State of Hoosier Cybersecurity

2020

December 2020

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)

Special thanks to Jay Bhatia and Eric Spencer 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.

CYBERSECURITY PROGRAM

OSTROM WORKSHOP

IBRC

Table of Contents

EXECUTIVE SUMMARY **1**

Key Findings 2

UNDERSTANDING CYBER RISK **4**

A. Cyber Threat Dimensions 4

1. Technical *4*

2. Economic *5*

3. Legal *6*

B. Steps to Managing Cyber Risks 8

1. Be Aware *8*

2. Be Organized *9*

3. Be Proactive *9*

C. Current Trends in Addressing Cyber Risk 10

1. Cyber Risk Insurance *10*

2. Artificial Intelligence *11*

3. Cybersecurity During the Pandemic *12*

METHODS **13**

A. Aims of this Study 13

B. Survey Development and Distribution 13

C. Limitations 15

RESULTS **16**

A. Risk Perceptions & Experiences 16

1. Potential Events & Consequences *16*

2. Previous Events and Responses *19*

B. Managing Cyber Risk 21

1. Prevention and Mitigation of Cyber Incidents *21*

2. Cybersecurity Practices, Personnel, and Training *25*

3. Usefulness of Standards & Frameworks *27*

C. Role of Cyber Risk Insurance 28

1. Adoption of Cyber Insurance *28*

2. Cyber Insurance Coverage *30*

3. Required Security Measures *32*

4. Non-Adoption of Cyber Risk Insurance *33*

POLICY OPPORTUNITIES **35**

A. Awareness Training 35

B. Proactive Cybersecurity 35

C. Defining "Reasonable" Cybersecurity 36

D. Incident Response Best Practices 38

E. Cyber Risk Insurance 38

APPENDIX A: SOURCES USED FOR FIGURE 1 ..... **39**

APPENDIX B: INDIANA CYBERSECURITY SURVEY PROTOCOL ... 40

Index of Figures

Figure 1: State-Level Cybersecurity Laws (2020) ... 7

Figure 2: State Breach Notification Laws ... 8

Figure 3: Description of Respondent Organizations ... 14

Figure 4: Respondents by Critical Infrastructure Sector ... 15

Figure 5: Proportion of Respondents Concerned About Cyber Incidents, By Type ... 16

Figure 6: Proportion of Respondents Most Concerned About Each Type of Cyber Incident ... 17

Figure 7: Causes of Data Breaches Reported to the Indiana Attorney General ... 18

Figure 8: Proportion of Respondents Concerned About Consequences of Cyber Incidents, By Type ... 19

Figure 9: Proportion of Respondents Most Concerned About Consequence of Cyber Incident ... 19

Figure 10: Types of Cyber Incidents Experienced by Respondents' Organizations ... 20

Figure 11: Consequences of Cyber Incidents Experienced by Respondents' Organizations ... 21

Figure 12: Mechanisms Used to Prevent Cyber Incidents ... 22

Figure 13: Reasons for Not Adopting Prevention Mechanisms ... 23

Figure 14: Mechanisms Used to Mitigate Cyber Incidents ... 24

Figure 15: Reasons for Not Adopting Mitigation Mechanisms ... 25

Figure 16: Cybersecurity Practices Adopted ... 26

Figure 17: Perceptions of Cybersecurity Documentation ... 27

Figure 18: Tools Used to Proactively Manage Cyber Risk ... 28

Figure 19: Year Cyber Risk Insurance Was Obtained ... 29

Figure 20: Reasons for Obtaining Cyber Risk Insurance ... 30

Figure 21: First Party Losses Covered Under Cyber Insurance ... 31

Figure 22: Third Party Losses Covered Under Cyber Insurance ... 32

Figure 23: Security Measures Required by Respondents' Insurer ... 33

Contact Information

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

Executive Summary

As is the case in many jurisdictions, public and private organizations in Indiana are unfortunately no stranger to cyber attacks. Counties across the state such as Lake,[1] Lawrence,[2] and LaPorte[3] have been targeted by criminals in recent ransomware campaigns, leading to hundreds of thousands in losses. Healthcare providers such as Hancock Memorial Hospital have been similarly breached, as have universities, small business, utilities, and school corporations.[4] Yet it has proven difficult to understand the full scope of these cyber threats, and how Hoosier organizations are attempting to prevent and respond to them.

To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, conducted this study to help explore how Indiana organizations perceive and manage cyber risks. We pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy.

The report is broken down into the following sections. Section 1 offers background on the technical, organizational, and legal dimensions of the cyber threat, along with a policy review highlighting recent primarily state-level efforts in Indiana and beyond to better manage cyber risk. Section 2 reviews the methods used in this study. Section 3 summarizes our results, paying particular attention to such topics as risk perceptions, management, and the evolving role of cyber risk insurance. Section 4 concludes the study with a look at policy opportunities to address the vulnerabilities and governance gaps revealed by the survey.

This goal of this report is to provide business leaders, policymakers, law enforcement professionals, and all Hoosiers with important information about cyber readiness, help organizations of all sizes better understand current cyber threats facing Indiana, and describe current efforts to address them. In the end, cybersecurity is a team sport, and we're all in this together.

[1] *See* Anna Ortiz, *Lake County, Ind., Sheriff's Email Online After Cyberattack*, GOVTECH (Sept. 9, 2019), https://www.govtech.com/security/Lake-County-Ind-Sheriffs-Email-Online-After-Cyberattack.html.

[2] *See* Rich Van Wyk, *Cyberattack Knocks out Lawrence County Government Computers*, WTHR (Feb. 13, 2020), https://www.wthr.com/article/news/local/indiana/cyberattack-knocks-out-lawrence-county-government-computers/531-637645fa-2797-416f-b890-e95112333106.

[3] *See* Mike Lowe, *Laporte County Government Pays $130K Ransom to Hackers*, WGNTV (July 18, 2019), https://wgntv.com/news/laporte-county-government-pays-130k-ransom-to-hackers/.

[4] *See* Patrick Howell O'Neill, *Indiana Hospital Shuts Down Systems After Ransomware Attack*, CYBERSCOOP (Jan. 15, 2018), https://www.cyberscoop.com/hancock-hospital-ransomware/.

Key Findings

- The Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident, while over 46% of respondents identified as somewhat concerned and almost 49% identified as very concerned. When asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents).
- In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% of respondents indicated that they had experienced a successful cyber incident during this timeframe, while 67% of respondents indicated that their organization did not experience a successful cyber incident and 13% were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss.
- The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; about 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and about 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, 95% had installed antivirus software, while over 75% had updated/patched software, and over 70% had provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.
- Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. Of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half attributed this decision to the organization being unsure what to do, while 40% explained that their organization did not think it was at risk. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.
- In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. Of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software and implementation of remote backups.
- The development and documentation of incident planning and response is a key cybersecurity practice. About 27% of respondents reported that their organization had written cyber incident planning and response documentation, with more than half indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive.

- Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% of respondents indicated this role was filled by their Chief Information Officer, and about 14% indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role).
- Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% of those organizations adopting a framework and 36% had adopted the Center for Internet Security (CIS) Critical Security Controls.
- About half of respondents indicated that their organization had cyber risk insurance; 26% indicated that their organization did not have cyber risk insurance; remaining respondents were either unsure or declined to answer. Respondents were next asked why their organization obtained a cyber risk insurance policy. Half of respondents described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40.82%) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy, response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

Understanding Cyber Risk

Although many consumers and businesses think of cyber risk in terms of hacked computers and stolen credit card numbers, there is a rapidly expanding universe of vulnerabilities fed in part by the explosion in Internet-connected devices and services comprising the Internet of Things. Even before the COVID-19 pandemic, which shifted many personal and professional activities online, cyber criminals, terrorists, hacktivists, and even foreign nation states were exploiting these vulnerabilities to steal identities, intellectual property, and compromise critical infrastructure. In this section, we begin by outlining the technical, economic, and legal dimensions of the cyber threat landscape currently facing organizations. We then turn to recommendations commonly made to organizations seeking to manage their cyber risk profiles, summarizing these best practices in terms of three steps: being aware, being organized, and being proactive. Finally, we discuss several issues that are currently changing the cyber risk landscape.

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.[5] Internet-connected lights and kitchen appliances can be hijacked to launch cyber attacks.[6] Internet traffic can be rerouted to servers around the world without the user's awareness.[7] Supply chain vulnerabilities and weak encryption can lead to a cascade of failures, yet are hard to identify and address.[8] Each of these cyber risks, as with so many others, require a suite of corporate

[5] *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.

[6] *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.

[7] *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.

[8] *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),

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.[9]

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.[10] 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 a 2019 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.[11] 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.[12] For example, a 2019 cybersecurity IBM survey of large firms found that only 16% of respondents considered user security awareness training to be a priority.[13]

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.[14]

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

https://www.industryweek.com/supply-chain/customer-relationships/article/21959294/how-vulnerable-is-your-supply-chain.

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

[10] *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/.

[11] 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.

[12] *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.

[13] *IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them*, IBM (Apr. 11, 2019), https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them.

[14] *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/.

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 is projected to decline to 7% CAGR by 2023.[15] Part of this decline may be explained by more boards pushing back and asking for improved data and understanding of what increased cybersecurity spending has achieved after years of heavy investment.[16] And, to date, many organizations have not faced significant fines, litigation costs, or incentives to change behavior. A 2018 report from Schinichi Kamiya and colleagues found that "[a]fter suffering a breach of customers' personal data, the average attacked firm loses 1.1 percent of its market value and experiences a 3.2 percentage point drop in its year-on-year sales growth rate."[17] In fact, some firms, such as LinkedIn, saw their stock prices actually rise following significant cyber attacks.[18] As a result, an open debate is underway about whether or not we are experiencing a market failure in cybersecurity and, if so, what role state and federal governments should have in addressing it.

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. 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. Figure 1 below shows variation in the number of cybersecurity laws adopted by states, taking into account laws that expressly criminalize phishing, distributed denial-of-service (DDoS) attacks, spyware, and ransomware, as well as the creation of a state-wide cybersecurity task force and adoption of the NAIC data security model law for the cyber-insurance industry. Furthermore, even states that have adopted similar laws may have implemented them at different times. For example, Figure 2 summarizes the year each state passed their Breach Notification Law.

Legislative policymaking is ongoing in this area. Thirty-eight states, Washington, D.C., and Puerto Rico have considered nearly 300 bills or resolutions that deal significantly with cybersecurity in 2020,[19] and 31 states enacted new cybersecurity legislation so far this year.

[15] *Id.*

[16] *See* Louis Columbus*, Why Cybersecurity is Really a Business Problem*, FORBES (June 25, 2020), https://www.forbes.com/sites/louiscolumbus/2020/06/25/why-cybersecurity-is-really-a-business-problem/#362b6134436c.

[17] Shinichi Kamiya, *What is the Impact of Successful Cyberattacks on Target Firms?*, NAT'L BUREAU OF ECON. RES. (NBER Working Paper No. 24409, 2018), http://www.nber.org/papers/w24409.

[18] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, June 10, 2012, at B1.

[19] Cybersecurity Legislation 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (last visited Aug. 11, 2020).

This marks a significant rise from 2015 when only 26 states considered resolutions and just eight states enacting legislation. Some of the areas seeing the most recent legislative activity include:

- Increasing penalties for cybercrimes.
- Regulating 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.

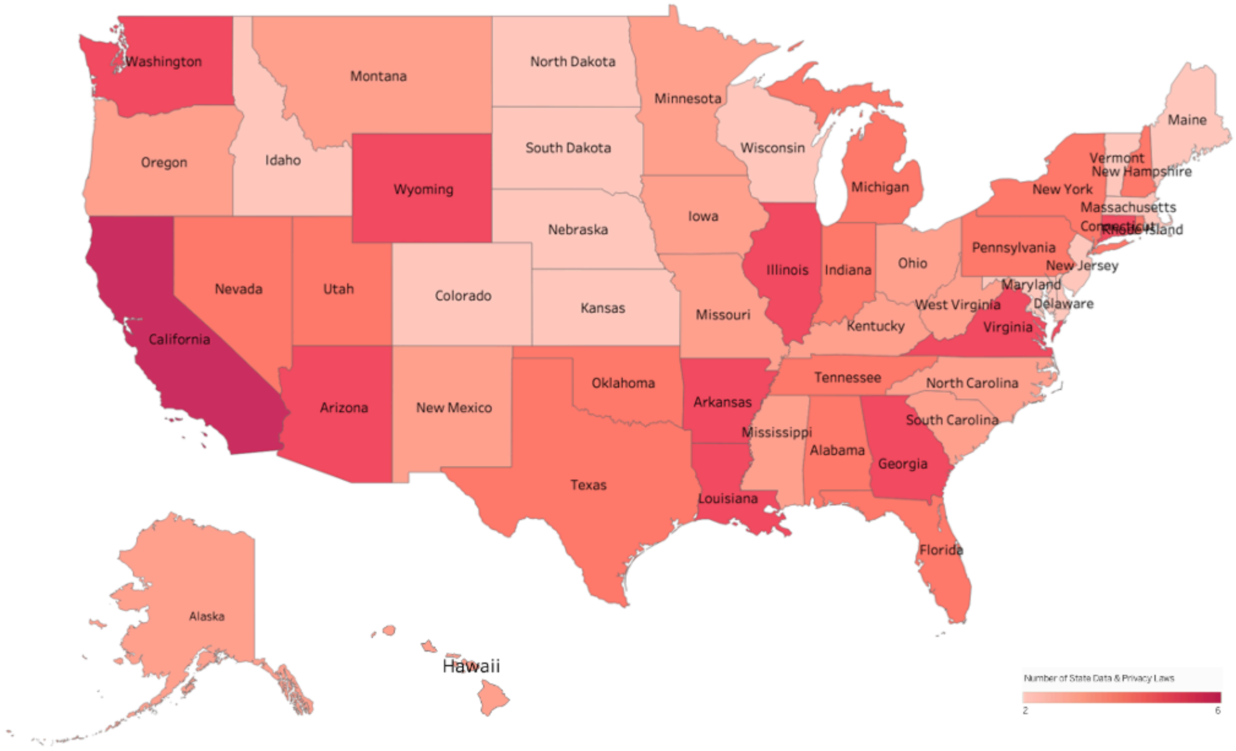


Figure 1: State-Level Cybersecurity Laws (2020)

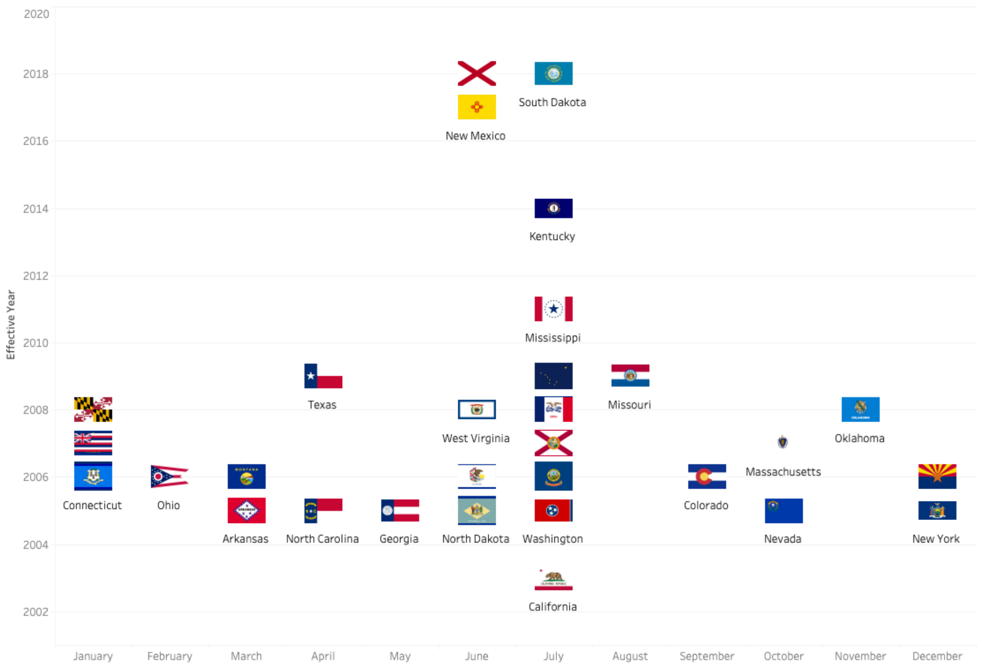


Figure 2: State Breach Notification Laws

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.[20] 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.[21] 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.[22] 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

[20] 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.

[21] *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.

[22] *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/.

understand their vulnerabilities, including network traffic analysis using deep packet inspection.[23]

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.[24] 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.[25] As is explored below in the Results section, still in 2020 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.[26] 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

[23] *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.

[24] *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/.

[25] *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/.

[26] *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.

the chance of a potential unmanaged risk.[27] Hiring qualified cybersecurity personnel is another source of concern, as demonstrated by the fact that there are currently more than 3.5 million unfilled cybersecurity jobs.[28] 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.[29] By some estimates the market is worth more than $2.5 billion in 2020, with projections that it could triple by 2030,[30] 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).[31] 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

[27] *See The 2020 State of IT*, Spiceworks, https://www.spiceworks.com/marketing/state-of-it/report/ (last visited Aug. 10, 2020).

[28] *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.

[29] 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.

[30] *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.

[31] *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.").

per data security incident. The CCPA also directs the California Attorney General to take enforcement actions for privacy violations.[32]

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.[33] 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.[34] 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 with some organizations predicting AI-powered technologies to triple by 2021.[35] An

[32] *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.

[33] *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.

[34] 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.

[35] *The 2020 State of IT*, *supra* note 27.

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 artificial intelligence must be re-trained to keep up.[36] 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.[37] It is designed to automatically identify the relevant features of a malicious file or vector without engineering from a cybersecurity expert.

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.

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.[38]

[36] *Id.*

[37] *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/.

[38] *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.

Methods

A. Aims of this Study

Given the multifaceted cyber threat landscape and the universality of cyber risk concerns to organizations today, it is to be expected that organizations will adopt different approaches to protecting their information and computer systems. These approaches will frequently be difficult to observe without querying organizations directly, as the steps an organization takes to buttress their cybersecurity postures may not be obvious from the outside. However, policymakers, analysts, and organizations themselves can benefit from a clearer description of this decision-making process. Better identification of the factors that organizations consider when making cybersecurity decisions can help policymakers develop incentives to promote decisions that protect consumers – and identify barriers to good decision-making. Analysts can conduct evaluations of cybersecurity policies in order to help identify which policies can be supported by empirical evidence. Organizations may benefit by better understanding the cybersecurity decision-making of their peers, as this may help them identify the standards of their industry.

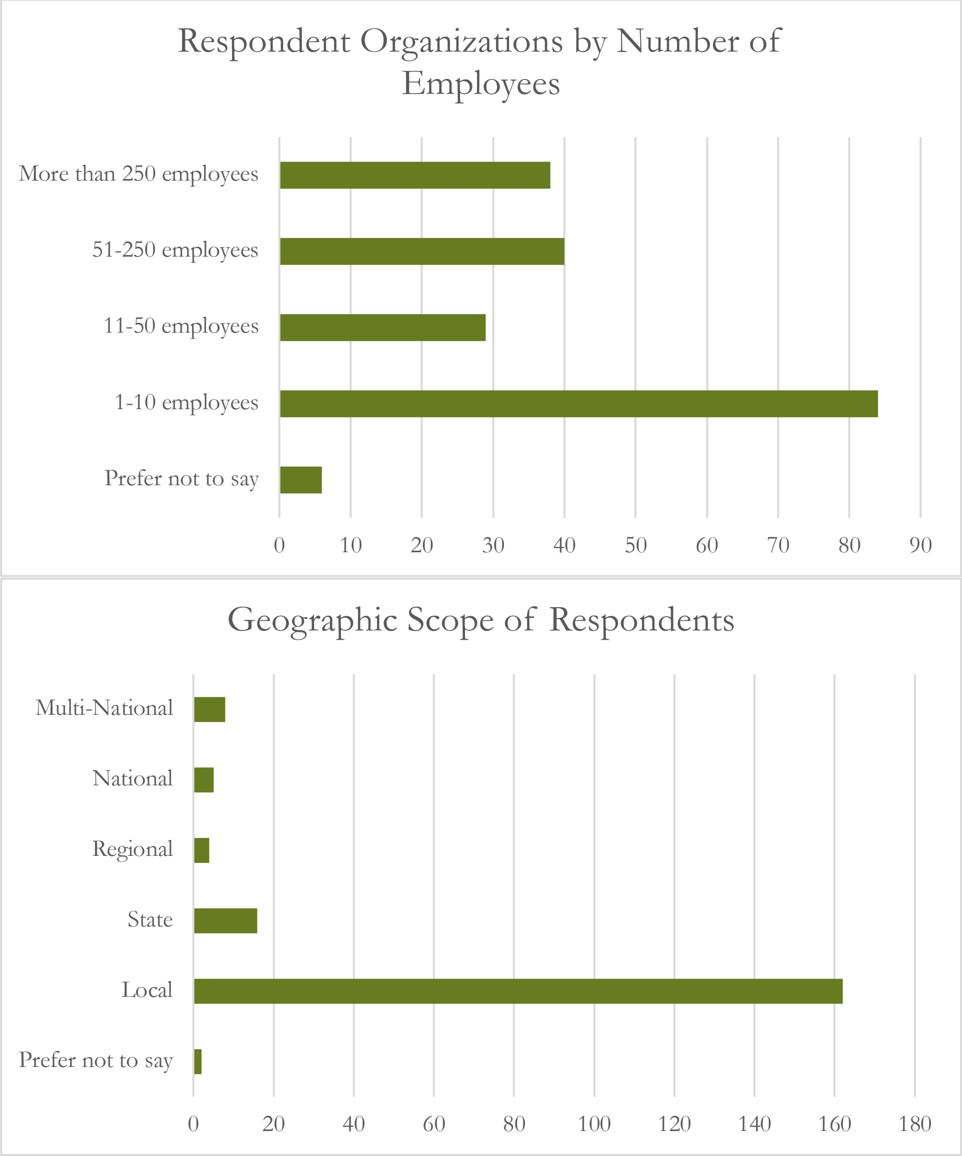
In order to contribute to our current understanding of cybersecurity decision-making, we conducted a survey of Indiana organizations to query them about their perceptions of cyber risk, how their organization manages these risks, and the role of cyber risk insurance in this decision-making process. The content and distribution of this survey are described in the remainder of this section; the next section presents a summary of key results.

B. Survey Development and Distribution

We began this study by consulting with a variety of stakeholders on both the general topics that should be addressed by a cyber risk survey, and any specific questions that they would think it necessary to include. We focused in particular on questions that would elicit information that would be most likely to be useful to cybersecurity decision-makers on both the governmental and organizational levels. Through this process, we identified several key topics to focus on, namely cyber risk perceptions, cyber risk management and planning, and cyber risk insurance use/non-use. We drafted questions to address each of these decision-making dimensions. These questions were then vetted for both completeness and clarity by cybersecurity analysts and stakeholders in order to maximize the likelihood that we would obtain useful information and ensure that would be understandable to potential respondents. The finished survey protocol is provided in Appendix B.

This survey was distributed in partnership with the Indiana Executive Cybersecurity Council and the Indiana Business Research Center. A solicitation and link to the survey was sent to an extensive mailing list of more than 3,000 public and private organizations in Indiana. We received 336 responses, including 197 complete responses and 139 incomplete responses. Incomplete responses were dropped for analysis. This left us with an overall response rate of 6%.

Figure 3 below describes the number of employees and geographic scope of respondent organizations. As can be seen, respondents represented a range of organizational sizes, but most commonly reported that their organization employed 1-10 people. Similarly, respondents most commonly reported that their organization was local in geographic scope by a wide margin (82%, N=162).


Respondent Organizations by Number of Employees

Geographic Scope of Respondents

Figure 3: Description of Respondent Organizations

As there are particular concerns about cybersecurity decision-making amongst organizations that comprise critical national infrastructure, respondents were also asked whether their organization fell within one of these categories. As is shown in Figure 4 below, about 58% of respondents indicated that their organization fell within a critical infrastructure sector. In particular, about 36% of respondents reported that their organization fell within the Government Facilities Sector.

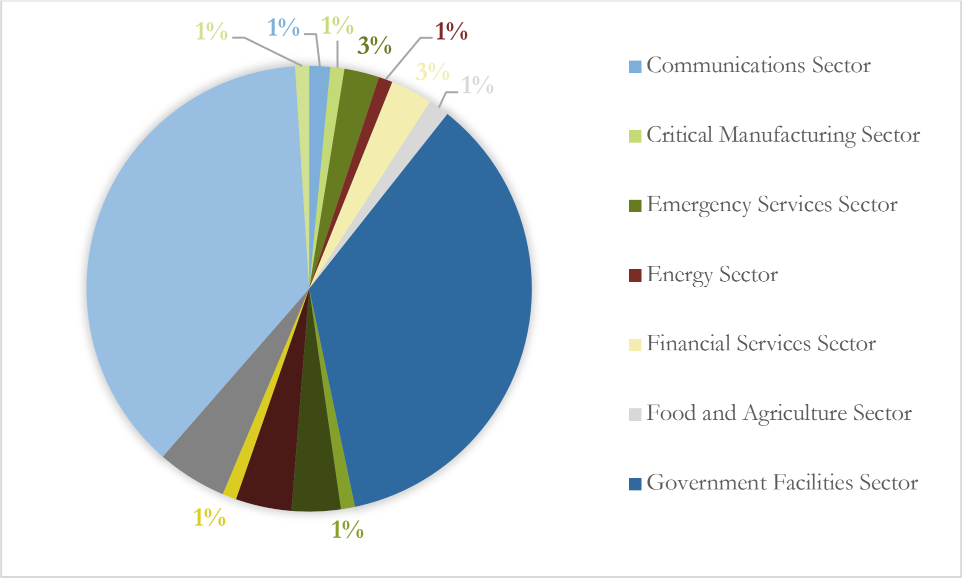


Figure 4: Respondents by Critical Infrastructure Sector

C. Limitations

There are several key limitations to this analysis. It may be that cybersecurity decision-making amongst organizations that chose to respond to this survey may be different from those organizations that did not chose to respond. In particular, representatives from organizations that are more concerned about cybersecurity decision-making may be more likely to respond to the survey, as the issues it raises are more salient to them and their employers. Combined with the relatively low response rate of the survey, this suggests that the results of this analysis should not be seen as representing the exact parameters of cybersecurity decision-making in general. Rather, it should be seen as an exploratory effort to understand the range of factors that might contribute to cybersecurity decision-making in Indiana. Additionally, responses to the survey will be influenced by how respondents interpreted the questions, as well as the scope of their knowledge of their organization's cybersecurity practices and their recollection of these practices. Future, more in-depth qualitative research with organizations could provide additional details and insights that would refine the insights from this paper.

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 Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Almost 49% identified as very concerned and over 46% of respondents identified as somewhat concerned about the risk of a cyber incident, while less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident. As shown in Figure 5 below, when asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents). Of those respondents who indicated that they were concerned about another type of cyber incident, the types of incidents they described included zero-day exploits, attacks through third party vendors, and an attack that resulted in the release of client/patron information.

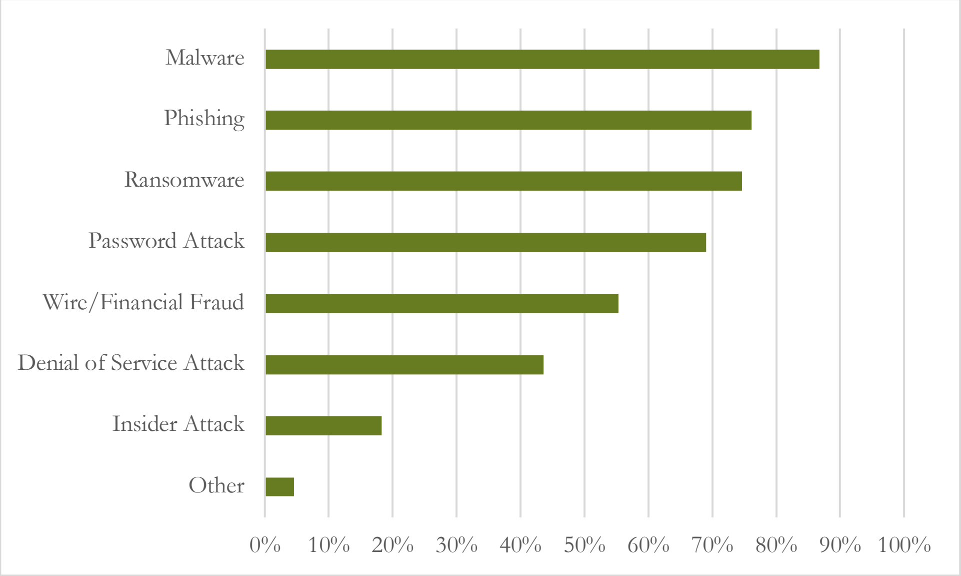


Figure 5: Proportion of Respondents Concerned About Cyber Incidents, By Type

Respondents were also asked to rank the types of cyber incidents they were concerned about in order of how concerned they were. Ransomware attacks were most commonly ranked as the highest concern amongst respondents who provided an answer to this question, while phishing attacks and malware attacks were ranked second and third respectively. Notably, respondents least frequently ranked insider attacks and other types of attacks as their highest source of concern, despite the overall prevalence of these issues.

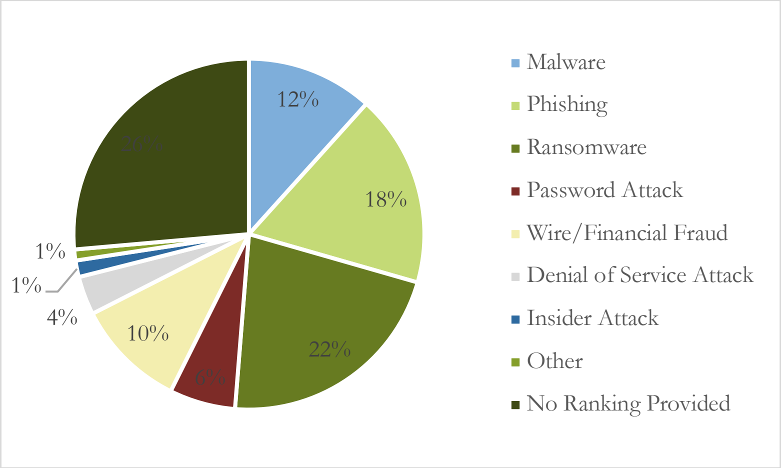


Figure 6: Proportion of Respondents Most Concerned About Each Type of Cyber Incident

In order to situate these results, we can compare them with data on data breaches reported to the Indiana Attorney General's office pursuant to Indiana's data breach notification statute in 2018 and 2019.[39] According to these data, the majority of data breaches reported to the Indiana Attorney General were caused by an external cause, as is shown in Figure 7 below.[40] The next most common cause of a reported data breach – inadvertent disclosure – occurred about a third as often as an external system breach. Reported data breaches were attributed to insider wrong-doing in about 6% of reported data breach. These results roughly align with concerns expressed by our respondents, who both most frequently mentioned external causes of cyber incidents such as malware and phishing attacks as potential sources of concern and ranked these external causes of cyber incidents as their sources of greatest concern.

[39] Ind. Code. Ann. § 24-4.9.

[40] The data used in this figure were obtained from public records of Notice of Security Breach Reports for Indiana. Simplified published versions of these reports are available at Indiana Attorney General, *Identity Theft Protection*, https://www.in.gov/attorneygeneral/2874.htm (last visited Oct. 29, 2020).

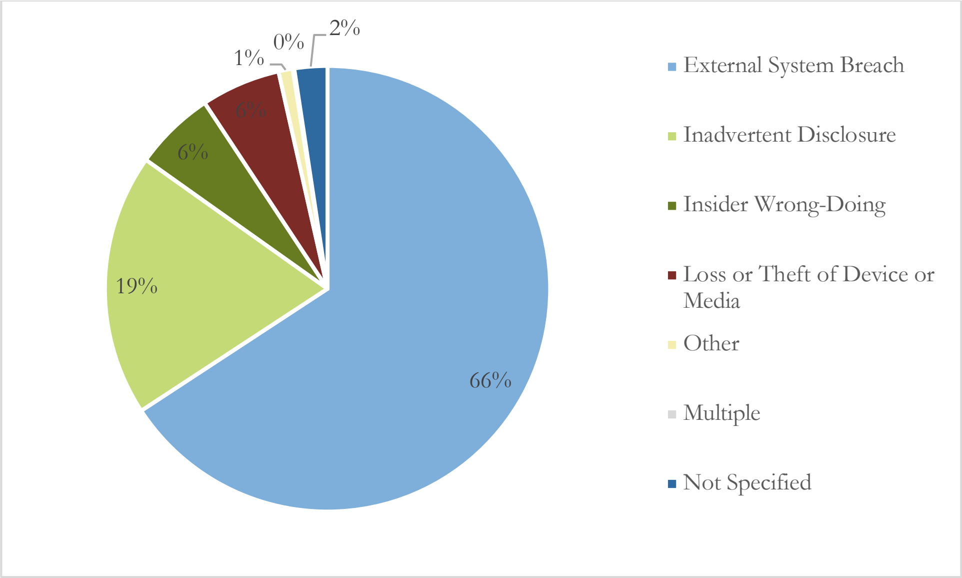


Figure 7: Causes of Data Breaches Reported to the Indiana Attorney General

Respondents were then asked about their concerns regarding the potential consequences of a cyber incident. As is shown in Figure 8 below, respondents most frequently indicated that they were concerned about data being deleted or lost (78% of respondents), data or information being exposed to outsiders (65% of respondents), and identity theft (64% of respondents). Interestingly, only a small proportion of respondents indicated that they were concerned with other potential consequences of a cyber incident. These respondents specifically indicated that they were concerned about personally identifying information being used against their stakeholders, and the loss of resources and staff time incurred in the course of responding to the incident.

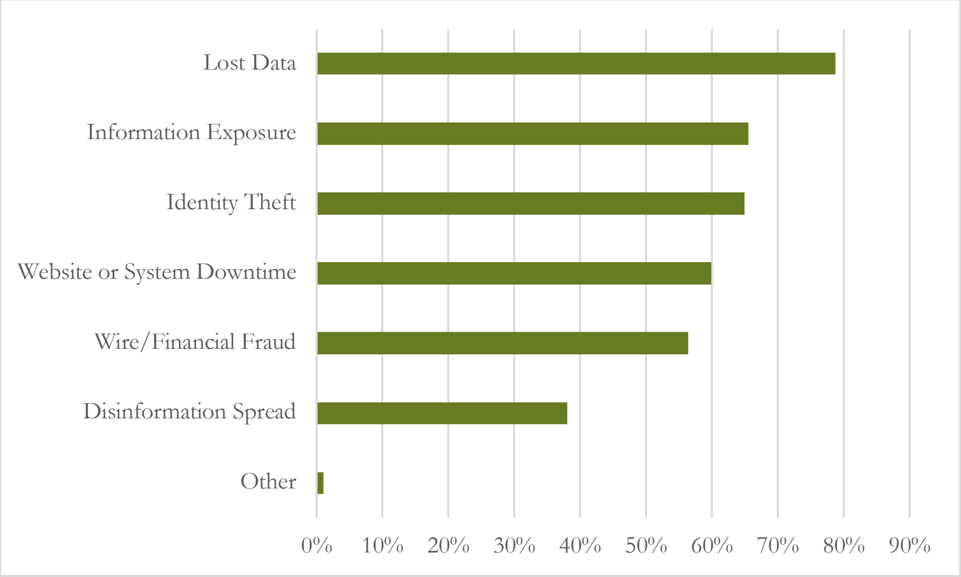


Figure 8: Proportion of Respondents Concerned About Consequences of Cyber Incidents, By Type

Respondents were again asked to rank the potential consequences of cyber incidents based on their level of concern. Of those who provided an answer to this question, respondents most frequently indicated that they were most concerned about data being deleted or lost (22% of respondents), data being exposed to outsiders (16% of respondents), and wire/financial fraud (11% of respondents).

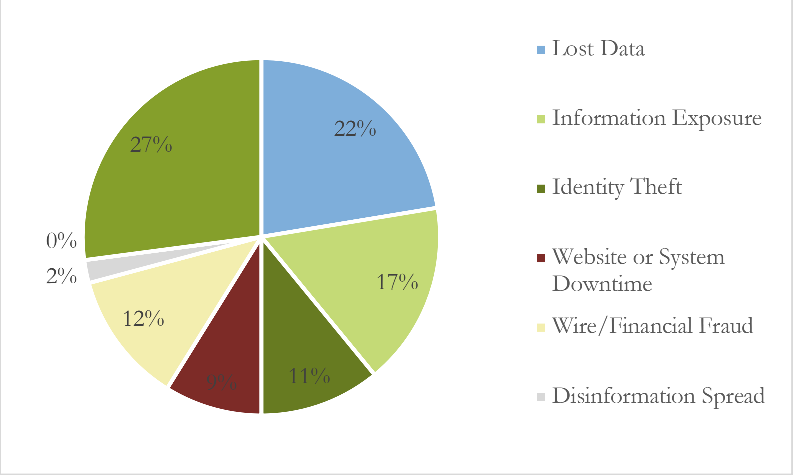


Figure 9: Proportion of Respondents Most Concerned About Consequence of Cyber Incident

2. Previous Events and Responses

In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% (N=38) of respondents indicated that they had experienced a successful cyber incident during this time frame, while 67% (N=132) of respondents indicated that their organization did not experience a successful cyber incident and 13% (N=25) were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss. Respondents were then asked to describe the most recent incident experienced by their organization. As is shown in Figure 10 below, the most common types of cyber incidents experienced by respondents were phishing attacks and wire/financial fraud, while no respondents indicated that the most recent incident experienced by their organization was a DDoS attack.

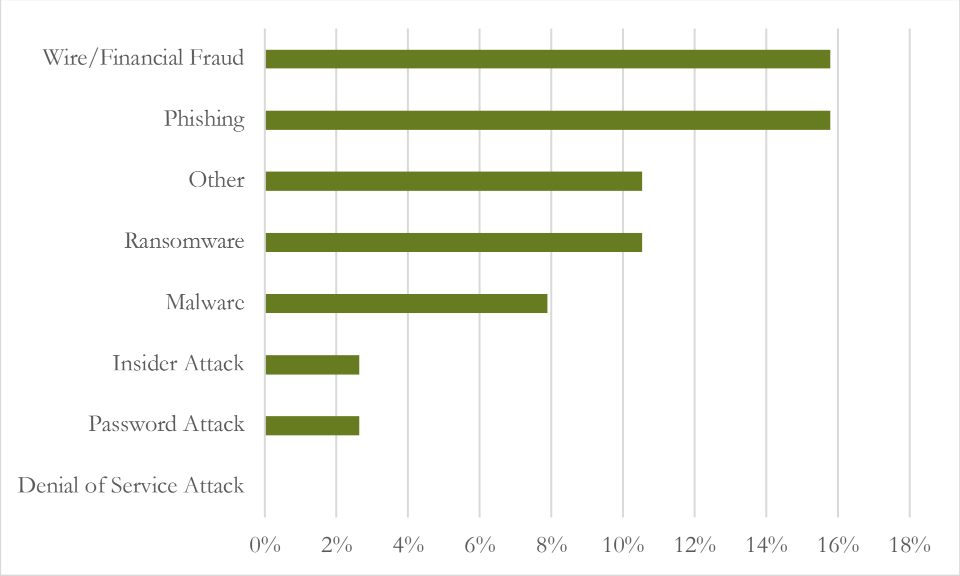


Figure 10: Types of Cyber Incidents Experienced by Respondents' Organizations

Respondents also described the consequences of the most recent cyber incident experienced by their organization; these results are summarized in Figure 11 below. Over 18% (N=7) respondents reported experiencing exposure of information to outsiders as a result of the cyber incident, while over 15% (N=6) reported wire/financial fraud as a result of the cyber incident.

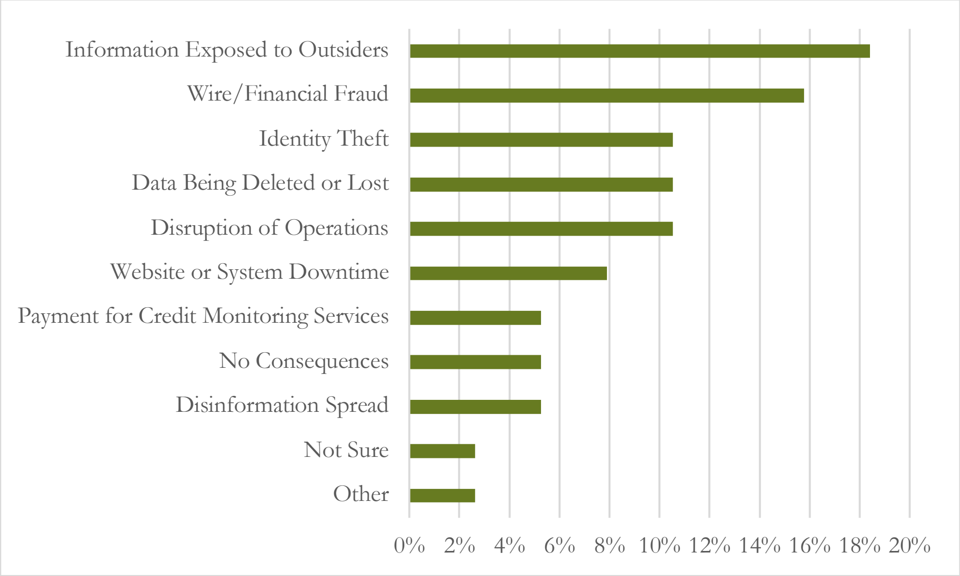


Figure 11: Consequences of Cyber Incidents Experienced by Respondents' Organizations

B. Managing Cyber Risk

1. Prevention and Mitigation of Cyber Incidents

Prevention is a key component of an effective cybersecurity strategy. The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; over 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and over 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, there was a high degree of commonality in the mechanisms adopted. As shown in Figure 12 below, over 95% of respondents who indicated that they had taken steps to prevent cyber incidents installed antivirus software (N=155), while over 75% (N=126) indicated that they had updated/patched software and over 70% (N=114) provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.

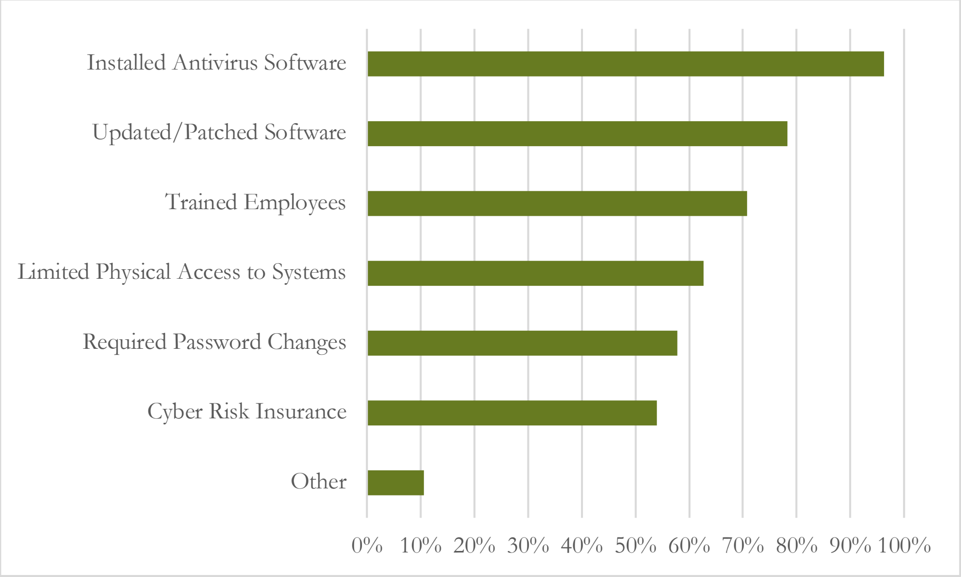


Figure 12: Mechanisms Used to Prevent Cyber Incidents

Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. As shown in Figure 13 below, of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half (N=8) attributed this decision to the organization being unsure what to do, while 40% (N=6) explained that their organization did not think it was at risk. Twenty percent (N=3) indicated that their organization had reasons other than those provided by the survey for not adopting cyber risk prevention mechanisms; these respondents generally went on to explain that their organization was either too small to engage in prevention mechanisms or did not have their own equipment to protect. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.

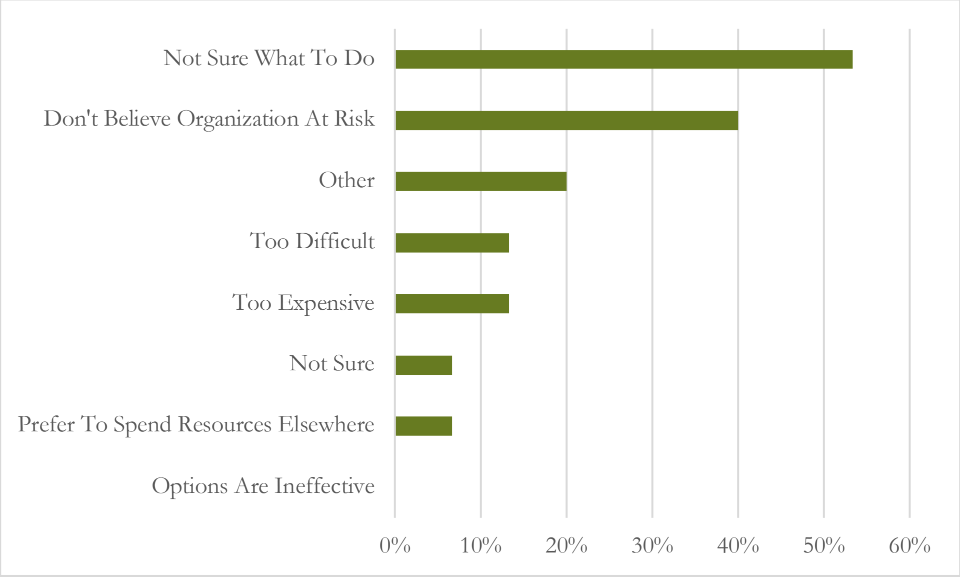


Figure 13: Reasons for Not Adopting Prevention Mechanisms

Almost 70% (N=134) respondents indicated that their organization had taken steps to mitigate the impact of a cyber incident, while about 11% (N=23) indicated that their organization had not taken these steps and about 19% (N=37) were not certain. Respondents who indicated that their organization had adopted mechanisms to mitigate cyber incidents were then asked what mitigation mechanisms their organization had undertaken. As is shown in Figure 14 below, almost 85% (N=113) of respondents indicated that their organization had installed automatic back-up systems, while approximately 60% (N=84) of respondents indicated that their organization had purchased cyber risk insurance. Almost 12% (N=16) of respondents described other cyber incident mitigation mechanisms undertaken by their organization; such mechanisms included upgrading hardware, strengthening firewalls, and testing their network or incident response plan.

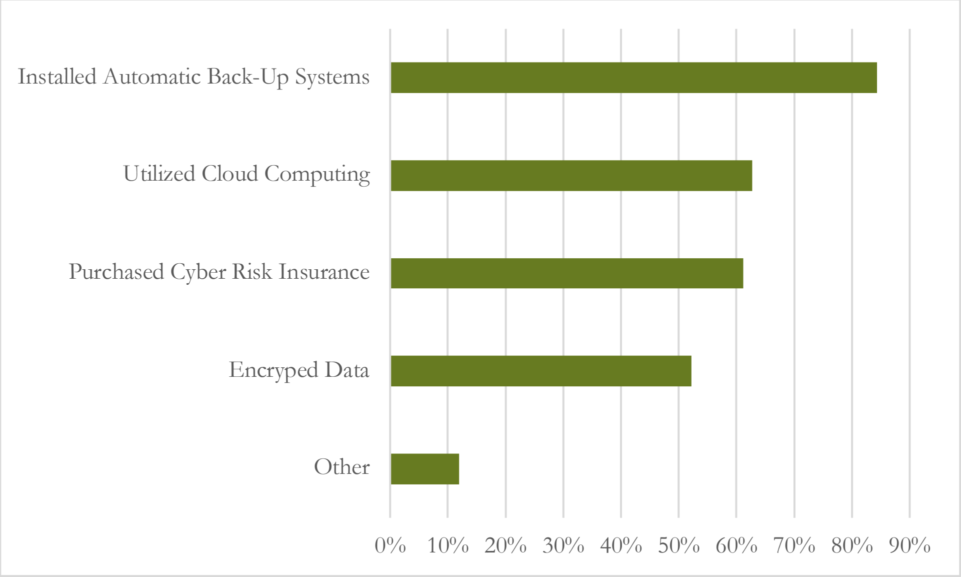


Figure 14: Mechanisms Used to Mitigate Cyber Incidents

Respondents who indicated that their organizations had not adopted mitigation measures were then asked why these measures had not been adopted. Respondents most commonly cited uncertainty about how to accomplish this as the reason their organization had not adopted mitigation mechanisms, with about 47% (N=11) respondents adopting this option. Twenty-six percent (N=6) of respondents indicated that their organization had not adopted mitigation mechanisms because they didn't believe themselves to be at risk. The approximately 17% (N=4) of respondents who characterized their organization as having other reasons for not adopting mitigation mechanisms elaborated that these reasons included not having technical infrastructure to secure or currently being at the stage of investigating mitigation options.

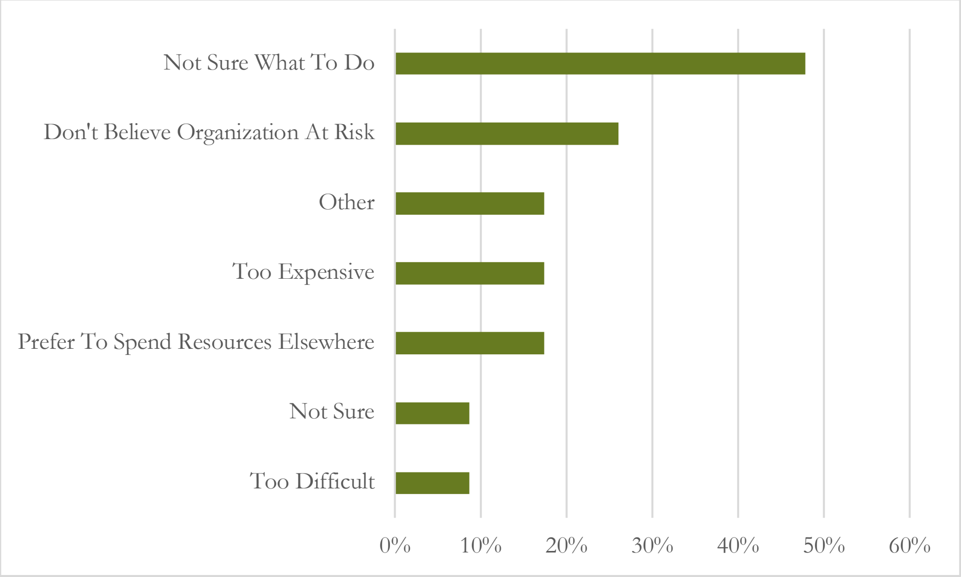


Figure 15: Reasons for Not Adopting Mitigation Mechanisms

2. Cybersecurity Practices, Personnel, and Training

In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. As is shown in Figure 16 below, of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software (N=88) and implementation of remote backups (N=86). The next most commonly adopted practice was use of multi-factor authentication, which about a quarter of respondents had indicated that their organization had adopted.

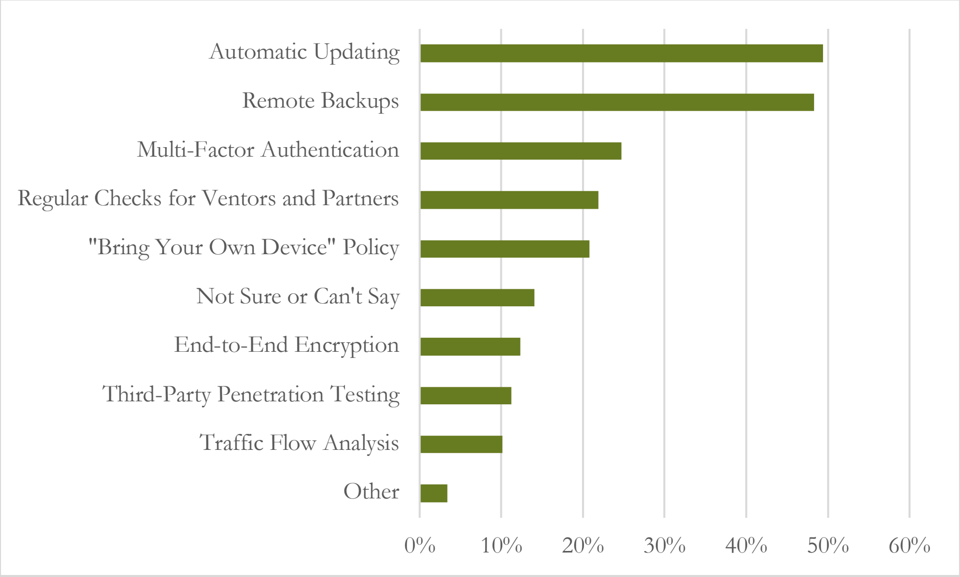


Figure 16: Cybersecurity Practices Adopted

The development and documentation of incident planning and response is a key cybersecurity practice. About 27% (N=55) of respondents reported that their organization had written cyber incident planning and response documentation, with more than half (N=109) indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive. Respondents who indicated that their organization had written cyber incident planning and response documentation were then asked about their perceptions of the documentation. As shown in Figure 17 below, these perceptions were weakly positive on average, with respondents on average falling between “somewhat agree” and “neither agree or disagree” for all statements. However, there was a degree of polarization in these responses, with “strongly agree” being the most frequently occurring response to all statements.

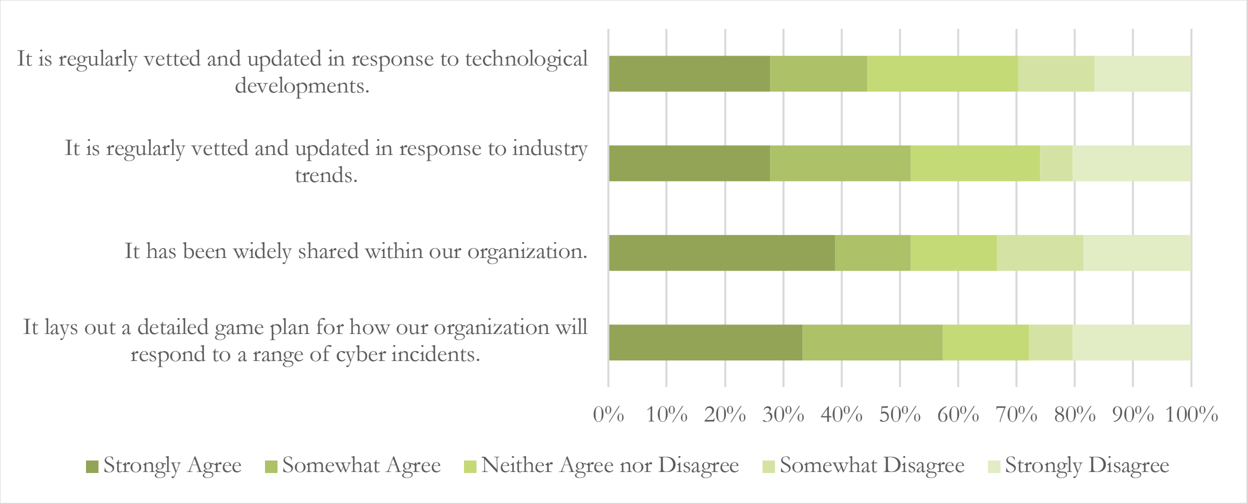


Figure 17: Perceptions of Cybersecurity Documentation

Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% (N=30) of respondents indicated this role was filled by their Chief Information Officer, and about 14% (N=28) indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role). The heterogeneity of these responses suggests that many Indiana organizations seek guidance about corporate governance best practices to ensure that cybersecurity and data privacy are adequately integrated into organizational decision-making.

Respondents were also asked how many cybersecurity professionals were employed at their organization. Sixty-seven percent (N=133) indicated that their organization did not employ a cybersecurity professional, and 23% (N=47) indicated that their organization employed between 1 and 5 cybersecurity professionals. Additionally, as all employees can play a role in ensuring an organization's cybersecurity, respondents were asked about cybersecurity training practices at their organizations. While 58% (N=116) indicated that their organization had provided some employees with cyber risk awareness training, only 29% (N=58) of respondents stated that they themselves had received such training. A plurality of respondents who received such training (44%, N=25) stated that they received yearly training, while a smaller minority (32%, N=18) stated that their received training once a quarter.

3. Usefulness of Standards & Frameworks

A proactive approach to cybersecurity includes preemptively identifying security weaknesses and adding processes to identify threats before they occur. However, a plurality of respondents (37%, N=69) were not sure whether their organization was using specific tools to proactively manage cyber risk. Thirty-four percent (N=32) indicated that their organization had revised or updated their incident response plan, while 32% (N=60) indicated that their organization had consulted news reports to proactively manage cyber risk. The 8% (N=16) of respondents who stated that their organization had taken other steps to proactively manage cyber risk described that these steps included having their computer system audited and hiring a consultant for monitoring.

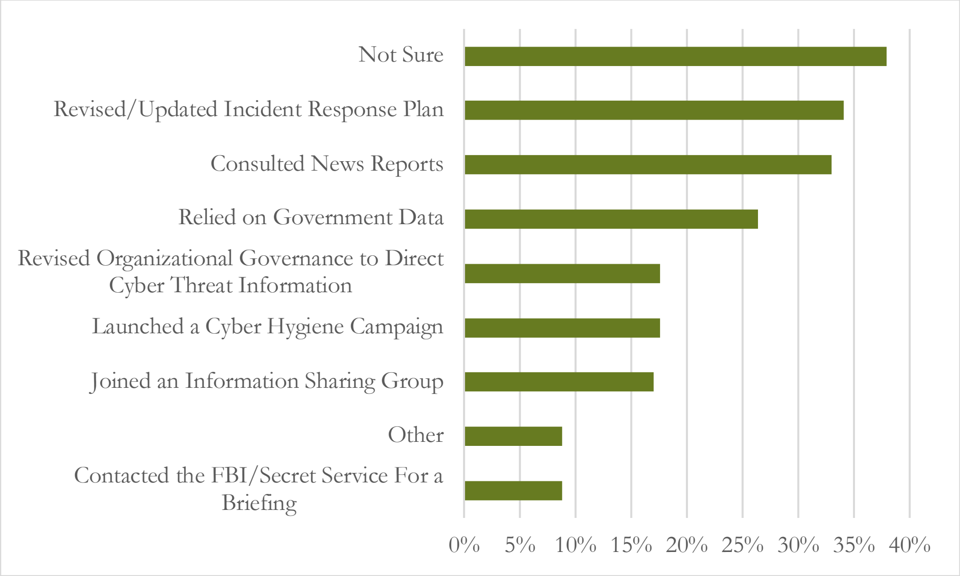


Figure 18: Tools Used to Proactively Manage Cyber Risk

Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents (29%) stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% (N=34) of those organizations adopting a framework and 36% (N=21) had adopted the Center for Internet Security (CIS) Critical Security Controls.

C. Role of Cyber Risk Insurance

About half of respondents (N=98) indicated that their organization had cyber risk insurance; 26% (N=52) indicated that their organization did not have cyber risk insurance; remaining respondents (N=47) were either unsure or declined to answer. In this section, we explore how organizations with cyber risk insurance decided to obtain this insurance coverage, what is covered under these policies, and what is required by these policies.

1. Adoption of Cyber Insurance

Respondents with knowledge of when their organization had obtained cyber risk insurance most frequently indicated that this insurance had been obtained within the last five years, as indicated in Figure 19 below. Interestingly, one respondent indicated that their organization had obtained cyber risk insurance in 2001, almost a decade before any other respondent.

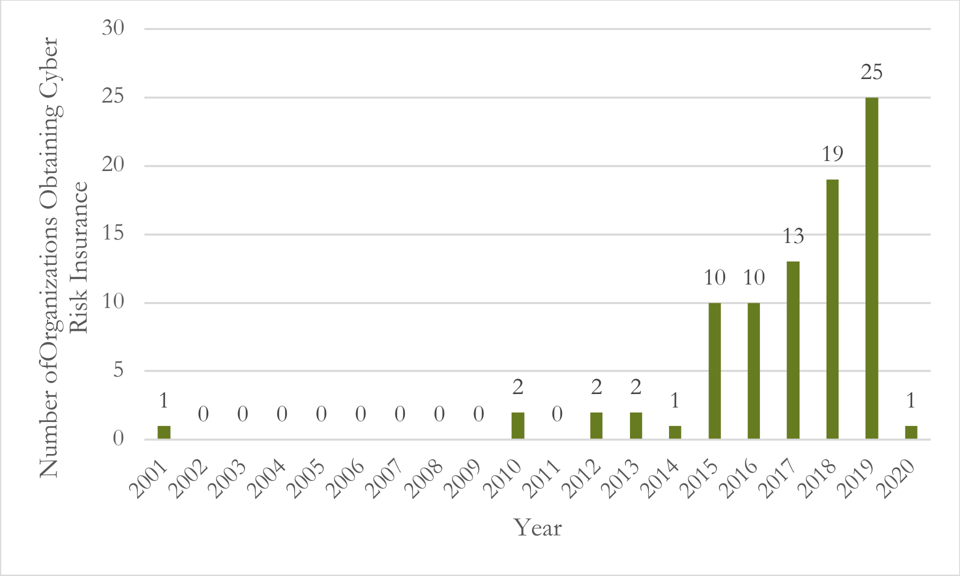


Figure 19: Year Cyber Risk Insurance Was Obtained

Respondents were then asked why their organization obtained a cyber risk insurance policy; the results of this question are described in Figure 20 below. Half of respondents (N=49) described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40%, N=40) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy,[41] response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

[41] As coverage provided under a general policy might be different than coverage provided under a cyber-specific insurance policy, these responses could raise concerns about an additional source of insurance policy variation amongst respondents. However, as only three respondents indicated that their organization obtained cyber insurance as part of a more general policy, these responses have probably not had an outsized influence on our overall analysis.

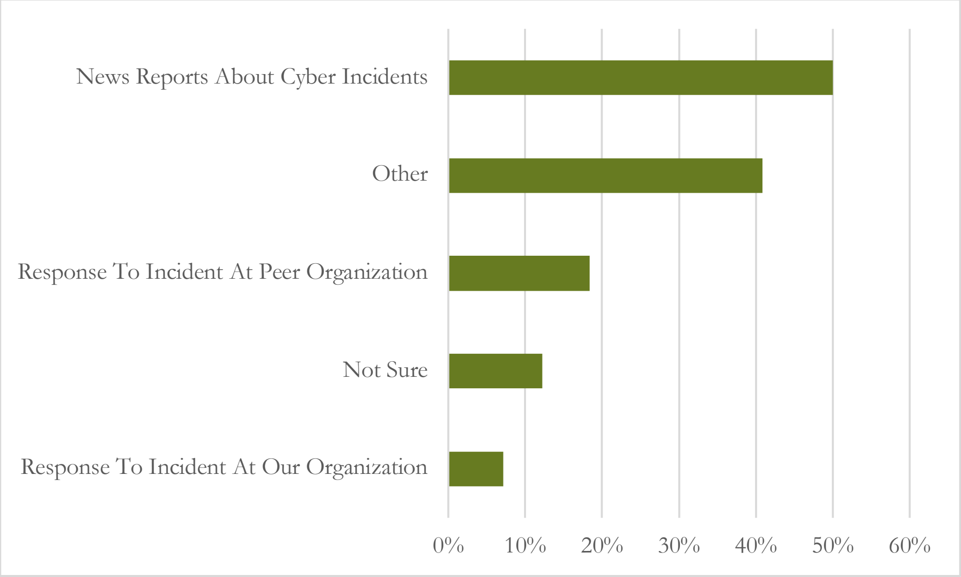


Figure 20: Reasons for Obtaining Cyber Risk Insurance

2. Cyber Insurance Coverage

Cyber insurance plans may offer coverage for incidents that occur under a variety of circumstances, and losses that occur to a variety of people and organizations. Insurance plans commonly cover first-party losses, which are losses that are incurred by the insured. Figure 21 below describes the first-party losses covered by respondent organizations' insurance plans. In particular, respondents whose organizations had cyber risk insurance most commonly reported that their organization's insurance policy covered losses due to damage to computers or information systems (54%, N=53), with a similar but slightly smaller number of respondents indicating that their organization's cyber insurance policy covered expenses related to responding to the breach (52%, N=51).

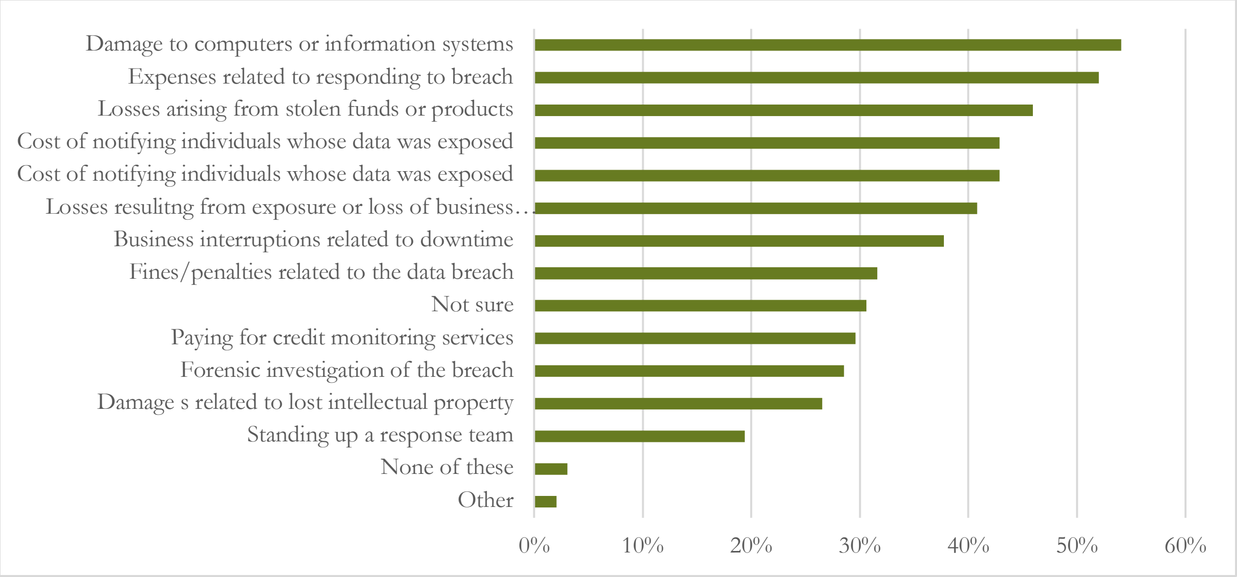


Figure 21: First Party Losses Covered Under Cyber Insurance

In addition to first party losses, cyber insurance plans may also cover third-party losses, which are losses incurred by other parties for which the insured party may nonetheless be liable. As is shown by Figure 22 below, respondents were less sure about the third-party losses covered under their organization’s cyber insurance policy. However, about 33% (N=33) of respondents whose organizations have cyber risk insurance policies reported that this policy included costs for legal defenses related to the data breach, while about 26% (N=26) reported that this policy included coverage for claims for damages from those whose information was exposed by the incident.

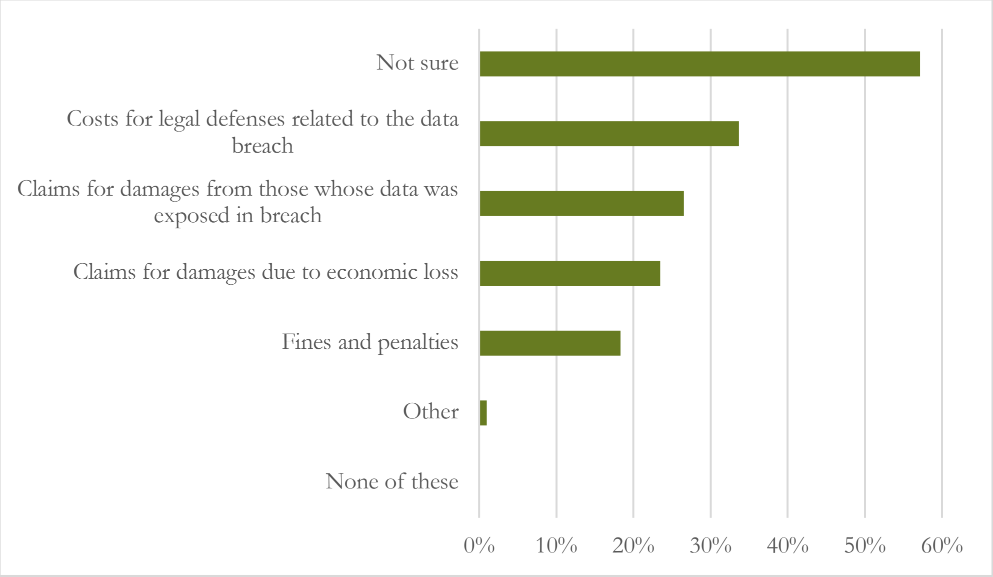


Figure 22: Third Party Losses Covered Under Cyber Insurance

Over 60% (N=59) of respondents with cyber insurance policies reported that these policies included a limit on coverage; the remainder were largely unsure as whether their policy included such a limit. Out of the 35 respondents who reported the amount of their coverage limit, the most commonly reported limit was $1 million; however, some respondents reported a coverage limit in the hundreds of millions of dollars. In addition to limitations on coverage amount, insurers may also exclude certain categories of incidents from coverage under a policy. The majority of respondents who indicated that their organization had insurance coverage were unsure as to whether that insurance policy excluded coverage in certain circumstances, although almost 20% (N=18) of respondents whose organizations had cyber risk insurance reported that this policy had coverage exclusions. Of those respondents who were able to provide information about these exclusions, the most frequently cited reason for exclusion was acts of war or terrorism, with losses that occurred because the organization failed to provide and maintain adequate security.

3. Required Security Measures

As insurers bear risks associated with potential cyber incidents, it is common for cyber risk insurance policies to require the insured organization to undertake certain security practices. Of those respondents who indicated that their organization had a cyber risk insurance policy, 47% of them indicated that this policy required them to undertake certain security measures. As is shown in Figure 23 below, the most commonly required security practices were employee training and cyber hygiene, with about 40% (N=19) of those whose organizations were required to adopt security practices by their insurer indicating that these required practices included employee training. About 34% (N=16) indicated that their insurer required their organization to engage in mandatory, automatic patching of systems. Respondents who indicated that their insurer required other security measures were asked to describe these security measures.

Responses included the development of a cybersecurity plan and compliance with the Payment Card Industry Data Security Standard.

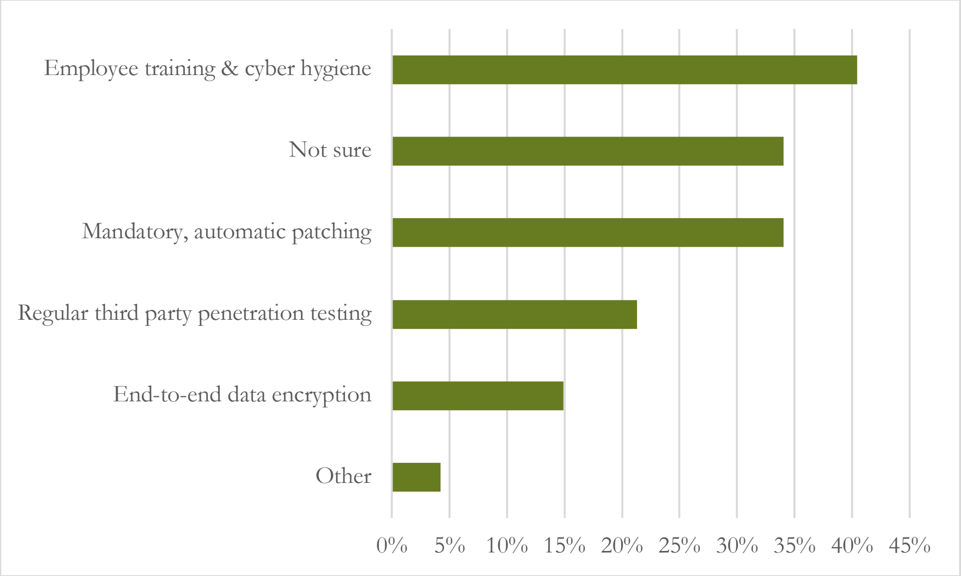


Figure 23: Security Measures Required by Respondents' Insurer

4. Non-Adoption of Cyber Risk Insurance

Policymakers and analysts interested in understanding cyber risk insurance decision-making can learn just as much from organizations that do not have cyber risk insurance as from those who do. Consequently, respondents whose organizations did not have a cyber risk insurance policy were asked whether their organization had ever considered obtaining a cyber risk insurance policy and, if so, why they did not decide to obtain such a policy. Almost half (48%; N=46) of respondents whose organizations did not have a cyber risk insurance policy indicated that their organization had never considered obtaining such a policy, while 38% (N=37) indicated that they were unsure. About 13% (N=12) indicated that their organization had considered obtaining such a policy and had decided against it. These respondents most commonly indicated that cost was a factor in the decision not to obtain cyber risk insurance, either because they believed it to be too expensive or their preferred to spend resources on other policies. One respondent who provided an additional reason that their organization had not adopted a cyber risk insurance policy indicated that their organization may have been "overwhelmed with what exactly we really needed to obtain."

Respondents who did not currently have cyber risk insurance were asked what would encourage their company to obtain a cyber risk insurance policy as an open-ended question. Responses unsurprisingly covered a range of potential factors. Many respondents described the cost of obtaining a policy as a significant factor, frequently mentioning affordability and the need for "a better value proposition." Other respondents indicated that their organization would be more likely to obtain cyber risk insurance if they perceived they were more at risk ("awareness of the treat and the damage that could result"), or if they obtained additional information about their level of risk either through incidents at peer organizations or general statistics. Finally, some respondents indicated that their organizations were unlikely to ever obtain cyber risk insurance, generally due to the fact that they did not perceive that their organization was ever likely to be at risk.

Policy Opportunities

A. Awareness Training

As was made clear in our results, there is a clear need to help educate organizations about cybersecurity best practices with more than half of respondents being unsure of which techniques and tools to use to best mitigate the particular cyber risks they face. In particular, given concerns over malware, phishing, and ransomware, public-private training sessions would seemingly be well suited to focus on these issues in particular. Indiana has made strides in this regard such as through the Indiana Cybersecurity Hub,[42] and the Indiana Information Sharing and Analysis Center (IN-ISAC).[43] However, greater coordinated outreach by leveraging educational institutions, civil society groups, and law enforcement could address this lack of awareness potentially through a push to promote October as Cybersecurity Awareness Month. Senior leadership in particular, including boards of directors, should be a key area of focus given the diffusion of cybersecurity responsibilities and persistent lack of clarity about accountability at so many Indiana organizations.

A concrete idea that the Executive Council could consider to help address this clear need is by working with universities and community colleges across the state to create a cybersecurity curriculum that local and state leaders could access and would answer these questions, such as best practices for ransomware mitigation. The site could also include model incident response plans, explainers for cyber risk insurance coverage and common exclusions, and other tools. Relatedly, we would encourage a deeper partnership – perhaps in collaboration with regional economic development authorities, the IN-ISAC, and the Indiana Business Research Center – between state and local leaders on quarterly trainings on various cybersecurity hot topics such as ransomware and the need to enable multi-factor authentication, end-to-end encryption for sensitive databases, and BYOD policies.

B. Proactive Cybersecurity

As seen in the results to this survey, while many organizations (82% of respondents) have taken some steps to prevent a cyber incident mostly through investing in antivirus solutions and patching, it is not uncommon to maintain a reactive cybersecurity stance across Indiana organizations. Proactive cybersecurity is an amorphous field, comprising a wide range of active and passive measures that are often commonly, though not always accurately, referred to as "active defense." While "hacking back" is a lightning rod within this field,[44] it is just one data

[42] *See* Indiana Cybersecurity Hub, https://www.in.gov/cybersecurity/ (last visited Oct. 1, 2020).

[43] IN-ISAC, https://www.in.gov/cybersecurity/in-isac/ (last visited Oct. 1, 2020).

[44] *See, e.g.*, Carl Franzen, *Should US companies be allowed to hack China in revenge? New report says yes*, VERGE (May 22, 2013), http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back [https://perma.cc/JX7X-FE7X]; *see also* Eric Chabrow, *The Case Against Hack-Back*, BANK INFO. SEC.

point in a larger and more dynamic movement, which includes technological, organizational, and legal best practices deep packet inspection to audits promoting defense-in-depth.[45] Such a "lean in" approach to cybersecurity is essential to help guard against the more reactive mindset that has long bedeviled the field of cybersecurity risk management.[46] There seems to be an opportunity to help educate Indiana organizations about the full range of proactive cybersecurity best practices available to them to help manage various cyber risks. This can include both spreading awareness of, and encouraging the uptake including through government procurement, of leading cybersecurity and privacy frameworks including from NIST. Although this was the dominant option selected by respondents, still more than 40% of Indiana participants are not utilizing it at present. The proposed 2020 IN Attorney General's cybersecurity rule, discussed next, would constitute such a nudge.[47]

C. Defining "Reasonable" Cybersecurity

On September 25, 2020 Indiana Attorney General Curtis Hill proposed a rule that would change the incident response process for Indiana organizations that have experienced a data breach. In brief, the proposal would make two main substantive revisions from the current structure: (1) impose a requirement for database owners to "create, implement and report a corrective action plan (CAP) to the Attorney General within thirty days" of the reported breach; and (2) establish "a 'safe harbor' for what constitutes 'reasonable measures' to safeguard personal information in Indiana."[48] Database owners are those persons or entities that "own or license computerized data that include personal information."[49] Under existing Indiana law, these owners should "implement and maintain reasonable procedures, including taking any appropriate corrective

(Jan. 6, 2015), http://www.bankinfosecurity.com/case-against-hack-back-a-7759 [https://perma.cc/9WXW-U7TK]; Tom Field, *To 'Hack Back' or Not?*, BANK INFO. SEC. (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545 [https://perma.cc/7XUH-H8T9] (discussing, among other things, the likelihood of prosecution in the United States for engaging in hacking back).

[45] *See, e.g.*, Orla Cox, *Proactive Cybersecurity — Taking Control Away from Attackers*, SYMANTEC (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [https://perma.cc/3XM6-R369]; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cybersecurity/d/d-id/1108270 [https://perma.cc/8XYL-H3PN]; *Hackback? Claptrap! — An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality.").

[46] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [https://perma.cc/N6L4-KAML] (comparing cybersecurity investment rates across countries and concluding that "it appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive").

[47] IN Attorney General Proposal Rule LSA Document # 20-366, https://www.workplaceprivacyreport.com/wp-content/uploads/sites/162/2020/09/IN-AG-Hill-Proposed-Regulations.pdf.

[48] *See* Joseph J. Lazzarotii, *Indiana AG Proposed Regulations Creating Corrective Action Plan Requirement and Cybersecurity Safe Harbor*, WORKPLACE PRIVACY REP. (Sept. 25, 2020), https://www.workplaceprivacyreport.com/2020/09/articles/data-breach-notification/indiana-ag-proposed-regulations-create-corrective-action-plan-requirement-and-safe-harbor/.

[49] *Id*.

action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[50] As Attorney General Hill said in describing the proposal: "This rule would provide businesses a playbook on how to protect data, and would protect the businesses that follow the playbook. It's a win for both consumers and businesses."[51]

A key piece of this effort is specifying 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."[52] 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.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Security Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browsing Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

[50] *Id*.

[51] *Id*.

[52] 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/.

Instead, the proposed Indiana rule mirrors the efforts from other Midwestern states including Ohio's safe harbor law and offers a list of leading cybersecurity frameworks that, if adopted, are presumptively reasonable. These include: the aforementioned NIST CSF, ISO 27000, along with sector-specific laws depending on the sector and industry in which the covered entity is operating, which could include the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act (HIPAA), and/or the payment card industry data security standard (PCI). There are also proposed requirements for regular improvements, such as by implementing up-to-date versions of the NIST CSF, timely tracking vulnerabilities and applying remediation strategies, and updating incident response plans at least annually.

D. Incident Response Best Practices

Under the proposed 2020 Indiana AG cybersecurity rule, covered entities may need to take steps to amend their incident response plans to submit a CAP within a timely fashion (e.g., within thirty days). This requirement would help address the demonstrated lack of planning as seen in the results of this survey with only 27% of respondents reporting that their organizations had a written incident response plan on file. Requirements built-in to the proposed rule to ensure that such plans are regularly updated (e.g., at least annually) could help address this shortfall. Additional steps to aid in this process, and dovetailing with the need for better cyber awareness, would be to encourage that such plans are widely communicated, and even vetted by third parties including insurance firms. The Executive Council could work with universities and other partners to coordinate regular incident response and tabletop exercises to highlight the importance of this proactive planning. One idea would be to focus on one critical infrastructure sector roughly each month, and then conduct a follow-up survey to see how practices have changed after the trainings have taken place.

E. 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 20% 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.

Appendix A: Sources Used for Figure 1

- **State Phishing** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx
- **Ransomware & DDOS** - https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Ransomware
- **Spyware** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx
- **Cybersecurity Taskforce** - https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx
- **Cybersecurity interest** - https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf

Appendix B: Indiana Cybersecurity Survey Protocol

Start of Block: Cyber Risk Perceptions

Q1.1
Cyber incidents - such as phishing attempts, malware attacks, and ransomware demands - are increasingly an area of concern for both the public and private sectors. Although organizations have options for managing cyber risk, relatively little is currently known about what steps are being taken, including what role insurance is playing in this planning process. Additional information would help identify barriers that prevent effective cyber risk planning, while enabling organizations to better understand how their cyber risk planning compares with that of their peers. To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, is conducting a study to help explore how Indiana organizations perceive and manage cyber risks. This study will pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy. The report resulting from this study will provide policymakers and law enforcement with important information about cyber readiness, and help Hoosier organizations like yours better understand current cyber practices in your industry.

We are asking you to participate in this study by filling out a short survey describing your organization's perceptions of cyber risk and use of cyber risk insurance. This survey will take no more than 25 minutes to complete. The responses you provide will only be reported in the aggregate. Your participation is entirely voluntary, and you would be free to terminate the survey at any point. Thank you very much.

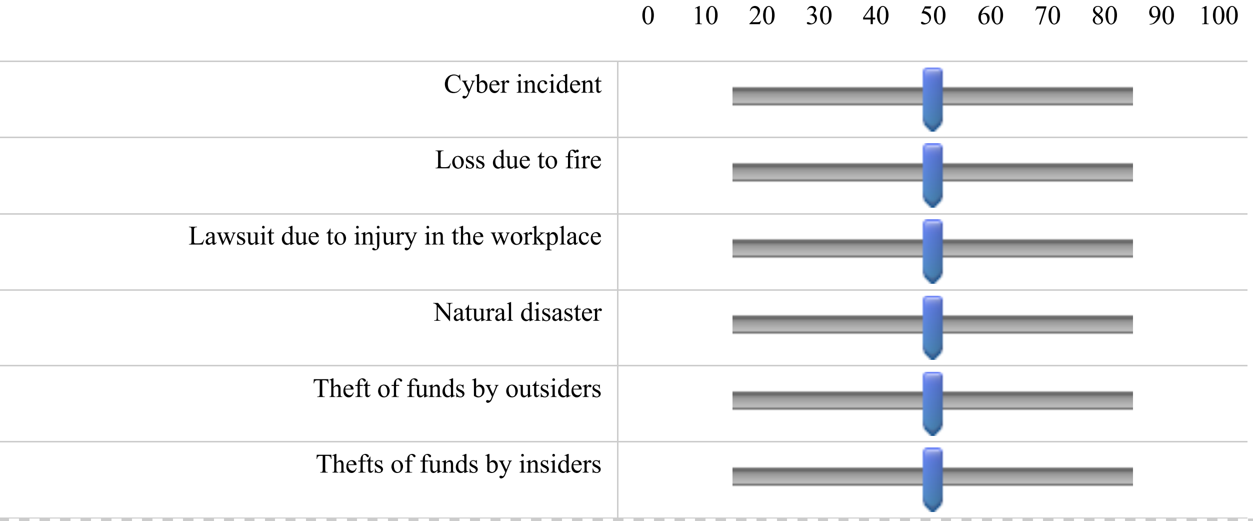
Curtis T. Hill, Jr.
Indiana Attorney General Co-Chair of the Legal and Insurance working group of the Indiana Executive Cybersecurity Council

I agree to participate in the survey
I do not agree to participate in the survey

Q1.2 How concerned is your organization about the risk of a cyber incident?
Not at all concerned
Somewhat concerned
Very concerned

Q1.3 Does your organization currently have an insurance policy that provides coverage for any of these events? (Select any that apply)
Cyber incident
Loss due to fire
Lawsuit due to injury in the workplace
Natural disaster
Theft of funds by outsider
Theft of funds by insider
Not sure

Q1.4 How likely do you think it is that the following events will impact your organization?
(0 being very unlikely, 100 being very likely)



0 10 20 30 40 50 60 70 80 90 100

Cyber incident

Loss due to fire

Lawsuit due to injury in the workplace

Natural disaster

Theft of funds by outsiders

Thefts of funds by insiders

Carry Forward All Choices - Displayed & Hidden from "How likely do you think it is that the following events will impact your organization? (0 being very unlikely, 100 being very likely)"

Q1.5 How much harm do you think your organization would face if each of the following events occurred? (0 being very little harm, 100 being a great deal of harm)

	0 10 20 30 40 50 60 70 80 90 100
Cyber incident	
Loss due to fire	
Lawsuit due to injury in the workplace	
Natural disaster	
Theft of funds by outsiders	
Thefts of funds by insiders	

Q1.6 What types of cyber incidents is your organization concerned about? (Select any that apply)

Ransomware (e.g., extortion)
Phishing (e.g., targeting key personnel through cyber-enabled means)
Insider attack (e.g., an employee selling access or secrets)
Malware (e.g., malicious software)
Wire/financial fraud (e.g., theft of money through electronic means)
Password attacks (e.g., someone else breaking your passwords)
Denial of service attacks (e.g., someone making it impossible for users to access your website)
Other (Please describe) ____

Carry Forward Selected Choices from "What types of cyber incidents is your organization concerned about? (Select any that apply)"

Q1.7 Please rank the potential types of cyber incidents you identified from most concerning to least concerning.

Ransomware (e.g., extortion)
Phishing (e.g., targeting key personnel through cyber-enabled means)
Insider attack (e.g., an employee selling access or secrets)
Malware (e.g., malicious software)
Wire/financial fraud (e.g., theft of money through electronic means)
Password attacks (e.g., someone else breaking your passwords)
Denial of service attacks (e.g., someone making it impossible for users to access your website)
Other (Please describe)

Q1.8 What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)

Data or information being exposed to outsiders
Data or information being deleted or lost
Disinformation about your organization being spread
Identity theft
Wire/financial fraud
Website or system downtime
Other (Please describe) ____

Carry Forward Selected Choices from "What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)"

X→

Q1.9 Please rank the potential consequences of cyber incidents you identified from most concerning to least concerning.

Data or information being exposed to outsiders
Data or information being deleted or lost
Disinformation about your organization being spread
Identity theft
Wire/financial fraud
Website or system downtime
Other (Please describe)

End of Block: Cyber Risk Perceptions

Start of Block: Cyber Risk Management and Planning

Q2.1 To your knowledge, has your organization experienced a successful cyber incident in the past three years?

Yes
No
Not sure or can't say

Q2.2 How many cyber incidents resulting in data theft did your organization experience in the last three years?

None
1-5
6-10
11-50
51-100
More than 100
Not sure or can't say

Display This Question:
If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.3 Please think back to the most severe cyber incident resulting in data theft experienced by your organization in the last three years. When did the cyber incident occur?

Month ____
Year ____

Display This Question:
If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.4 What type of cyber incident did your organization experience?

Ransomware
Phishing
Insider attack
Malware
Password attacks
Denial of service attacks
Wire/financial fraud
Other (Please describe) ____
Not sure

Display This Question:

If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.5 What were the consequences of the cyber incident experienced by your organization?

No consequences occurred
Data or information being exposed to outsiders
Data or information being deleted or lost
Disinformation about your organization being spread
Identity theft
Wire/financial fraud
Payment for credit monitoring services
Website or system downtime
Disruption of operations
Other (Please describe) ____
Not sure

Q2.6 Has your organization taken any steps to prevent potential cyber incidents?

Yes
No
Not sure

Display This Question:

If Has your organization taken any steps to prevent potential cyber incidents? = Yes

Q2.7 What steps has your organization taken? (Select all that apply)

Installed antivirus software
Trained employees to spot potential cyber risks
Invested in cyber risk insurance
Limited physical access to computer systems
Required employees to regularly change passwords
Update and patch software regularly
Other (Please describe) ____

Display This Question:
If Has your organization taken any steps to prevent potential cyber incidents? = No

Q2.8 Why hasn't your organization taken steps to prevent potential cyber incidents? (Select all that apply)

Too expensive
Too difficult
Not sure what to do
Prefer to spend resources on other priorities
Options for preventing cyber incidents are ineffective
Don't believe our organization is at risk
Other (Please describe) ____
Not sure

Q2.9 Has your organization taken any steps to mitigate potential cyber incidents?

Yes
No
Not sure

Display This Question:
If Has your organization taken any steps to mitigate potential cyber incidents? = Yes

Q2.10 What steps has your organization taken? (Select all that apply)

Installed automatic back-up systems
Encrypted data
Purchased cyber risk insurance
Utilized cloud computing
Other (Please describe) ____

Display This Question:
If Has your organization taken any steps to mitigate potential cyber incidents? = No

Q2.11 Why hasn't your organization taken steps to mitigate potential cyber incidents?

Too expensive
Too difficult
Not sure what to do
Prefer to spend resources on other priorities
Don't believe our organization is at risk
Other (Please describe) ____
Not sure

Q2.12
Does your organization use any of the following tools to proactively manage the cyber threats facing your organization? (Select all that apply)

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

Q2.13 Did your organization refer to any externally developed cyber tools, frameworks, or controls in making decisions about cyber practices?

Yes
No
Not sure

Skip To: Q2.15 If Did your organization refer to any externally developed cyber tools, frameworks, or controls in m... != Yes

Q2.14 If so, which? (Select all that apply)

NIST Cybersecurity Framework
ISA
ISME
NISTIR 7621 Measure
ISO 15408
ISO 27001-02
ETSI
Center for Internet Security (CIS) Critical Security Controls
SP 800-53 R4 Controls
Australia Top 35 Controls
Other (Please specify) ____

Q2.15 To your knowledge, has your organization provided anyone with training intended to raise awareness of the potential for cyber threats like hacking, phishing, spamming, or other threats related to stealing or compromising digital?

Yes
No
Not sure

Q2.16 Did you receive training in a formal setting offered by your organization?

Yes
No
Not Sure

Skip To: Q2.18 If Did you receive training in a formal setting offered by your organization? != Yes

Q2.17 How often have you attended trainings designed to improve your awareness of cyber threats?

Once a quarter
Once a year
Every few years
I have attended only one training

Q2.18 Have others in your organization received training in a formal setting offered by your organization?

Yes
No
Not sure

Q2.19 Who in your organization is ultimately responsible for managing cyber risks?

CEO
Board of Directors Committee
Chief Information Security Officers (CISO)
Chief Information Officer (CIO)
Chief Privacy Officer (CPO)
Chief Information Governance Officer (CIGO)
Other (Please specify) ____
Not sure

Q2.20 How many cybersecurity professionals are currently employed at your organization?

None
1-5
6-10
11+

Q2.21 Does your organization have written documentation related to cyber incident planning and response?

Yes
No
Not sure

Skip To: Q2.23 If Does your organization have written documentation related to cyber incident planning and response? != Yes

Q2.22 How strongly would you agree or disagree with the following statements about your organization's cybersecurity documentation?

Strongly agree | Somewhat agree | Neither agree nor disagree | Somewhat disagree | Strongly disagree

0 10 20 30 40 50 60 70 80 90 100

It lays out a detailed game plan for how our organization will respond to a range of cyber incidents
It has been widely shared within our organization
It is regularly vetted and updated in response to industry trends
It is regularly vetted and updated in response to technological developments

Q2.23 Which, if any, of the following practices does your organization currently employ? (Select all that apply)

- Multi-factor authentication
- End-to-end encryption
- Remote backups
- Automatic updating of operating systems and software
- Traffic flow analysis
- Third-party penetration testing
- Policy on "Bring Your Own Device" (BYOD)
- Regular checks for vendors and partners
- Others (Please describe) ____
- None of the above
- Not sure or can't say

Q2.24 Does your organization currently have insurance specifically tailored to cover cyber incidents?

- Yes
- No
- Not sure

End of Block: Cyber Risk Management and Planning

Start of Block: Cyber Risk Insurance Use

Q3.1 When did your organization obtain a cyber risk insurance policy?

- Year ____
- Month ____

Q3.2 Why did your organization get a cyber risk insurance policy? (Select all that apply)

- Response to an incident at our organization
- Response to an incident at a peer organization
- News reports about cyber incidents
- Other (Please describe) ____
- Not sure

Q3.3 Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)

- Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Credit monitoring services
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Losses arising from stolen funds or products
- Damage to computer or information systems (including cost of restoring lost data)
- Damages related to lost intellectual property
- Forensic investigation of the breach
- Standing up a call center and response team
- Other (Please describe) ____
- None of the above
- Not sure

Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = None of the above
Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = Not sure

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

Q3.4 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 cyber breach (such as hiring a firm to secure systems)
Cost of notifying affected customers or others whose data was exposed in a breach
Credit monitoring services
Fines/penalties related to the data breach
Business interruptions related to denial of service or other downtime
Losses resulting from exposure or use of confidential business information
Losses arising from stolen funds or products
Damage to computer or information systems (including cost of restoring lost data)
Damages related to lost intellectual property
Forensic investigation of the breach
Standing up a call center and response team
Other (Please describe)
None of the above
Not sure

Q3.5 Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe) ____
None of the above
Not sure

Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = None of the above
Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = Not sure

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

Q3.6 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 for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe)
None of the above
Not sure

Q3.7 Does your cyber risk insurance policy require your organization to undertake certain security measures?

Yes
No
Not sure

Skip To: Q3.9 If Does your cyber risk insurance policy require your organization to undertake certain security mea... != Yes

🔀

Q3.8 What security measures are required by your cyber risk insurance policy? (Select all that apply)

Mandatory, automatic patching
End-to-end data encryption
Employee training & cyber hygiene
Regular third party penetration testing
Other (please list) ____
None of the above
Not sure

Q3.9 Does your cyber risk insurance policy have a limit?

Yes
No
Not sure

Skip To: Q3.11 If Does your cyber risk insurance policy have a limit? != Yes

Q3.10 What is the limit?

____

Q3.11 Does your cyber risk insurance policy exclude coverage in certain circumstances?

Yes
No
Not sure

Skip To: Q3.13 If Does your cyber risk insurance policy exclude coverage in certain circumstances? != Yes

Q3.12 Under what circumstances would your cyber risk insurance policy exclude coverage (Select all that apply)
Act of war/terrorism
Internet of Things-related breach
Losses from unencrypted devices
Contractual liability
Criminal or fraudulent acts
Losses related to unauthorized collection of customer data
Losses that occurred because your organization failed to provide and maintain adequate security
Other (Please describe) ____
None of the above

Q3.13 Is your policy retroactive to cover losses that occurred (in whole or in part) before its start date?
Yes
No
Not sure

Q3.14 Does your company require subcontractors to have cyber risk insurance?
Yes
No
Not sure

Skip To: End of Block If Does your company require subcontractors to have cyber risk insurance? != Yes

Q3.15 What losses must be covered under a subcontractor's cyber risk insurance policy?
Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems)
Cost of notifying affected customers or others whose data was exposed in a breach
Fines/penalties related to the data breach
Business interruptions related to denial of service or other downtime
Losses resulting from exposure or use of confidential business information
Not sure

End of Block: Cyber Risk Insurance Use

Start of Block: Cyber Risk Insurance Non-Use

Q4.1 Has your company ever had a cyber risk insurance policy?
Yes
No
Not sure

Skip To: Q4.6 If Has your company ever had a cyber risk insurance policy? != Yes

Q4.2 During what period did your company have a cyber risk insurance policy?
Date cyber risk insurance coverage began ____
Date cyber risk insurance coverage ended ____

Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)"

Q4.3 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 cyber breach (such as hiring a firm to secure systems)
Cost of notifying affected customers or others whose data was exposed in a breach
Credit monitoring services
Fines/penalties related to the data breach
Business interruptions related to denial of service or other downtime
Losses resulting from exposure or use of confidential business information
Losses arising from stolen funds or products
Damage to computer or information systems (including cost of restoring lost data)
Damages related to lost intellectual property
Forensic investigation of the breach
Standing up a call center and response team
Other (Please describe) ____
None of the above
Not sure

Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)"

Q4.4 Which (if any) losses to others (third-party losses) were covered under this policy?

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe) ____
None of the above
Not sure

Q4.5 Why did you discontinue your former cyber risk insurance policy? (Select all that apply)

Too expensive
Couldn't get a policy
Covered under other insurance policies
Prefer to spend resources on other priorities
Options for preventing cybersecurity incidents are ineffective
Don't believe our organization is at risk
Other (Please describe) ____
Not sure

Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Couldn't get a policy
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Covered under other insurance policies
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Prefer to spend resources on other priorities
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Options for preventing cybersecurity incidents are ineffective

Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Don't believe our organization is at risk
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Other (Please describe)
Skip To: Q4.6 If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Not sure

Q4.6 Has your company ever considered obtaining a cyber risk insurance policy?
Yes
No
Not sure

Skip To: Q4.8 If Has your company ever considered obtaining a cyber risk insurance policy? != Yes

Q4.7 Why did your company decide not to obtain a cyber risk insurance policy? (Select all that apply)
Too expensive
Difficult to obtain
Covered under other insurance policies
Prefer to spend resources on other priorities
Options for preventing cybersecurity incidents are ineffective
Don't believe our organization is at risk
Other (Please describe) ____

Q4.8 What would encourage your company to obtain a cyber risk insurance policy?
____
____
____
____
____

End of Block: Cyber Risk Insurance Non-Use

Start of Block: Organization and Respondent

Q5.1 What is your job title?
____

Q5.2 How many employees does your organization have?
1-10 employees
11-50 employees
51-250 employees
More than 250 employees

Q65 Does your organization fall within one of the following critical infrastructure sectors?

Chemical Sector
Commercial Facilities Sector
Communications Sector
Critical Manufacturing Sector
Dams Sector
Defense Industrial Base Sector
Emergency Services Sector
Energy Sector
Financial Services Sector
Food and Agriculture Sector
Government Facilities Sector
Healthcare and Public Health Sector
Information Technology Sector
Nuclear Reactors, Materials, and Waste Sector
Transportation Systems Sector
Water and Wastewater Systems Sector
No, my organization does not fall within a critical infrastructure sector
Prefer not to say

Skip To: Q5.4 If Does your organization fall within one of the following critical infrastructure sectors? != No, my organization does not fall within a critical infrastructure sector

Q5.3 What sector is your organization in?

Accommodation and Food Services
Administrative and Support Services
Agriculture, Forestry, Fishing, and Hunting
Arts, Entertainment, and Recreation
Construction
Educational Services
Finance and Insurance
Government
Health Care and Social Assistance
Manufacturing
Mining
Other Services
Professional, Scientific, and Technical Services
Real Estate, Rental, and Leasing
Retail Trade
Transportation and Warehousing
Utilities
Wholesale Trade
Other (Please specify) ____

Q5.4 Which of the following types of information about individuals does your organization handle? (Select all that apply)

Personally identifiable information (e.g., home addresses, email addresses, social security numbers)
Personal financial information (e.g., credit card numbers, banking information, credit scores)
Personal health information (e.g., allergies, past medications)
Other (Please describe) ____
We do not collect any personal data

Q5.5 How would you describe the geographic scope of your organization?

Local (e.g., city or county)
State
Regional (e.g., more than one state)
National
Multi-national
Does not apply

Q5.6 Would you be willing to participate in a follow-up interview to further explore how your company is managing cyber risk?

Yes
No

Display This Question:

If Would you be willing to participate in a follow-up interview to further explore how your company... = Yes

Q5.7 Thank you for your willingness to participate in a follow up interview. Please provide your name, affiliation, and email for contact purposes only.

____

End of Block: Organization and Respondent