled confidentially. However, there may be circumstances where this information must be released or

shared as required by law. The University of Arizona Institutional Review Board may review the research records for monitoring purposes. For questions, concerns, or complaints about the study you may contact Anne Boustead, at boustead@arizona.edu. For questions about your rights as a participant in this study or to discuss other study-related concerns or complaints with someone who is not part of the research team, you may contact the Human Subjects Protection Program Director at 520-626-8630 or online at https://research.arizona.edu/compliance/human-subjects-protection-program. By selecting "Yes, I agree to participate" and advancing to the next page, you are allowing your responses to be used for research purposes.

Q1 Do you consent to participate in this study?

- ○ Yes, I agree (1)
- ○ No, I do not agree (2)

Skip To: End of Survey If Do you consent to participate in this study? = No, I do not agree

End of Block: Consent

Start of Block: Section 1: Cyber Risk Perceptions

QID2 How concerned is your organization about the risk of a cybersecurity incident?

- ○ Not at all concerned (1)
- ○ Somewhat concerned (2)
- ○ Very concerned (3)

QID3 Is your organization more or less concerned about the risk of a cybersecurity incident than they were during spring of 2021?

- ○ Much less concerned (1)
- ○ Less concerned (2)
- ○ About the same level of concern (3)
- ○ More concerned (4)
- ○ Much more concerned (5)
- ○ Don't know / Can't say (6)

QID5 Which of the following types of cybersecurity incidents is your organization concerned about? (select all that apply)

- ☐ Ransomware (e.g., extortion) (1)
- ☐ Phishing (e.g., targeting key personnel through cyber-enabled means) (2)
- ☐ Insider attack (e.g., employee selling access or secrets) (3)
- ☐ Malware (e.g., malicious software) (4)
- ☐ Password attacks (e.g., someone else breaking your passwords) (5)
- ☐ Denial of service attacks (e.g., someone making it impossible for users to access your website) (6)
- ☐ Other (please describe) (7) _____

Display This Question:

If If Which of the following types of cybersecurity incidents is your organization concerned about? (select all that apply) q://QID5/SelectedChoicesCount Is Greater Than 1

Carry Forward Selected Choices from "Which of the following types of cybersecurity incidents is your organization concerned about? (select all that apply) "

QID6 Please rank the types of cybersecurity incidents you identified from most concerning to least concerning.

- _____ Ransomware (e.g., extortion) (1)
- _____ Phishing (e.g., targeting key personnel through cyber-enabled means) (2)
- _____ Insider attack (e.g., employee selling access or secrets) (3)
- _____ Malware (e.g., malicious software) (4)
- _____ Password attacks (e.g., someone else breaking your passwords) (5)
- _____ Denial of service attacks (e.g., someone making it impossible for users to access your website) (6)
- _____ Other (please describe) (7)

Display This Question:

If If Which of the following types of cybersecurity incidents is your organization concerned about? (select all that apply) q://QID5/SelectedChoicesCount Is Greater Than 1

QID7 Is your organization more or less concerned about these types of cybersecurity incidents than they were in spring 2021?

	Much less concerned			About as concerned			Much more concerned			
	0	10	20	30	40	50	60	70	80	90	100
Ransomware ()											
Phishing ()											
Insider attack ()											
Malware ()											
Password attacks ()											
Denial of service attacks ()											

QID8 What potential consequences of cybersecurity incidents is your organization concerned about?

- ☐ Data or information being exposed to outsiders (1)
- ☐ Data or information being deleted or lost (2)
- ☐ Disinformation about your organization being spread (3)
- ☐ Identity theft (4)
- ☐ Fraud (5)
- ☐ Website or system downtime (6)
- ☐ Other (please describe) (7) _____

Display This Question:

If If What potential consequences of cybersecurity incidents is your organization concerned about? q://QID8/SelectedChoicesCount Is Greater Than 1

Carry Forward Selected Choices from "What potential consequences of cybersecurity incidents is your organization concerned about? "

Q64 Please rank the potential consequences of cybersecurity incidents you identified from most concerning to least concerning

- _____ Data or information being exposed to outsiders (1)
- _____ Data or information being deleted or lost (2)
- _____ Disinformation about your organization being spread (3)
- _____ Identity theft (4)
- _____ Fraud (5)
- _____ Website or system downtime (6)
- _____ Other (please describe) (7)

QID9 Is your organization more or less concerned about these potential consequences of cybersecurity incidents than they were in spring 2021?

	Much less concerned — About as concerned — Much more concerned 0 10 20 30 40 50 60 70 80 90 100
Data or information being exposed to outsiders ()	
Data or information being deleted or lost ()	
Disinformation about your organization being spread ()	
Identity theft ()	
Fraud ()	
Website or system downtime ()	

End of Block: Section 1: Cyber Risk Perceptions

Start of Block: Section 2: Cyber Risk Management and Planning

QID10 To your knowledge, has your organization experienced a successful cyber attack since spring 2021?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure or can't say (3)

Skip To: QID15 If To your knowledge, has your organization experienced a successful cyber attack since spring 2021? != Yes

QID11 How many cyber attacks resulting in data theft did your organization experience since spring 2021?

- ○ None (1)
- ○ 1-5 (2)
- ○ 6-10 (3)
- ○ 11-50 (4)
- ○ 50-100 (5)
- ○ 100+ (6)
- ○ I'm not sure (7)

Page Break

QID12 Please think back to the most severe cyber attack resulting in data theft experienced by your organization since spring 2021. When did the cyber attack occur?

	Month	Year
Please select: (1)	▼ January (1 ... December (12)	▼ 2021 (1 ... 2023 (3)

QID13 Thinking about the most severe cyber attack experienced by your organization since spring 2021, What type of cyber attack did your organization experience?

- ☐ Ransomware (1)
- ☐ Phishing (2)
- ☐ Insider attack (3)
- ☐ Malware (4)
- ☐ Password attacks (5)
- ☐ Denial of service attacks (6)
- ☐ Other (please describe) (7) _____
- ☐ Not sure (8)

QID14 What were the consequences of the cyber attack experienced by your organization?

- [ ] No consequences occurred (1)
- [ ] Data or information being exposed to outsiders (2)
- [ ] Data or information being deleted or lost (3)
- [ ] Disinformation about your organization being spread (4)
- [ ] Identity theft (5)
- [ ] Fraud (6)
- [ ] Payment for credit monitoring services (7)
- [ ] Website or system downtime (8)
- [ ] Disruption of operations (9)
- [ ] Other (please describe) (10) _____
- [ ] Not sure (11)

QID15 Which of the following practices does your organization currently employ? (Select all that apply)

- ☐ Multi-factor authentication (1)
- ☐ End-to-end encryption (2)
- ☐ Remote backups (3)
- ☐ Automatic updating of operating systems and software (4)
- ☐ Traffic flow analysis (5)
- ☐ Third-party penetration testing (6)
- ☐ Policy on Bring Your Own Device (BYOD) (7)
- ☐ Antivirus software (8)
- ☐ Training employees to spot potential cybersecurity risks (9)
- ☐ Invested in cyber risk insurance (10)
- ☐ Limiting physical access to computer systems (11)
- ☐ Updating and patching software regularly (12)
- ☐ Requiring employees to regularly change passwords (13)
- ☐ Other (please describe) (14)

_____

- ☐ None of the above (15)

Carry Forward Selected Choices from "Which of the following practices does your organization currently employ? (Select all that apply)"

QID16 Did your organization adopt any of the following practices since spring 2021?

- [ ] Multi-factor authentication (1)
- [ ] End-to-end encryption (2)
- [ ] Remote backups (3)
- [ ] Automatic updating of operating systems and software (4)
- [ ] Traffic flow analysis (5)
- [ ] Third-party penetration testing (6)
- [ ] Policy on Bring Your Own Device (BYOD) (7)
- [ ] Antivirus software (8)
- [ ] Training employees to spot potential cybersecurity risks (9)
- [ ] Invested in cyber risk insurance (10)
- [ ] Limiting physical access to computer systems (11)
- [ ] Updating and patching software regularly (12)
- [ ] Requiring employees to regularly change passwords (13)
- [ ] Other (please describe) (14) _____
- [ ] None of the above (15)

QID18 Does your organization use any of the following tools to more proactively manage the cyber threats facing your organization? (Select all that apply)

- ☐ Joined an information sharing group such as an ISAC (1)
- ☐ Consulted news reports (2)
- ☐ Relied on government data such as from IN-ISAC or US CERT (3)
- ☐ Contacted the FBI/Secret Service for a briefing (4)
- ☐ Revised and updated the organization's incident response plan (5)
- ☐ Launched a cyber hygiene campaign (6)
- ☐ Revised organizational governance to ensure that cyber threat information was getting where it was needed. (7)
- ☐ Other (Please describe) (8) _____
- ☐ Not sure (9)

QID19 Did your organization refer to any externally developed cybersecurity frameworks or controls in making decisions about cybersecurity practices?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: QID21 If Did your organization refer to any externally developed cybersecurity frameworks or controls in m... != Yes

QID20 If so, which? (Select any that apply)

- ☐ Australia Top 35 Controls (1)
- ☐ Center for Internet Security (CIS) Top 20 Controls (2)
- ☐ Cybersecurity Maturity Model Certification (CMMC) 2.0 (3)
- ☐ Information Sharing Architecture (ISA) (4)
- ☐ Information Assurance for Small and Medium Enterprises (IASME) (5)
- ☐ National Institute for Standards and Technology (NIST) Cybersecurity Framework (6)
- ☐ NISTIR 7621 Measure (7)
- ☐ NIST SP 800-53 R4 Controls (8)
- ☐ International Standards Organization (ISO) 15408 (9)
- ☐ ISO 27001-02 (10)
- ☐ European Telecommunications Standards Institute (ETSI) (11)
- ☐ Other (please specify) (12) _____
- ☐ Not sure (13)

QID21 Has your organization provided to anyone (that you know of) any training intended to raise awareness of the potential for cybersecurity threats like hacking, phishing, spamming, or other threat related to stealing or compromising digital data?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: QID25 If Has your organization provided to anyone (that you know of) any training intended to raise awaren... != Yes

QID22 Did you receive training in a formal setting offered by your organization?

- ○ Yes (1)
- ○ No (2)

Skip To: QID24 If Did you receive training in a formal setting offered by your organization? = No

QID23 How often have you attended trainings designed to improve your awareness of cybersecurity threats?

- ○ Once a quarter (1)
- ○ Once a year (2)
- ○ Every few years (3)
- ○ I have attended only 1 training (4)

QID24 Have others in your organization received training in a formal setting offered by your organization?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

QID25 Who in your organization is ultimately responsible for managing cyber risks?

- ○ CEO (1)
- ○ Board of Directors Committee (2)
- ○ Chief Information Security Officer (CISO) (3)
- ○ Chief Information Officer (CIO) (4)
- ○ Chief Privacy Officer (CPO) (5)
- ○ Chief Information Governance Officer (CIGO) (6)
- ○ Data Protection Officer (DPO) (7)
- ○ Other (please specify) (8) _____
- ○ Not sure (9)

QID26 How many cybersecurity professionals are currently employed at your organization?

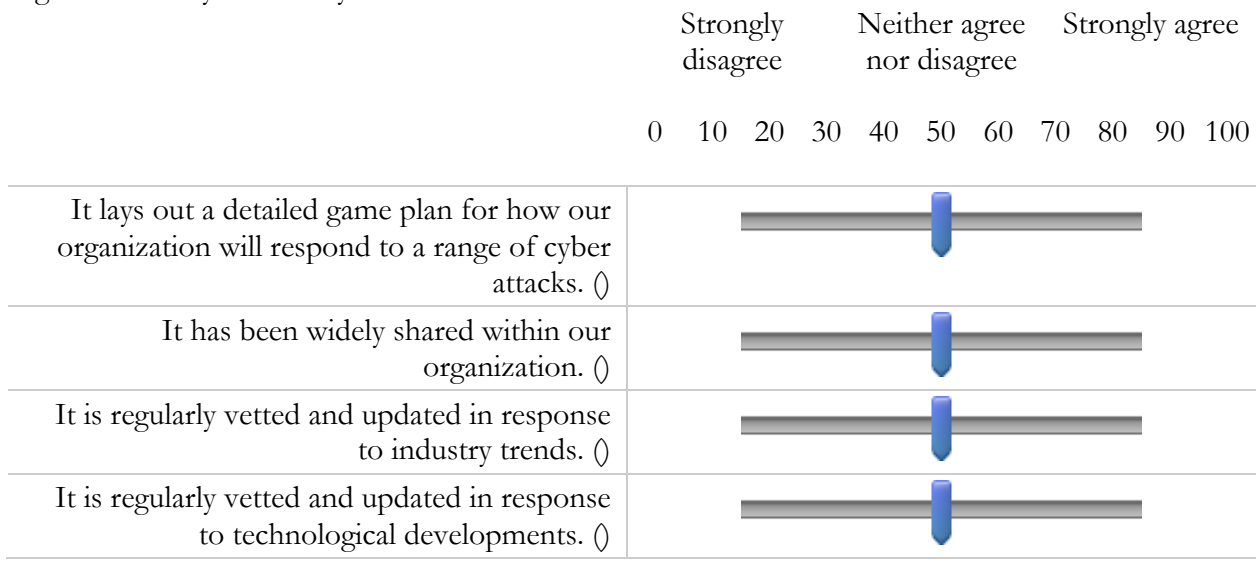
- ○ None (1)
- ○ 1-5 (2)
- ○ 6-10 (3)
- ○ 11+ (4)
- ○ Not sure (5)

QID27 Does your organization have written documentation related to cybersecurity planning and response?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: End of Block If Does your organization have written documentation related to cybersecurity planning and response? != Yes

QID28 How strongly would you agree or disagree with the following statements about your organization's cybersecurity documentation?



End of Block: Section 2: Cyber Risk Management and Planning

Start of Block: Section 3: Cybersecurity Insurance Use Questions - Sep 5, 2022

QID29 Does your organization currently have insurance specifically tailored to cover cyber incidents?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: QID41 If Does your organization currently have insurance specifically tailored to cover cyber incidents? != Yes

QID30 How long has your organization had a cyber risk insurance policy?

- ○ Years (1) _____
- ○ Months (2) _____

QID31 Why did your organization get a cyber risk insurance policy?

- ☐ Response to an incidence at our organization (1)
- ☐ Response to an incidence at a peer organization (2)
- ☐ News reports about cyber incidents (3)
- ☐ Other (please specify) (4) _____
- ☐ Not sure (5)

QID32 Which (if any) losses to your organization (first-party losses) are covered under this policy?

- [ ] Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems) (1)
- [ ] Cost of notifying affected customers or others whose data exposed in a breach (2)
- [ ] Credit monitoring services (3)
- [ ] Fines/penalties related to the data breach (4)
- [ ] Business interruptions related to denial of service or other downtime (5)
- [ ] Losses resulting from exposure or use of confidential business information (6)
- [ ] Damage to computer or information systems (including cost of restoring lost data) (7)
- [ ] Damages related to lost intellectual property (8)
- [ ] Forensic investigation of the breach (9)
- [ ] Standing up a call center and response team (10)
- [ ] Other (please list) (11) _____
- [ ] None of the above (12)

Display This Question:

If If Which (if any) losses to your organization (first-party losses) are covered under this policy? q://QID32/SelectedChoicesCount Is Greater Than 1

Carry Forward Selected Choices from "Which (if any) losses to your organization (first-party losses) are covered under this policy? "

QID33 Please rank how important it is for your organization to have coverage for the first-party losses you selected, from most important to least important.

- _____ Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems) (1)
- _____ Cost of notifying affected customers or others whose data exposed in a breach (2)
- _____ Credit monitoring services (3)
- _____ Fines/penalties related to the data breach (4)
- _____ Business interruptions related to denial of service or other downtime (5)
- _____ Losses resulting from exposure or use of confidential business information (6)
- _____ Damage to computer or information systems (including cost of restoring lost data) (7)
- _____ Damages related to lost intellectual property (8)
- _____ Forensic investigation of the breach (9)
- _____ Standing up a call center and response team (10)
- _____ Other (please list) (11)
- _____ None of the above (12)

QID34 Which (if any) losses to others (third-party losses) are covered under this policy?

☐ Claims from damages from customers or others whose information was exposed in the breach (1)

☐ Costs for legal defenses related to the data breach (2)

☐ Fines and penalties (3)

☐ Other (please list) (4)

_____

☐ None of the above (5)

Display This Question:

If If Which (if any) losses to others (third-party losses) are covered under this policy? q://QID34/SelectedChoicesCount Is Greater Than 1

Carry Forward Selected Choices from "Which (if any) losses to others (third-party losses) are covered under this policy? "

QID35 Please rank how important it is for your organization to have coverage for the third-party losses you selected, from most important to least important.

- _____ Claims from damages from customers or others whose information was exposed in the breach (1)
- _____ Costs for legal defenses related to the data breach (2)
- _____ Fines and penalties (3)
- _____ Other (please list) (4)
- _____ None of the above (5)

QID36 Does your cyber risk insurance policy require your organization to undertake certain security measures?

- Yes (1)
- No (2)
- Not sure (3)

Skip To: QID38 If Does your cyber risk insurance policy require your organization to undertake certain security mea... != Yes

QID37 What security measures are required by your cyber risk insurance policy?

- [ ] Mandatory, automatic patching (1)
- [ ] End-to-end data encryption (2)
- [ ] Employee training & cyber hygiene (3)
- [ ] Regular third party penetration testing (4)
- [ ] Other (please list) (5) _____
- [ ] None of the above (6)

QID38 Has the price of your cyber risk insurance changed since spring 2021?

- ○ No (1)
- ○ Yes, it has decreased (2)
- ○ Yes, it has increased (3)
- ○ Not sure (4)

QID39 Does your cyber risk insurance policy exclude coverage in certain circumstances?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: End of Block If Does your cyber risk insurance policy exclude coverage in certain circumstances? != Yes

QID40 Under what circumstances would your cyber risk insurance policy exclude coverage? (Select all that apply)

- ☐ Act of war/terrorism (1)
- ☐ Internet of Things-related breach (2)
- ☐ Losses from unencrypted devices (3)
- ☐ Contractual liability (4)
- ☐ Criminal or fraudulent acts (5)
- ☐ Losses related to unauthorized collection of customer data (6)
- ☐ Losses that occurred because your organization failed to provide and maintain adequate security (7)
- ☐ Other (please list) (8) _____
- ☐ None of the above (9)

Skip To: End of Block If Condition: Selected Count Is Greater Than or Equal to 1. Skip To: End of Block.

QID41 Has your company ever had a cyber risk insurance policy?

- ○ Yes (1)
- ○ No (2)

Skip To: QID46 If Has your company ever had a cyber risk insurance policy? = No

QID42 During what period did your company have a cyber risk insurance policy?

- From (1) _____
- To (2) _____

QID43 Which (if any) losses to your organization (first-party losses) were covered under this policy? (Select all that apply)

- [ ] Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems) (1)
- [ ] Cost of notifying affected customers or others whose data exposed in a breach (2)
- [ ] Credit monitoring services (3)
- [ ] Fines/penalties related to the data breach (4)
- [ ] Business interruptions related to denial of service or other downtime (5)
- [ ] Losses resulting from exposure or use of confidential business information (6)
- [ ] Damage to computer or information systems (including cost of restoring lost data) (7)
- [ ] Damages related to lost intellectual property (8)
- [ ] Forensic investigation of the breach (9)
- [ ] Standing up a call center and response team (10)
- [ ] Other (please list) (11) _____
- [ ] None of the above (12)

QID44 Which (if any) losses to others (third-party losses) were covered under this policy? (Select all that apply)

- [ ] Claims from damages from customers or others whose information was exposed in the breach (1)
- [ ] Costs for legal defenses related to the data breach (2)
- [ ] Fines and penalties (3)
- [ ] Other (please list) (4) _____
- [ ] None of the above (5)

QID45 Why did you discontinue your former cyber risk insurance policy? (Select all that apply)

- ☐ Too expensive (1)
- ☐ Couldn't get policy (2)
- ☐ Covered under other insurance policies (3)
- ☐ Prefer to spend resources on other priorities (4)
- ☐ Options for preventing cybersecurity incidents are ineffective (5)
- ☐ Don't believe our organization is at risk (6)
- ☐ Other (please list) (7) _____
- ☐ Not sure / Can't say (8)

Skip To: QID48 If Condition: Selected Count Is Greater Than or Equal to 1. Skip To: What would encourage your company to ....

QID46 Has your company ever considered obtaining a cyber risk insurance policy?

- ○ Yes (1)
- ○ No (2)
- ○ Not sure (3)

Skip To: QID48 If Has your company ever considered obtaining a cyber risk insurance policy? != Yes

QID47 Why did your company decide not to obtain a cyber risk insurance policy? (Select all that apply)

- ○ Too expensive (1)
- ○ Difficult to obtain (2)
- ○ Covered under other insurance policies (3)
- ○ Prefer to spend resources on other priorities (4)
- ○ Options for preventing cybersecurity incidents are ineffective (5)
- ○ Don't believe our organization is at risk (6)
- ○ Other (Please list) (7) _____
- ○ Not sure / Can't say (8)

QID48 What would encourage your company to obtain a cyber risk insurance policy?

_____

_____

_____

_____

_____

End of Block: Section 3: Cybersecurity Insurance Use Questions - Sep 5, 2022

Start of Block: Block 4: Experimental Section

Display This Question:

If Random = 1

Q65
You have a leadership position with a company that develops consumer technologies, and is based out of a midwest state in the United States. This company employs 50 people and has an annual revenue of $50 M. As part of this position, you are responsible for making financial strategy decisions for your company.

An expert speaking at an industry event recently revealed that companies in your industry are currently facing significant financial risks due to increased economic uncertainty from events over the past 2 years. The expert noted that these events cost organizations in your industry $6,000,000 per incident on average, and 1 in 10 organizations will face such an existential threat.

Display This Question:

If Random = 2

Q66
You have a leadership position with a company that develops consumer technologies, and is based out of a midwest state in the United States. This company employs 50 people and has an annual revenue of $50 M. As part of this position, you are responsible for making financial strategy decisions for your company.

An expert speaking at an industry event recently revealed that malicious cybersecurity events cost organizations in your industry $6,000,000 per incident on average, and 1 in 10 organizations will face a malicious cyber incident.

Display This Question:

If Random = 3

Q67
You have a leadership position with a company that develops consumer technologies, and is based out of a midwest state in the United States. This company employs 50 people and has an annual revenue of $50 M. As part of this position, you are responsible for making financial strategy decisions for your company.

An expert speaking at an industry event recently revealed that the average organization in your industry spends 10% of their IT budget on cybersecurity, with an average yearly cost of $600,000.

Q68 Your company is currently revising their priorities for spending on services that reduce risk. Select the three highest priority areas for your company to spend money to reduce risk or mitigate potential adverse effects.

- [ ] Cybersecurity (1)
- [ ] Natural Disasters (2)
- [ ] Lawsuits (3)
- [ ] Executive/Board Continuity (4)
- [ ] Political Instability (5)
- [ ] Public Health Emergencies (6)

Q69 Your advisors inform you that your organization has not adopted the following specific cybersecurity practices. Select the three highest priority practices for your company to adopt.

- [ ] Mandate multi-factor authentication (1)
- [ ] Mandate end-to-end encryption (2)
- [ ] Create an automated system for updating operating systems and software (3)
- [ ] Adopt an external cybersecurity decision-making framework (e.g., MITRE's ATT&CK framework) to manage supply chain risk (4)
- [ ] Re-evaluate and/or implement annual cybersecurity training with penalties for employees who systematically violate protocols (5)
- [ ] Institute regular checks with vendors or partners. (6)

Carry Forward Selected Choices from "Your advisors inform you that your organization has not adopted the following specific cybersecurity practices. Select the three highest priority practices for your company to adopt."

Q70 As a percentage of your organization's yearly revenue, how much do you think your organization would be willing to pay in order to adopt each practice?

- Mandate multi-factor authentication (1) _____
- Mandate end-to-end encryption (2) _____
- Create an automated system for updating operating systems and software (3) _____
- Adopt an external cybersecurity decision-making framework (e.g., MITRE's ATT&CK framework) to manage supply chain risk (4) _____
- Re-evaluate and/or implement annual cybersecurity training with penalties for employees who systematically violate protocols (5) _____
- Institute regular checks with vendors or partners. (6) _____

End of Block: Block 4: Experimental Section

Start of Block: Block 5: Organization and Respondent Questions

Q50 What is your job title?

_____

Q51 Which best describes your occupation?

- ○ General organization leadership (e.g., CEO/CFO) (1)
- ○ Technology organization leadership (e.g., CIO, CISO) (2)
- ○ IT Management (3)
- ○ Security Management (4)
- ○ Operations Management (5)
- ○ Other [Please specify] (6) _____

Q52 What is your age range?

- ○ 18-24 (4)
- ○ 25-34 (5)
- ○ 35-44 (6)
- ○ 45-54 (7)
- ○ 55-64 (8)
- ○ 65 or older (9)

Q53 What is your gender?

- ○ Male (1)
- ○ Female (2)
- ○ Non-binary / third gender (3)
- ○ Prefer not to say (4)

Q54 What is your organization's annual operating budget?

_____

Q55 How many employees does your organization have?

- 1-10 employees (1)
- 10-50 employees (2)
- 50-250 employees (3)
- More than 250 employees (4)

Q56 What sector is your organization in?

- ○ Accommodation and Food Services (1)
- ○ Administration and Support Services (2)
- ○ Agriculture, Forestry, Fishing, and Hunting (3)
- ○ Arts, Entertainment, and Recreation (4)
- ○ Construction (5)
- ○ Educational Services (6)
- ○ Finances and Insurance (7)
- ○ Government (8)
- ○ Health Care and Social Assistance (9)
- ○ Manufacturing (10)
- ○ Other Services (11)
- ○ Professional, Scientific, and Technical Services (12)
- ○ Real Estate and Rental and Leasing (13)
- ○ Retail Trade (14)
- ○ Transportation and Warehousing (15)
- ○ Utilities (16)
- ○ Wholesale Trade (17)
- ○ Other (Please specify) (18) _____

Q57
Which of the following types of information does your organization handle? (Select all that apply)

- ☐ Personally identifiable information (e.g., home addresses, email addresses, social security numbers) (1)
- ☐ Personal financial information (e.g., credit card numbers, banking information, credit scores) (2)
- ☐ Personal health information (e.g., allergies, blood pressure, past medications) (3)
- ☐ Other (Please describe) (4) _____
- ☐ We do not collect any personal data (5)
- ☐ Not sure (6)

Q58
How would you describe the geographic scope of your organization?

- ○ Local (e.g., city or county) (1)
- ○ State (2)
- ○ Regional (e.g., more than one state) (3)
- ○ National (4)
- ○ Multi-national (5)
- ○ Does not apply (6)

End of Block: Block 5: Organization and Respondent Questions

Apendix B: Notes

[1] *See* Darlene Storm, *New Attacks Secretly Use Smartphone Cameras, Speakers, and Microphones*, COMPUTER WORLD (Aug. 20, 2014), https://www.computerworld.com/article/2598704/new-attacks-secretly-use-smartphone-cameras--speakers-and-microphones.html.

[2] *See* Sarah Murray, *When Fridges Attack*: Why Hackers Could Target the Grid, FIN. TIMES (Oct. 17, 2018), https://www.ft.com/content/2c17ff5e-4f02-11e8-ac41-759eee1efb74.

[3] *See* Zak Doffmann, *Russia and China 'Hijack' Your Internet Traffic: Here's What You Do*, FORBES (Apr. 18, 2020), https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/#2b936c395b16.

[4] *See* Nate Berg, *Starbudks, PepsiCo, and BMW Partner to Fix a Global Problem Worth Trillions*, FAST COMPANY (Aug. 6, 2020), https://www.fastcompany.com/90536448/starbucks-pepsico-and-bmw-partner-to-fix-a-global-problem-worth-trillions; Caroline Dowling, *How Vulnerable is Your Supply Chain?*, INDUSTRY WK. (Dec. 6, 2012), https://www.industryweek.com/supply-chain/customer-relationships/article/21959294/how-vulnerable-is-your-supply-chain.

[5] *See Hackers Attack Every 39 Seconds*, SEC. MAG. (Feb. 10, 2017), https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

[6] *See Press Release: New Study Reveals Impact of Cyberattacks on Consumer Confidence, Corporate Reputation*, DHM RES. (Oct. 3, 2019), https://www.dhmresearch.com/press-release-new-study-reveals-impact-of-cyberattacks-on-consumer-confidence-corporate-reputation/.

[7] Survey: *Cybercrime More Devastating to SMBs than Other Threats Combined*, GLOBE NEWS WIRE (Feb. 26, 2019), https://www.globenewswire.com/news-release/2019/02/26/1742542/0/en/Survey-Cybercrime-More-Devastating-to-SMBs-than-Other-Threats-Combined.html.

[8] *White Hat, Black Hat and the Emergence of the Gray Hat: The True Costs of Cybercrime* (Osterman Res. White Paper, Aug. 8, 2018), http://resources.malwarebytes.com/files/2018/08/GLOBAL-White-Hat-Black-Hat-and-the-Emergence-of-the-Gray-Hat-The-True-Costs-of-Cybercrime_Sponsored-by-Malwarebytes.pdf.

[9] *See Congress Moving Closer Toward Cybersecurity Aid to State and Local Governments*, ST. SCOOP (Sept. 23, 2019), https://statescoop.com/congress-moving-closer-toward-cybersecurity-aid-to-state-and-local-governments/.

[10] *Id.*

[11] *Cybersecurity Spending Set to Soar: Over $200 Billion Projection for 2024*, CYBER EXPRESS (Mar. 2024), https://thecyberexpress.com/cybersecurity-spending-trends-2024/.

[12] For more information on this topic, see *Defining 'Reasonable' Cybersecurity: Lessons from the States,* 25 YALE JOURNAL OF LAW AND TECHNOLOGY 86 (2023) (with Anne Boustead & Christos Madrikis).

[13] Scott J. Shackelford, *The Three 'B's' of Cybersecurity for Small Businesses*, CONVERSATION (Apr. 17, 2017), https://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259.

[14] *See Understanding and Dealing with Phishing During the Covid-19 Pandemic*, ENISA (May 6, 2020), https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic.

[15] *See* Steve Grobman, *Adjusting to the New Security Realities of a Remote Workforce*, CYBER SCOOP (May 27, 2020), https://www.cyberscoop.com/steve-grobman-new-cybersecurity-realities-remote-workforce/.

[16] *See* Duncan Geere, *How Deep Packet Inspection Works*, WIRED (Apr. 27, 2012), https://www.wired.co.uk/article/how-deep-packet-inspection-works. SaaS-based web gateway architecture has also been a proposed solution that can provide essential security controls to safeguard users visiting websites. In addition to protecting businesses from incoming threats and outgoing information exfiltration, it also allows organizations to apply similar corporate internet access policies to the increasing number of remote workers due to the COVID-19 pandemic.

[17] *See* Bruce Berman, *$21 Trillion in U.S. Intangible Assets is 84% of S&P 500 Value*, IP CLOSE UP (June 4, 2019), https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/.

[18] *See* John Gaudiosi, *Why Sony Didn't Learn From its 2011 Hack*, FORTUNE (Dec. 24, 2014), https://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[19] *91% of Cyber Attacks Start with a Phishing Email: Here's How to Protect Against Phishing*, DIGITAL GUARDIAN (July 26, 2017), https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing.
[20] *See The 2020 State of IT*, Spiceworks, https://www.spiceworks.com/marketing/state-of-it/report/ (last visited Aug. 10, 2020).
[21] *See The Dearth of Skilled. Cybersecurity Personnel*, SC MAG. (Jan. 23, 2020), https://www.scmagazine.com/home/advertise/the-dearth-of-skilled-cybersecurity-personnel/. In the absence of trained personnel, network security operations can turn to policy-based automation to reduce incomprehensibility, improve visibility, and focus resources on more complex tasks to improve operational efficiencies that directly impact the upshot of the business.
[22] Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

[23] *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*, PWC (2020), https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.
[24] *See* Carolyn Cohn, *Europe's New Data Privacy Law Boosts Cyber Insurance Sales*, INSURANCE J. (May 22, 2018), https://www.insurancejournal.com/news/international/2018/05/22/489977.htm ("Insurers say the directive, together with major cyber attacks like last year's WannaCry and NotPetya viruses, is driving demand in Europe for cyber insurance – a sector seen as relatively profitable.").

[25] *See* Daniel R. Stoller, *Cyber Insurance Purchases Will Surge With California Privacy Law*, BLOOMBERG L. (Feb. 5, 2020), https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-law.

[26] *See* Vishaal Hariprasad, *Introducing 'Cyber Meteorology:' A New Strategy for Cyber Insurance*, DARK READING (Feb. 3, 2020), https://www.darkreading.com/risk/introducing-cyber-meteorology-a-new-strategy-for-cyber-insurance-/d/d-id/1336924.

[27] Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.

[28] *The 2020 State of IT*, *supra* note 20.
[29] *Id.*
[30] *See* Abhimanyu S. Ahuja, *The Impact of Artificial Intelligence in Medicine on the Future Role of the Physician*, PEERJ (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6779111/.
[31] *The Role of AI in Assessing Cyber Risks: A Modern Tale of Defense*, NTT DATA INSURANCE (2024), https://insurance.nttdata.com/post/the-role-of-ai-in-assessing-cyber-risks-a-modern-tale-of-defense/#:~:text=In%20conclusion%2C%20AI%20is%20not,businesses%20approach%20cyber%20risk%20management.
[32] *See Survey Results: The Economic Impact of Cyber Insurance*, COWBELL (June 2020), https://cowbell.insure/wp-content/uploads/2020/06/Cowbell-Cyber-data-report.pdf.
[33] *See, e.g.*, Benjamin W. Perry, *U.S. Continues Patchwork of Comprehensive Data Privacy Requirements: New Laws Set to Take Effect Over Next 2 Years*, NAT'L L. REV. (Aug. 6, 2024), https://natlawreview.com/article/us-continues-patchwork-comprehensive-data-privacy-requirements-new-laws-set-take.
[34] U.S. Gov't Accountability Off., Cybersecurity: An Overview of Cyber Challenges Facing the Nation, and Actions Needed to Address Them, https://www.gao.gov/cybersecurity (last visited Oct. 17, 2024).
[35] Shields Up: Guidance for Families, CISA, https://www.cisa.gov/shields-up/guidance-families (last visited Sept. 11, 2024).
[36] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., PLANNING CONSIDERATIONS FOR CYBER INCIDENTS: GUIDANCE FOR EMERGENCY MANAGERS (2023), https://www.cisa.gov/sites/default/files/2023-11/Planning_Considerations_for_Cyber_Incidents_508c.pdf
[37] Paul Otto & Brian Kennedy, "*Reasonable Security" Becomes Reasonably Clear to California Attorney General*, CHRONICLE OF DATA PROTECTION (Mar. 1, 2016), https://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear/.
[38] Scott J. Shackelford et al., *The Difficulties of Defining "Secure-by-Design*," LAWFARE (Feb. 6, 2024), https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design.