CRA | Business Intelligence

Cybersecurity Risk: *A Top Issue in the Boardroom*

FINDINGS FROM AN OCTOBER 2021 RESEARCH STUDY

Sponsored by

RECIPROCITY®

Cybersecurity Risk: A Top Issue in the Boardroom

FINDINGS FROM AN OCTOBER 2021 RESEARCH STUDY

BACKGROUND

With data breaches, ransomware attacks and other security risks dominating news cycles in recent years, corporate boards of directors are paying attention to cybersecurity and risk in ways unheard of a decade ago. They increasingly understand that this is now their problem rather than simply being another technical security staff concern. Board members have come to realize the need to integrate traditional, distinct management activities into a cohesive set of policies and procedures that increase the effectiveness of people, business processes, technology, and facilities.

The governance, risk and compliance (GRC) discipline can achieve this by breaking down the traditional barriers between business units, requiring that they work in a collaborative fashion to achieve the company's strategic goals. If properly implemented, GRC policies, practices, and software can reduce security risks and increase operational efficiency. If improperly implemented or if senior management support is minimal, the potential for security failure increases.

"We know, from our own customer base, that companies are struggling to not only see risk and understand the impact to their business, but to communicate it out in a way that other parts of the organization can really understand the impact."

–Michael Geller, COO at Reciprocity

METHODOLOGY

The data and insights in this report are based on an online survey conducted in October 2021 by CyberRisk Alliance among 252 senior-level executives (manager titles and above) in IT, cybersecurity and governance, risk, and compliance roles employed at mid-size to large organizations (250 to 5,000 employees) in the United States. Respondents were employed in a variety of industries focusing on IT services/software, manufacturing, financial services, banking, and professional services. The study was underwritten by Reciprocity.

Survey objectives included identifying organizations' prioritized cybersecurity strategies, tactics, and focus areas in mitigating risk, including their concerns about governance, risk management, compliance, audit, and related fields. Respondents answered structured survey questions as well as various open-ended questions.

EXECUTIVE SUMMARY

According to survey respondents, board priorities increasingly include identifying, monitoring, and mitigating risk.

Risk management has risen significantly on the board of directors' radar from a checklist item to ensure the company meets compliance requirements to one of the many pillars required to ensure a corporation can manage security risk. That importance has been made plain by a significant escalation of ransomware and other attacks in the past year, including those that have led to real-world consequences, like the Colonial Pipeline attack in May that ground operations to a halt and left people scrambling to fuel their vehicles.

Boards also increasingly understand that security challenges to solve include finding qualified staff and training employees.

Corporate investments are increasingly devoted to GRC, audits, and ways to realign the strategies of technical staff, CIOs and CISOs with the boards' business imperatives. Increasingly, companies are bringing in external auditors because they are considered more credible than audits conducted in house. There's also a growing push to invest in the human element of security to balance out investments in technology. Part of this realignment is implementing a security framework, such as the one developed by the National Institute of Standards and Technology (NIST), as well as developing more effective auditing policies and procedures, to clearly identify the ROI of cybersecurity.

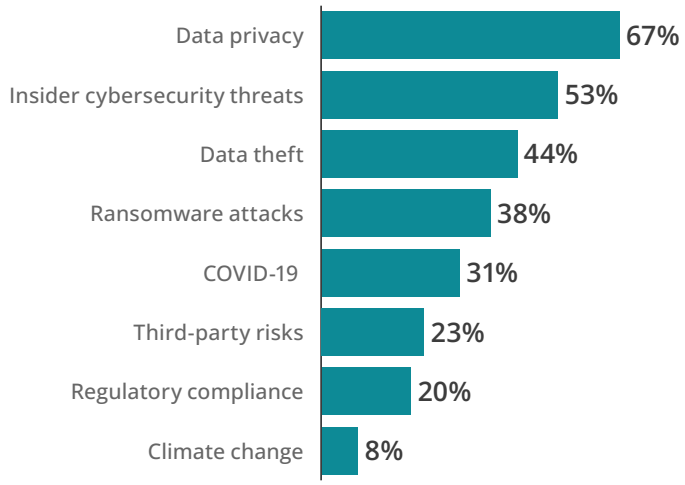
Developing a more effective and efficient risk management operation and integrating it with the audit and compliance operations within the corporate hierarchy has become a business imperative for mid-size and large organizations. The COVID-19 pandemic created a plethora of new risk management vulnerabilities that became huge targets for criminal and state-sponsored entities who armed themselves with the latest versions of ransomware and ransomware-as-a-service.

This survey identified several areas that might well drive decision making to address corporate risk-related issues for the foreseeable future. Some of these findings hint at a change in North American corporate executives' view of whether they should take a reactive or proactive approach to cybersecurity.

In recent years, U.S.-based companies tended to be more reactive (respond and recover) than proactive (identify, protect, and detect) based on the NIST cybersecurity framework. Among the key findings of this study:

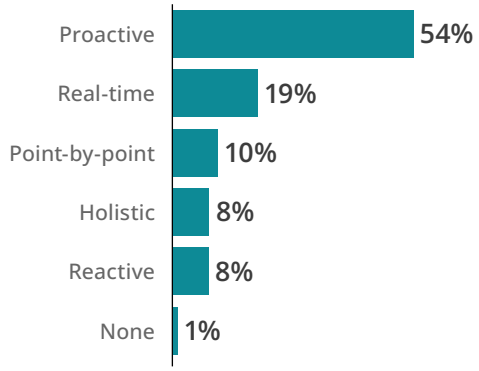
- More than half of all respondents (54%) said they have a proactive risk management approach, but fewer than 20% of all respondents claimed that they have a real-time approach. Financial and professional services respondents were the most likely to use frameworks and other best practices.
- Continuous risk monitoring, improving risk identification, and aligning risk to business objectives — a key requirement of many boards of directors — are top objectives for investing in GRC software.
- Top risks to organizations include data privacy (67%), insider threats (53%), data theft (44%), and ransomware (38%). The shifts created by the pandemic accounted for 31% of the risk.
- At least half of all respondents say that improving their risk program and training for employees and IT staff are top challenges.

Top Risks to Organizations



According to a chief technology officer from the manufacturing sector, "A successful, external cybersecurity compliance audit has to be a proactive step or method that sees risk, analyzes the level of the risk towards the organization, and offers a solution to it."

Risk Management Approaches

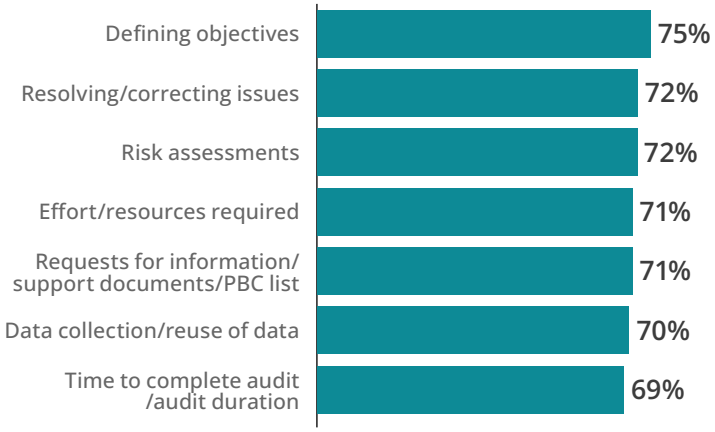


EXTERNAL AUDITS MORE CREDIBLE AND LESS BIASED

Not surprisingly, some 83% of respondents said their organizations conduct external cybersecurity compliance audits, begging the question if the other companies are doing self-attestation audits or simply not doing audits at all. Self-attestation is considered acceptable for many compliance requirements but leaves open the question of accuracy when a third-party auditor or certified public accountant is not certifying the audit.

Effectiveness of Managing External Audit

Respondents indicating "Mostly Effective" or "Very Effective"



There are two other key reasons why a company is often required to use outside experts to conduct audits. When a company is breached, it is highly advised that an outside forensics team be brought in to conduct the investigation. This is often required by cyber insurance carriers. If the breach was caused by an insider, regardless of whether that insider is an employee, contractor, or service provider who has access to network-attached devices, the insider should never be part of the investigative team. Outside forensics investigators reduce the possibility of a malicious insider corrupting the investigation to protect themselves or a co-conspirator.

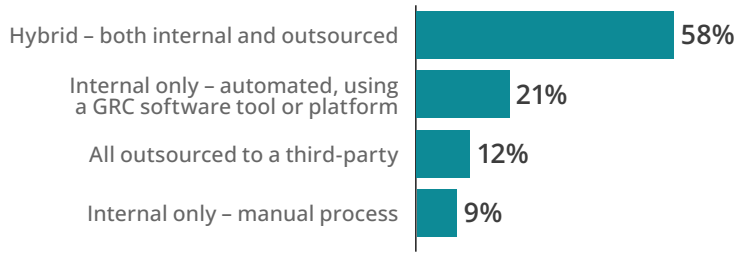
Additionally, insiders often either overlook potential threats because of over-familiarity with the network or because they decide to ignore a potential threat due to personal or internal political reasons.

An example of the latter situation is overlooking a potential threat because the individual involved might be the investigator's supervisor, a corporate executive, or perhaps a friend or colleague. Pointing a finger at someone within the organization could cause the employee doing the investigation to lose their job or a friend, regardless of whether the suspect did the deed or not.

Using external investigators and auditors eliminates any of these issues because the outsiders have no vested interest in the internal politics, nor do they necessarily know the players involved. A disinterested third party ideally brings clarity without bias to audits and investigations.

Although enterprises still need to ensure they are secure, today's security teams must deal with the wild card that reared its head in 2020 due to the pandemic — the massive increase of remote workers. One IT director from the banking sector called out this emerging security vulnerability trend, noting, "We know there are high-risk practices, especially [among] our growing remote workforce."

Risk Management Solutions



While external audits are the norm in incident response situations, a strong internal audit team is essentially part of the overall governance component of GRC. While 58% of respondents said they use a hybrid approach of internal and outsourced security management, nearly a quarter (21%), use GRC software.

A successful audit provides the technical staff with a roadmap to improve cybersecurity and reduce risk.

"I want there to be clear objectives and I want certain questions answered," said the CISO at a financial services firm. "Are there weak spots? Are there extraneous tools that don't perform a useful function? Are we equipped to handle security threats? It's also helpful to see if we remain in compliance with data security laws."

A senior vice president in the manufacturing sector noted, "Conducting network security audits is a good way to ensure your business controls and policies [are sufficient] to ensure data security and manage risks." A chief technology officer in the banking sector expressed similar thoughts: "We managed to get our security issue fixed mostly by getting new technologies and better cybersecurity audits."

A telecom industry engineering executive stresses that security audits need to address all mobile devices that connect to the corporate network. This will provide auditors with evidence if remote devices are trying to access the corporate networks inappropriately.

When asked how the respondents would define a successful external cybersecurity compliance audit, one manufacturing consultant took a pragmatic approach: "A successful compliance [audit] would include finding the external problem and getting rid of it." A lead engineer at another manufacturing firm focused on an external audit, describing it as "a completely hands-off and successful evaluation of our systems, with suggestions for improvement."

Perfection is not required for a successful audit. The CEO of an IT services firm offered his description of a successful audit, noting,

"Our company has some challenges when it comes down to managing our external cybersecurity, but we work together [with our auditors] to come up with many ideas to overcome those challenges."

Survey results clearly demonstrated that companies are actively moving to shore up their risk management with 89% indicating they are very likely to or have already adopted or added a new risk framework, such as the one developed by NIST. Some 91% said they are very likely to or have already hired additional IT security staff, while 83% said they are very likely to or have already outsourced cybersecurity risk management to an outside firm. Another 87% said they are very likely to or already have made the purchase of a GRC tool or platform. The respondents plainly see a need to shore up their security and recognize that security is not only a technology issue but also effects the board room and senior management.

Likelihood to Improve Risk Management

Respondents indicating "Already Have" or "Likely"

Even though ransomware attacks have increased in both scope and the cost of the attacks, as well as an increase in third-party breaches, companies continue to believe that they have good visibility into the risk exposure to their business. Some 78% of respondents say they have very good or excellent visibility into their networks.

This belies an FBI warning in July 2020 that cyberattacks are becoming more intense, frequent, and dangerous. Dallas FBI Special Agent in Charge Matthew DeSarno said, "Our statistics aren't complete because we just flat out don't know how many companies have been hit. Many companies are attacked and may have paid the ransom and never report it at all."

DeSarno spoke following the July 4 weekend when some 40,000 companies on five continents were warned that they might have been victims of the Russian-based REvil gang that hit Kaseya.

COMBINING TECHNOLOGY WITH HUMAN OVERSIGHT

Although cybersecurity is generally considered a technology issue, the reality is that it is about much more. It is a business imperative for the board of directors as well. From a technical perspective, the CISO and CIO address the transactional aspects of cybersecurity, such as creating stronger defenses to fight against ransomware and other malware attacks, endpoint detection and response, and cloud-based attacks.

Concurrently, corporate general counsels, chief risk officers, chief compliance officers, chief financial officers, and CEOs are all focusing on ensuring business continuity, maintaining corporate valuation, ensuring the company is compliant with laws and regulations, and, in general, ensuring their attention is on the goals and directives from the board

of directors. Developing cybersecurity strategies, particularly those addressing risk and compliance, require not only input from the technical teams but generally require a champion from the C-suite to garner buy-in from the board of directors.

Having a human analyst in a security operations center reviewing such anomalous behavior could have led to the potential attack being identified before it reached the network. Although fully automated systems are desirable, companies should not reject out-of-hand having human oversight.

"Keep your organization's approach to network security and risk management relevant and up-to-date," stressed an IT security administrator in the telecom/communications industry. The administrator noted that the technical staffs are "not just cybersecurity experts; we are experienced business and risk experts," believing they have the business acumen to optimize systems to drive growth and understand both business strategy and management. Having technologists that can speak the language of the board of directors — profit and loss plus business operations — is a rare commodity.

Although many companies develop security services internally to manage third-party risk, not all can meet the growing requirements. One senior vice president at an IT services company said that his firm outsources threat intelligence, risk management, and compliance. Companies need to understand their strengths and weaknesses; outsourcing essential business operations when necessary is a common-sense approach rather than gambling that internal staff without that expertise can lock down all of the vulnerabilities.

Although automated systems are high on the list of preferred options across the board, these systems are not foolproof. Artificial intelligence-based systems still need to be trained to eliminate false positives, and fully automated systems can be tricked into creating potential vulnerabilities.

For example, in corporate networks that have both Intel/Windows- and Apple-based systems, holes have been reported in identity and access management systems.

News reports over the years found that some networks that had separate IAM systems for each of the platforms had vulnerabilities when the IAM software for one platform assumed the other would catch anomalies it did not recognize. However, there was no human oversight to ensure that the second IAM system was able to identify and manage

the vulnerability. As a result, attackers were able to breach networks where the attack was ignored by both automated IAM systems.

GROWING LIABILITY SPURS BOARDROOM FOCUS

Meanwhile, new laws are holding board members personally liable for cybersecurity breaches. This includes the elimination of force majeure, the common contractual protection often used to indicate that an event could not be anticipated. Some courts are now ruling that because companies are buying cyber insurance, the board must consider a data breach as a possibility, and thus force majeure as a protection no longer applies.

To overcome the barriers to mitigating risk, companies must negotiate the proverbial minefield of challenges posed by increased risk. Without the right tools and training, it is possible for vulnerabilities to pass unidentified, as has been the case in many recent major breaches.

An IT director in the financial services sector underscored the importance of getting policies and procedures in place to defend against data breaches. He suggested that enterprises "centralize your cybersecurity policies. It acts as a checklist for policies and procedures. Being able to ensure proper security mechanisms are in place while also making sure they comply with relevant regulations," is essential.

LOOKING AHEAD

Seven of 10 respondents are likely to change their risk management strategies, hire additional IT staff, implement continuous auditing and add new frameworks during 2022, the survey revealed.

Underscoring the importance of a hybrid security environment, a financial services director of IT said that the senior leadership at his firm "realizes the importance of cyber security as more of our employees are working in a hybrid environment. So, they are quite supportive when we ask for an increased budget, especially in the current hybrid working environment."

A senior director of IT at a telecom firm said his company's goal going forward is protecting its reputation, a common casualty from a breach or ransomware attack. "When it comes to reputation, we have to be strategic. Frequent cyber-attacks tarnish the business' reputation and put it at risk of losing clients to competitors. A software industry CISO said risks from ransomware and other attacks, including regular attacks on the company's database by hackers, are likely to require an increase in the cybersecurity budget for 2022.

CONCLUSION

Governance, risk management, compliance, and audit are the cornerstones today for companies building defenses against cyber attackers employing massive ransomware attacks. Solid cyber hygiene, combined with proactive risk assessments and mitigation of identified risks, and augmented by proactive third-party risk management, works to insulate enterprises from many of the most common and aggressive forms of attacks.

While no organization can be completely protected 100% of the time — a single, accidental click could result in a data breach — companies that have aggressive defenses stand the best chance to defend against all but the most pernicious attackers.

Enterprises need to address such primary concerns as insider threats, data theft, ransomware, third-party risk, and worsening risk volatility.

Companies identified they have specific needs relating to risk. These needs include:

- Continuous risk monitoring, risk identification, and risk alignment to business that focus on GRC
- Improved time to complete audit process and data collection/reuse of data in external audits
- Addressing the high-risk practices of remote workforces and recommendations for new policies, procedures and processes to reduce the organization's risk profile

Respondents indicated they need support for their organizations' requirements for information in the budget and spending approval process. In many cases, increased budgets, and spending in 2022 are contingent on presenting proof of the ROI to the board of directors and executive leadership (including the potential for increased ROI by hiring a third party), which includes in-depth reports and analyses, including documented cases, breach intents and recent examples.

This ROI can be used to demonstrate to the board that investments in cybersecurity ultimately meet the business imperative while supporting the ability to obtain cyber insurance.

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, *Security Weekly*, *InfoSec World*, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at ***http://cyberriskalliance.com/***.

ABOUT RECIPROCITY

Reciprocity equips organizations with the fastest, easiest and most prescriptive information security solutions in the market. Our fully integrated and automated ZenGRC platform powers a full catalog of compliance, risk and other infosec applications. Supported by our award-winning customer service and industry-leading GRC expert teams, we help businesses realize the industry's fastest time to value while fostering in-house expertise. More information is available at ***https://reciprocity.com/***.

