Risk Cooperative

2022 360° CYBER RISK SURVEY

CONTENTS

METHODOLOGY

The 360° Cyber Risk Survey, conducted by Risk Cooperative, was designed to evaluate the collective state of readiness amongst middle-market organizations across a range of industry verticals. The questions were meant to align with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Specifically, the survey categories were developed from the referenced NIST Framework Core functions:

Identify | Protect | Detect | Respond | Recover

The 360° Cyber Risk Survey was conducted online by independent participants. The survey findings were closely scrutinized and rounded to the nearest tenth percentage point. In some cases, respondents were given the option to select all applicable responses and statistics from those questions are noted accordingly.

INTRODUCTION

The cyber risk landscape has changed significantly since the initial 360° Cyber Risk Survey was conducted—both in the frequency of cyber attacks and their complexity. Today, organizations are more intentioinal about cybersecurity and the necessary investment required with regards to their Information Technology (IT) strategy than in previous years. However, the budget allocation and focus of cybersecurity spending continues to vary greatly by industry and company size. Local COVID 19 responses and a rise in teleworking arrangements have also factored into cybersecurity decision-making. As the survey report will highlight, there remain critical actions that are still not being prioritized by organizations across the board.

Additionally, while the data shows organizations of all sizes appear to understand the very real threat a cyber attack represents to their business, many continue to struggle with how to quantify the investment into such an intangible—yet costly—initiative. Larger companies make large-scale investments to increase their cybersecurity defenses at similar rates to our initial survey, while middle-market and small businesses often cannot afford such robust cybersecurity measures, and have become an increasingly attractive target for cyber criminals.

As ransomware and other disruptive attacks continue to grow amongst small- to mid-sized organizations, this critical group must focus on the most effective and cost-efficient mitigation tools. This latest 360° Cyber Risk Survey report will provide the most current benchmarked data, informed analysis, and actionable best practices to help middle-market organizations, senior leaders, and boards of directors obtain a better understanding of the operational and financial impacts of cyber risks. Learning best practices being implemented by industry peers, plus general trends within the cyber risk landscape, will give organizations a roadmap to build better operational resiliency.

A successful cybersecurity and mitigation strategy requires a multi-pronged approach, leveraging technology, education, and financial risk transfer programs. Enterprise-wide risk assessments and mitigation strategies are important tools in this journey, requiring stakeholder engagement from the board-level down to frontline staff members. With cyber risks continuing to evolve, building greater agility and resiliency is imperative to stay ahead of the threat.

01

ORGANIZATIONAL BACKGROUND

This section covers the industries represented by the respondent organizations, applicable standards and regulations, plus respondent roles and responsibilities relative to their organization's cyber operations.

OVERVIEW

Survey respondents represented a cross section of public and private sectors. The majority of respondents (19.1%) were in the healthcare space, followed by non-profit (14.7%), financial services (13.2%), professional services (11.8%) and technology (10.3%). Compared to prior years (when government contractors (33.9% and professional services (19,.6%) represented more than half of respondents), this spread represents a greater distribution across industries, while unsurprisingly still concentrated on segments more "at risk" for potential cyber attacks.

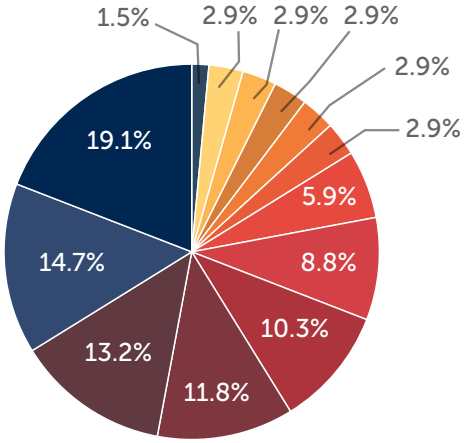


Figure 1 | Survey Respondent Industries

- Automotive
- Construction
- Energy
- Real Estate
- Infrastructure & Logistics
- Public Sector
- Education
- Technology
- Professional Services
- Financial Services
- Non-Profit
- Health Care
- Government Contractors

SURVEY INSIGHTS

47.0%

Of survey respondents had more than 50% of cybersecurity preparedness activities included within their operational responsibilities.

ACCOUNTABILITY & COORDINATION

Cyber risks have enterprise-wide impacts. Therefore, the success of a cybersecurity program is highly dependent upon a supported organizational structure where leaders are clearly assigned and held accountable. In organizations with successful cybersecurity programs, coordination is encouraged and achieved to optimize outcomes.

36.4%

Of the respondents reported that overall accountability for cybersecurity initiatives was held by the Chief Information Security Officer (CISO).

24.2%

Followed by the Chief Executive Officer (CEO), marking a significant shift from prior years where the CEO was solely responsible, indicating a maturity in cybersecurity frameworks and prioritization.

13.6%

The third highest response was the Board of Directors, another indication of how seriously organizations are now taking cyber risk.

While overall cybersecurity oversight remains primarily with the CISO and CEO, the trend toward Board of Directors involvement is encouraging. As will all complex risks, successfully mitigating cyber risk requires close interaction across department leads, including in Legal and Human Resources departments. For some larger organizations, a General Counsel or legal support may be in-house, but smaller organizations may require support from outside counsel.

Coordination with the legal team remains critical, especially with regards to third party vendor requirements, determining liability for incidents and complying with regulations such as breach notification legislation. 50.8% of respondents said that their legal and IT departments coordinate with the security group on cyber risk management initiatives. 14.9% of respondents said that coordination between these groups was unknown, a significant uptick from prior year responses. Coordination protocols should be established and understood by all involved parties.

CLOUD SERVICES

Cloud services continue to be a growing trend for data storage amongst survey respondents. Advantages of migrating to cloud services can include decreased acquisition and maintenance costs, more efficient uses of personnel, increased time availability, and greater accessibility.

TOP CLOUD SERVICES UTILIZED BY RESPONDENTS INCLUDE

50.8%
Software as a Service (SaaS)

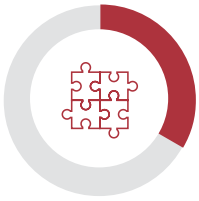
33.9%
Infrastructure as a Service (IaaS)

29.2%
Platform as a Service (PaaS)

TOP BUSINESS FUNCTIONS MANAGED IN THE CLOUD INCLUDE

*Respondents were able to select multiple departments that applied to their organizations.

54.6%
IT



33.3%
Core Business Services

42.4%
Human Resources

33.3%
Accounting/Finance

Leveraging a cloud based platform or service provider for these business functions has numerous benefits to an organization, especially with the increased prevalence of tele- and remote-working environments. However, these platforms also create additional vulnerabilities and potential risks the organization must take into consideration. It is a common misconception that cloud service providers assume total responsibility for risks, including cyber breaches, which is not always the case. Ultimately, risk management should still be managed by the organization.

Indeed, third party vendors have become a growing area of cyber vulnerability. A robust vendor risk management program should be established to thoroughly vet providers, require minimum security controls (where applicable), monitor compliance with contract agreements, and determine residual risks and controls within the purview of the organization. These vendor risk management activities should feed into the overall IT and enterprise risk management programs.

BEST PRACTICE RECOMMENDATIONS

- **Cybersecurity Accountability.** Ensure that the stakeholder responsible for cybersecurity initiatives is held accountable for program performance and coordinates with all relevant departments to achieve the objectives. Ideally, cybersecurity ownership and accountability should be outside the IT department for the program to be truly effective.

- **Business Unit Coordination.** Involve all relevant business units in IT strategic planning activities and corresponding status meetings to ensure sufficient representation. To determine which business unit leaders to include in cybersecurity initiatives consider various factors, such as the business model, industry type, types of information exchanged, regulatory requirements, standards, and related items. This is especially essential in coordination efforts between executive, IT, and legal teams.

- **Vendor Risk Management.** Vendors and third party providers continue to be a leading cause of cyber breaches for organizations. To effectively manage this potential vulnerability, not only must organizations develop and implement vendor and third party supplier cyber standards, they must conduct ongoing vendor audits to ensure contractual commitments are met. It is imperative that any vendor audit process is designed to fully understand the risks (if any) within the control environment of the vendor, including cloud solution provider.

  Organizations must request, receive, and review System and Organization Controls (SOC) audit reports (formerly known as Service Organization Control reports). A SOC report is an independent auditor's evaluation of a service organization's services, which provides transparency and cultivates trust. Organizations must still oversee service organizations who do not have such reports. The vendor audits as well as any risk management procedures that are implemented should account for these situations by holding discussions with the provider and perhaps conducting on-site visits as needed. These activities should determine potential impacts to system(s), operational activities, and enterprise resiliency. Not all controls are the responsibility of service organizations. It's important to fully understand and implement the controls that rest with end user organizations. Vendor risk management procedures should also include periodic monitoring of the service providers to validate commitments are being met.

- **Governance and Compliance.** To support a culture for cybersecurity and resilience, develop a governance program and related IT policies and procedures in collaboration with relevant business units. Document and apply an industry leading IT framework for developing or enhancing this program. Disseminate the IT policies to all personnel of the organization. Conduct periodic security awareness training to ensure that the IT policies are well understood and cover other relevant security topics.

02

RISK IDENTIFICATION

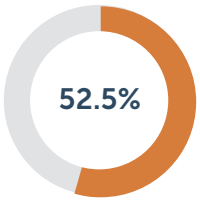
This section covers activities involved with identifying cybersecurity risks, which include IT, Governance (i.e., organizational structure, policies, and procedures), Risk Management, Asset Management, and Third Party Management.

OVERVIEW

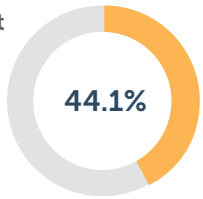
As cyber risk continues to evolve, ongoing risk identification is critical to any effective risk mitigation strategy. The risk identification process is a core component of a risk management program. The survey findings show that a large portion of the respondents still do not have risk management frameworks, or policies developed. In fact, the data indicates a slight decline of 3-5% in these efforts compared to prior years.

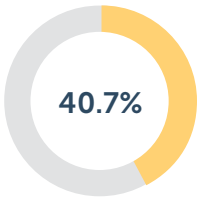
These activities should be established and governed by a comprehensive risk management strategy including a defined risk appetite, established thresholds, and the development of risk identification and mitigation procedures. It is imperative to maintain a complete and accurate asset inventory noting critical components. Risk identification should not be limited to conducting vulnerability scans and penetration tests.

Respondents noted that **Risk Management** policies and procedures were finalized and disseminated to end users and relevant stakeholders.



Respondents had final **Asset Management** policies and disseminated documentation — a decrease from prior years where nearly half of respondents had gone through this process.





Respondents have set up **Information Classification** systems, a new initiative that reinforces the maturity in organizations' understanding of overall cyber risk and data assets.

The absence of these documents does not necessarily mean that the activities are not happening. However, the activities may not be occurring in a standardized manner, in accordance with other policies, and relevant stakeholders may be unaware of risk management processes. Additionally, the regulatory landscape has grown more strict, with auditors now seeking demonstrative evidence of policies being enforced and updated on a regular basis. In some cases, increased fines have been imposed on organizations that cannot meet this new threshold.

VULNERABILITY MANAGEMENT

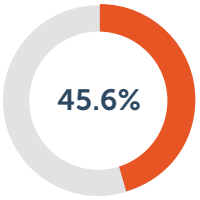
37.3%
Of respondents did not conduct penetration/ vulnerability tests

27.1%
Conducted such tests quarterly

23.7%
Annually

11.9%
Semi-Annually

Almost half of the respondents reported their last vulnerability assessment was conducted within the last twelve months.



OUTSOURCING VULNERABILITY TESTS

The demand for cybersecurity professionals remains high, and outsourcing these types of assessments and services to Managed Security Service Providers or other such vendors is an increasingly popular option amongst respondents who may be operating with personnel constraints or lack of in-house expertise.

10.8%

Of the total respondents have contracted an MSSP for ongoing cybersecurity services.

58.2%

Of respondents use a third party provider

41.8%

and conduct the tests internally.

20.3%

Of respondents did not know who conducted such tests.

Conducting penetration tests and vulnerability assessments on an ongoing basis is required for an organization to adequately mitigate cyber risks. The frequency of these tests should be adjusted based on the findings and the sufficiency of remediation activities. The organization's understanding of high risk areas including its data classification and the overall risk management strategy should also inform the frequency of such tests.

RECOMMENDATIONS

- **Risk Management.** Develop and implement risk management procedures. Once risks are identified it is imperative for an effective process to be in place to implement mitigating actions. These processes should ensure risks are tracked, prioritized, and managed completely.
- **Asset Management.** Develop asset management documentation. Procedures should be in place to obtain a complete and accurate inventory of assets and their authorized custodians.
- **Vulnerability Scans and Penetration Tests**. Conduct these scans and tests at a periodic frequency. Whether conducted by in-house personnel or a third party, the results from these tests are needed to dynamically manage identified risks.

03

INFORMATION & ASSET PROTECTION

This section covers activities involved with implementing safeguards to protect information and IT assets (e.g., workstations and infrastructure), which includes security awareness and role based training.

OVERVIEW

If data is the new currency, then protecting information and interconnected assets is imperative to survival, business operations and resiliency. The information and digital assets most vital to an organization need advanced safeguards to protect them. Organizations that lack clear information classification guidelines are more vulnerable to data compromise. Once appropriate safeguards are in place to protect information assets, all levels of personnel should be trained on their responsibilities.

Safeguards to protect information and assets can begin with a variety of sources such as regulations, standards, and control frameworks. Organizations must identify the regulatory requirements applicable to them and their industries, then adopt a framework that confirms compliance and best protects their information. Note however, that compliance does not necessarily ensure security. Instead it should be viewed as a baseline supported by additional policy, procedural, and technological framework necessary to protect critical systems and to address known vulnerabilities.

The management of healthcare data is governed by the Health Insurance Portability and Accountability Act (HIPAA). Similarly, Federal government data must be managed in accordance with the Federal Information Security Modernization Act (FISMA) and some agencies have additional requirements. In other cases, standards may exist instead such as the Payment Card Industry Data Security Standard (PCI DSS) which is for merchants who store, process, or transmit cardholder data. As the federal government seeks to address data privacy and security concerns, the regulatory environment continues to get more complex.

Educating personnel on their responsibilities towards protecting digital assets is as important as applying the appropriate safeguards. Awareness, education and training responsibilities include providing communication, appropriate documentation and sufficient training related to the information protection. Organizations with robust and frequent training program can minimize the risk of breaches. Middle market organizations may not conduct security awareness training, or may do so infrequently, which hinders achieving optimal information protection program effectiveness. Training of internal personnel must be coupled with proper oversight of vendor relationships to validate information and assets are handled appropriately. Further, training should be viewed as an investment in business reliability and should not be simply viewed as an expense.

SURVEY INSIGHTS

54.6%

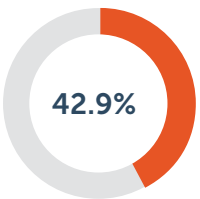
Of organizations have defined what "sensitive information" means to their business.

IDENTIFYING SENSITIVE INFORMATION

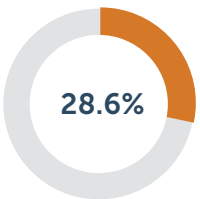
The rise of cyber attacks over recent years has forced organizations to better understand and evaluate potential threats. The majority of organizations surveyed understood the definition of sensitive data, an increase of almost 10% from prior years, with clear protocols in place to protect such data. Additionally, the majority of organizations were able to quantify the impact sensitive data had on their overall business operations.

RELIANCE ON SENSITIVE INFORMATION

Notably, the number of respondents reporting a heavy reliance on sensitive information has increased by more than 15% over prior years, while those with the least reliance on this data has been reduced by 10%.



Of respondents reported that **51% or more** of their business depends on sensitive data (e.g., Personally Identifiable Information (PII) and Protected Health Information (PHI)).



Of respondents reported **1-10%** reliance on sensitive information.

INFORMATION SAFEGUARDS

Information protection should integrate and coordinate the capabilities of people, processes, and technology to establish multiple countermeasures to protect the confidentiality and integrity of information assets. Multiple layers of different types of safeguards have unique characteristics which can prevent an unauthorized person from gaining access to the information assets. This approach, known as "multi-layered security stack," can significantly reduce the risk of a breach. The right mix of information safeguards requires focus on three areas:

People | This includes the right tone at the top, clear assignment of roles and responsibilities, segregation of duties and training of personnel.

Technology | Diversified technological defenses within and outside the perimeter, including firewalls, intrusion detection, physical security controls, data loss prevention, etc.

Processes | The activities required to safeguard information on a day-to-day basis, including access management, vulnerability reviews, process controls, and incident response planning.

80.4%

The majority of respondents use network security devices (e.g., firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS)).

60.7%

Of respondents have physical security controls in place (e.g., badge readers).

51.8%

Role-based access provisioning

58.9%

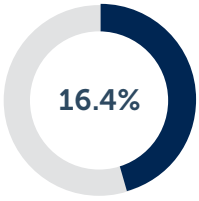
Segregation of duties controls

44.6%

Data loss prevention (DLP) software

ASSET MANAGEMENT

An IT asset is any organization-owned information, system, or hardware that is used in the course of business activities. The asset management process typically involves gathering a detailed inventory of an organization's hardware and software and timely validation of the assets at a regular frequency. More than half of total respondents conducted asset validity at some interval as detailed below:



Of respondents conducted asset validation activities on an annual basis

9.1%	14.6%	9.1%	5.4%
Quarterly	Monthly	Weekly	Semi-Monthly

However, an alarming 45.5% of respondents conducted no validation of their assets at all. This can create significant vulnerabilities within an organizations IT framework, which cyber criminals can take advantage of.

EDUCATION

Education and training are crucial to protect against information and asset security incidents. The majority of respondents (85.7%) are conducting cyber training at some frequency throughout the year, a significant increase compared to prior years (63.6%). Of the respondents that provide training, the majority continue to do so on an annual basis (48.2%), though there is an uptick in respondents are conducting trainings at more frequent intervals than in prior years. Of the entities conducting role-based training it was predominantly on an ad hoc basis (21.4%), though the majority of respondents did not conduct any role-based training (44.6%).

Security awareness training is intended to be applicable to all personnel by informing them of their responsibilities to protect organization assets. This also involves continuing education on current trends and ways to counter cyber threats (e.g., phishing emails, viruses, and ransomware). This training is essential to cultivating a security risk aware culture. However, alone, it is insufficient for various roles especially within the IT department. Due to the evolving nature of cyber risks and a lack of adequate resources, most organizations conduct ad hoc training. However, the reality is that in the 21st century risk environment, all roles, including senior leaders in the C-suite and Board, should have periodic training. While not the only solution, it can often be a low cost and highly effective measure to limit cyber risk.

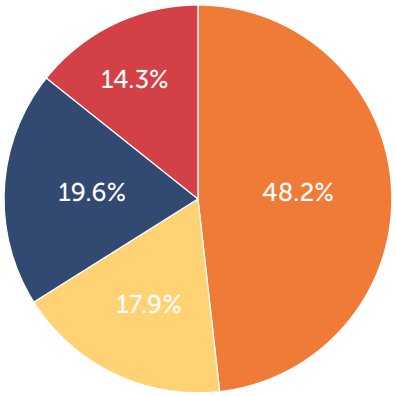


Figure 2 | Security Awareness Training Frequency

- Annually
- Semi-Annually
- Quarterly
- Not Conducted

REGULATIONS & STANDARDS COMPLIANCE

Cyber regulations are growing both in the U.S. as well as abroad. Since the initial Cyber 360° survey was conducted, numerous new cyber regulations have emerged to ensure consumer data is being protected and organizations are better prepared. Of the total respondents only 16.4% answered "unknown" when asked to report the types of standards and regulations applicable to their organization. This demonstrates that, while most track these regulations, there are still some organizations who are either unaware or uncertain of the standards to which they must adhere. Regardless of the reason, this leaves them potentially exposed costly non-compliance fines. It is also essential for organizations to be fully informed of their compliance obligations in order to ensure their supply chain and business partners are also compliant—which, importantly, applies to the usage of cloud service providers to conduct operational activities. In some cases, multiple regulations and standards may apply, which warrants consolidated control-mapping efforts to streamline maintenance efficiency.

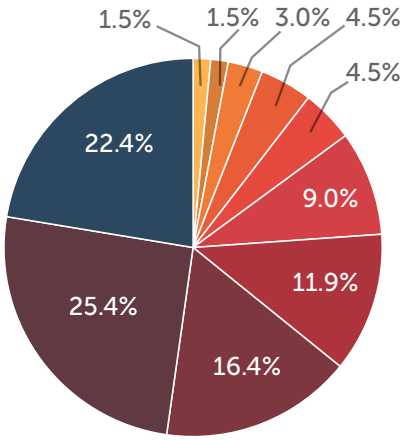


Figure 3 | Regulations and Standards Impacting Respondents

- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management/Modernization Act (FISMA)
- Financial Industry Regulatory Authority (FINRA)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Federal Financial Institutions Examination Council (FFIEC)
- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Unknown
- Health Insurance Portability and Accountability Act (HIPAA)
- Other

Defense Federal Acquisition Regulation Supplement (DFARS)	Since 2017, the Federal Acquisition Regulation (FAR) governs the way that the government can procure goods and services. DFARS applies to Department of Defense (DoD) contractors who are managing covered defense information within their systems.
Federal Information Security Modernization Act (FISMA)	FISMA applies throughout the Federal government and for contractors involved with supporting, maintaining, providing the information and information systems that support the operations and assets of an agency.
Gramm-Leach-Bliley Act (GLBA)	GLBA is also known as the Federal Modernization Act of 1999, which is a Federal law designed to control the management of individuals' private information by financial institutions.
Payment Card Industry Data Security Standard (PCI DSS)	PCI DSS is a proprietary information security standard for credit card management organizations. Specifically, it applies to organizations that store, process, or transmit cardholder data. The PCI Security Standards Council administers PCI DSS.
Sarbanes-Oxley Act (SOX)	The SOX Act was passed by the U.S. Congress in 2002 and requires all publicly held companies to establish internal controls for financial reporting to protect stakeholders from fraudulent accounting activities. Many non-public companies also comply with SOX as a best practice.
General Data Protection Regulation (GDPR)	GDPR standardizes privacy laws across the European Union and is applicable to all member states. GDPR went into effect on May 25, 2018.
North American Electronic Reliability Corporation Critical Infrastructure Protection (NERC CIP)	The NERC's mission is to oversee the bulk power system in North America to assure its reliability and security. CIP is a cybersecurity reliability standard used to achieve the mission.
Cybersecurity Maturity model Certification (CMMC)	CMMC is a unified security standard for establishing strong cyber infrastructure and practices across the Defense Industrial Base (DIB). It builds on the currently existing NIST standards. The DoD released the standards in January 2020 to initiate a five year rollout that culminate in the final deadline on October 1, 2025.

Table 1 | Regulation and Standards Descriptions

The most recent compliance standard underway is Cybersecurity Maturity model Certification (CMMC). This is a training, certification, and third party assessment program of the United States government Defense Industrial Base aimed at measuring the maturity of an organization's cybersecurity processes toward demonstrating compliance with the protection of Federal Contract Information (FCI) and Controlled Unclassified Information. CMMC will become a key requirement for any DoD contractor.

THIRD-PARTY MANAGEMENT AND MINIMUM SECURITY STANDARDS

A growing area that cyber attackers have been exploiting is third party providers. Cyber attackers are aware that sometimes, the easiest way to carry out an intrusion, is to compromise a business partner rather than the primary target. Hence, it is imperative to implement a comprehensive third-party management program. Basic elements such as policy, vetting form, and corresponding procedures are key. The next step of communicating the program and user responsibilities is essential to promoting standardization and compliance. Services must be evaluated for cyber risks during the vetting process and on an on-going basis to ensure minimum standards are adhered to per contractual agreements. Without a program and oversight group (e.g., contracts team or IT risk and compliance team) to ensure minimum standards are being met, organizations are vulnerable to unidentified or improperly managed risks. The costs of implementing such programs should be evaluated with the consequences of not having them in place at all or in an effective manner.

With the increased number of attacks originating via suppliers and third party vendors, all organizations should be focused on implementing a robust third party management and vetting system.

THIRD PARTY MANAGEMENT PROGRAM

45.0%
Of respondents noted that there was no third party management program in place at their organization.

23.3%
Of respondents were unaware of any such program.

31.7%
Of respondents noted that a Third Party Management Program is in place to vet third parties.

THIRD PARTY MINIMUM CYBERSECURITY STANDARDS

32.2%
Of respondents noted these requirements are not in place.

20.3%
Of respondents were unaware of such activities.

47.5%
Of respondents noted that third parties are required to meet minimum cybersecurity standards set by the organization.

THIRD PARTY CYBERSECURITY COMPLIANCE MONITORING

33.9%
Of respondents said that third party compliance with contractual and cybersecurity standards was not monitored.

35.6%
Of respondents did not know if such activities occurred.

30.5%
Of respondents said such activities were monitored.

RECOMMENDATIONS

- **Network Segmentation and Information Classification.** Consider network segmentation to isolate sensitive information including those that require compliance with regulations or standards from other types of data. Determine effective safeguards for critical and sensitive data (e.g., multifactor authentication and role-based access). An Information Classification policy and procedures should be developed to categorize data to ensure the appropriate safeguards are implemented.

- **Information Safeguards and File-Sharing Mediums.** Implement and evaluate a defense-in-depth approach to security safeguards for effectiveness. File sharing mediums should be evaluated at initial deployment and on a periodic basis to identify risks and restrict access to the minimum needed.

- **Asset Management.** Determine high priority and total inventory of assets to include in monitoring activities. Conduct asset validity checks on a periodic basis. Coordinate asset management activities with Human Resources (HR) on-boarding and separation activities.

- **Security Awareness Training.** Develop a training program that includes security awareness training and role-based training. Incorporate compliance with the program requiring personnel to take the training. Determine when ad hoc security refreshers should be shared via email, online courses, or in person.

- **Regulation and Standards Compliance.** Conduct an assessment to determine all applicable regulations and standards to the organization. This includes understanding the business services provided, the types of data managed, contractual agreement details with customers and business partners plus, related information. Identify gaps with requirements. Determine remediation solutions and priorities. Implement a compliance program to monitor controls and maintain awareness of requirement changes. Involve this subject in strategic planning documents and sessions to ensure continued compliance.

- **Third Party Audit and Security Standards.** Determine the minimum security standards that should be in place for the various types of third party relationships. Coordinate with legal personnel to determine the best way to incorporate and mandate these requirements. Ensure monitoring of compliance with these standards is incorporated into the third party management program.

04

EVENT DETECTION

This section covers activities involved with determining when a cybersecurity event has occurred, which includes the types of software and tools used for these processes. Incident management plans to address detected events are also covered.

OVERVIEW

In prior years, when participants were asked to estimate the likelihood of a cyber attack occurring within the next 12 months, the majority of respondents overwhelmingly stated that the likelihood is inevitable. This time, however, respondents gave a more divided response, with the majority of respondents at each end of the spectrum — Not Likely (37.9%) and Inevitable (34.9%).

These findings are very telling of the conflicted view of cyber preparedness amongst organizations today. It shows both how organizations have grown somewhat desensitized to cyber risk, acknowledging it is a matter of when, (not if) they fall prey to an attack. While those who answered Not Likely continue to hold a heightened sense of hubris that they are not vulnerable to cyber risk. In a shift from prior years when respondents were divided in their estimations of risk from common threats such as ransomware, insider threats, viruses, intrusions and old architecture threats, this year the majority indicated that all of these threats had a low likelihood of materializing. This further illustrates the disconnect between cyber vulnerability and preparedness.

DETECTION MEASURES

Implementing appropriate event detection software and measures, applying appropriate configurations, and having a process in place to address areas of concern are crucial to cybersecurity resilience.

38.0%

The most common type of event detection measure in place was an Intrusion Detection System.

22.0%

Followed by the use of Security Information and Event Management (SIEM) tools.

20.0%

Audit Logging and Review.

16.0%

Third Party Security Monitoring was last, a complete reversal from prior years where this was the most used approach.

SURVEY INSIGHTS

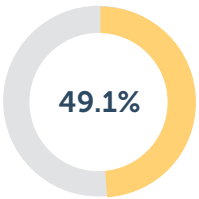
Have incident management procedures been finalized and disseminated to end users and relevant stakeholders?

44.2% **55.8%**

Surprisingly more than 50% of respondents indicated that incident management procedures had NOT been finalized or disseminated to end users at their organizations—a higher percentage than prior years. This is crucial step to any cybersecurity plan as you need a well rehearsed and tested response plan to reduce the overall impact of a cyber intrusion event, and a requirement now for any cyber insurance policy.

INCIDENT MANAGEMENT

A cyber attack can impact almost every vertical of a business, disrupting operations and having potential legal and reputational consequences. Yet our survey reveals that, disturbingly, nearly 60% of the respondents have not finalized and disseminated incident response procedures across the enterprise leadership. Incident management teams should be comprised of individuals representing multiple business units (e.g., Senior leadership, IT, communications, legal, accounting/finance, and local authorities). The diversity of representation is essential to ensuring all perspectives are considered and factored into the incident management plans.



Of respondents reported that their organizations have designated a cyber crisis management team.

BREACH RESPONSE

Being unaware of a breach does not mean one did not occur. Event detection tools may not be in place or configured appropriately to identify incidents. When sufficient safeguards are in place to deter and detect attack, a "set it and forget" approach is dangerous. Instead, these controls must be continuously reviewed to withstand evolving threats.

37.7%
Of respondents experienced a data breach, cybersecurity attack, or intrusion.

43.4%
Of respondents noted that they did not experience any of these types of attacks.

17.0%
Of respondents noted the presence of such incidents were unknown.

34.4%
For those respondents who experienced a breach or similar event, roughly a third of respondents indicated there was no adverse impact.

BREACH IMPACTS

When a breach has been experienced, a variety of impacts could result from the event. For the 37.7% of respondents who experienced a data breach, they noted the following adverse impacts on their organizations. In addition they also reported the remediation actions taken.

32.3%
Organizations indicated the largest **expected impact** of a cyber attack remained the theft of sensitive information.

24.2%
Financial losses represented the second greatest impact.

21.5%
Followed by loss of brand reputation and customer trust

16.7%
Regulatory fines

12.3%
Intellectual Property Theft

10.8%
Loss of market share

6.3%
Supply Chain Disruption

*Respondents were able to select multiple impacts encountered.

40.6%
For those who **experienced** a cyber attack, the most common impact was operational downtime.

25.0%
Followed by business interruption and lost revenues

21.9%
Experienced reputational harm

6.3%
Lost customers

6.3%
Saw theft of intellectual property

41.2%
In recovering from the reported breaches, the majority of respondents increased network security measures (E.g. firewalls, intrusion detection, etc.)

17.7%
This was followed by training

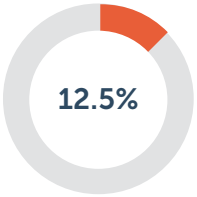
5.9%
Hired cybersecurity consultants/specialists

5.9%
Invested in cybersecurity systems/services

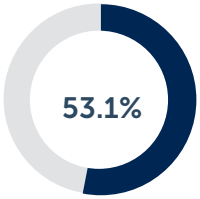
5.9%
Personnel changes/ restructuring

BUSINESS CONTINUITY AND DISASTER RECOVERY

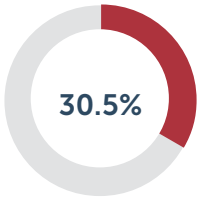
The impacts of a cyber breach for mid-market organizations can significantly affect operations, revenue, and reputation. These organizations may not be able to absorb the costs of an incident and continue to resume business activities. Larger organizations may have capital reserves to address the monetary impact of breaches, including legal fees and lost revenue. Hence, the importance of business continuity and disaster recovery planning cannot be emphasized enough.



Of respondents set aside business continuity funds to support cyber incident management activities.



The majority of respondents have not allocated funds for this purpose.



Were unaware of any budget allocated.

BUSINESS CONTINUITY DISASTER RECOVERY PLANS

Cyber events can lead to considerable business interruptions or even closure. One third of respondents did not have Business Continuity / Disaster recovery plans finalized and distributed. Without these recovery mechanisms, the resumption of operations may be delayed and may not achieve the intended level of performance.

50.0%

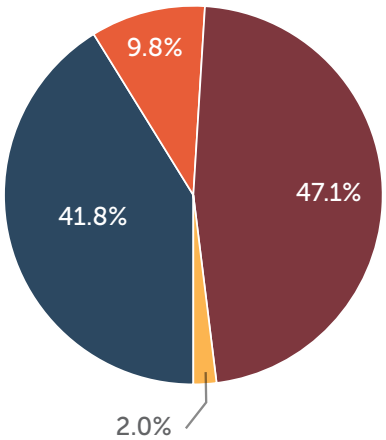
Of respondents noted that Business Continuity/ Disaster recovery plans were finalized and disseminated to relevant stakeholders.

34.0%

Did not have these plans finalized and distributed.

16.0%

Of respondents were unaware of such documentation.



When a significant cyber incident occurs, response teams are relying upon their plans to be accurate and effective to expedite activities. Hence, periodic tests of these plans is crucial to ensure that the procedures in place will effectively recover any impacted systems or infrastructure. Organizations should consider what works best for them based in developing these plans factoring in the types of services provided, the recovery and redundancy controls in place, and their thresholds for recovery.

Figure 4 | Business Continuity/ Disaster Recovery Plan Testing

- Yes - Tested Annually
- Yes - Tested Every Other Year
- No
- Other

CYBER INSURANCE

58.8%

Of survey respondents indicated that they had some sort of cyber liability insurance in place at their organizations.

The adoption of cyber insurance by middle market companies has continued to rise over the years. This is a positive indication because cyber insurance provides an added layer of financial resiliency, as well as critical breach response resources, which these organizations may not have readily available otherwise. However, the cyber insurance market has become more limited due to the growing number of cyber breach losses incurred, resulting in insurers establishing more rigorous underwriting and cybersecurity standards. Premium rates have also increased significantly, ranging from 50% to 100% rate hikes. Many clients will now need to focus on implementing these increased standards, as well as added costs, if they wish to retain coverage.

Another area of concern is the type of cyber insurance that is being purchased. As cyber risk spans across several insurance risk classes, a range of policies can provide certain levels of cyber coverage. However, not all cyber policies are created equal. Companies who do not opt for a standalone cyber insurance policy may find that they only have limited coverage for compliance or notification expenses but lack coverage for breach response or lost business revenue losses.

While the trend for cyber insurance is growing, a large number of respondents (41.1%) still have no coverage in place. This is rather alarming given the high rate of attacks within this group category. Of the 41.1% respondents, when asked how their company would fund remediation expenses, they responded as follows:

SURVEY INSIGHTS

41.1%

Of organizations still have no cyber insurance coverage in place.

31.3%
Current Operating Funds

12.5%
Set Aside Funds for Cyber Incidents

53.1%
No Pre-set Plan

3.1%
Other

Companies that are not insured against cyber risks and are not budgeting for the associated expenses will find themselves at risk of going out of business when they experience a cyber incident.

While small and mid-market organizations may be uncertain whether cyber insurance is a worthwhile, or affordable expense, the growing costs associated with cyber incidents is greater. Cyber insurance has become more commonplace with a multitude of carriers offering coverage, however not all policies offer the same level of protection. As in prior years, when organizations evaluate cyber insurance products, they need to be sure they are conducting in-depth reviews and working with knowledgeable insurance partners. Understanding the exclusions and coverage gaps is more important now as many carrier have reduced or limited certain coverage components. Another area to continue to look out for is making sure that the selected cyber policy provides breach response coverage and business interruption coverage. Many policies continue to only offer liability protection, leaving companies exposed in the event of ransomware or other major disruptive incidents occurring.

RECOMMENDATIONS

- **Incident Response Plan.** Insurers and regulators alike are requiring organizations to have fully developed cyber incident response plans in place. This requires organizations develop, finalize, and distribute a robust response plan within their organization. This plan should also be distributed to all staff throughout the organization, and practiced by the key stakeholders with pivotal roles within the cyber crisis management team.

- **Breach Response.** Breach response activities should be incorporated into any incident response plan as well as the policy documents. If external consultants or providers are utilized, they too should be well versed and incorporated into the incident response plan. Likewise, cyber insurance should be taken into consideration as insurers will have their own breach response protocols and providers in place. A coordinated response plan helps to provide a more effective mitigation strategy while containing costs. Alerting insurers also helps to ensure all costs are covered under the policy avoiding any surprises down the line. The breach response plan should also include remediation activity procedures to determine what type of actions will be taken and a process to document cases where action is not taken.

- **Business Continuity / Disaster Recovery Funds.** Developing and disseminating business continuity/ recovery plans is another critical step. Conducting periodic tests of these procedures will also help strengthen the organization and validate the plans effectiveness. These plans should be regularly updated, incorporating lessons learned from tests, simulations or real life incidents as they occur.

TOP CHALLENGES

Survey respondents indicated the top challenges faced by their organizations. The top challenges are listed in order of highest response. Respondents could select all applicable challenges for this question.

LACK OF CYBERSECURITY PERSONNEL

The limited pool of qualified cybersecurity professionals remains a top concern across all industries. This shortage of talent is only getting worse, exacerbated by the growing frequency and sophistication of cyber-attacks. The need to invest in hiring and developing cybersecurity professionals is becoming abundantly clear to corporations and governments alike. However, this is not an issue that will be solved in the immediate future. In the United States, there are around 879,000 cybersecurity professionals in the workforce and an unfilled need for another 359,000 workers, according to a 2020 survey by (ISC)2, an international nonprofit that offers cybersecurity training and certification programs. Globally, the gap is even larger at nearly 3.12 million unfilled positions

RECOMMENDATIONS

- Outsource cybersecurity to a third party Manages Security Services Provider to meet immediate needs and establish knowledge sharing programs to build up internal talent simultaneously.
- Leverage cyber insurance to augment internal IT teams with breach response capabilities should an incident occur.
- Explore cybersecurity focused recruiting firms to find and onboard key personnel.
- Explore partnering with universities and colleges to develop a talent pipeline.
- Coordinate internal IT staff with external risk management and cybersecurity providers to help ensure enterprise wide cyber consideration.
- Participate in programs that encourage the next generation to pursue Science, Technology, Engineering, and Mathematics (STEM) careers.
- Continue standard methods of posting job openings on professional organization job boards. This includes full-time, seasonal, and internship opportunities. Firms that do not have the cybersecurity expertise in house, or do not deem it cost effective to do so, can seek outside providers to carry out these services.

INSUFFICIENT/LACK OF DOCUMENTED POLICIES AND PROCEDURES

Development and dissemination of cybersecurity policies and procedures remains a challenge for many organizations. Given the previously mentioned shortage of cybersecurity professionals, this is not a surprising finding. Cyber policies and procedures should not only work to support an organization remain compliant, but they should also be designed to help build resiliency and meet strategic objectives. Firms that have developed these plans often fall short of successful implementation.

RECOMMENDATIONS

- Look for trusted online resources, such as National Institutes of Standards and Technology (NIST) and National Cybersecurity Alliance (NCSA), to help guide the development and implementation of cybersecurity policies.
- Engage risk management of cybersecurity consultants to help develop and implement policies.
- Develop a maintenance process of documentation that includes periodic reviews and approved updates.
- Promote enterprise wide access, sharing and adoption of these policies to ensure all staff are aware of the firms protocols.
- Conducting ongoing training and updates is another critical aspect of this process.

INSUFFICIENT CYBERSECURITY BUDGET

While the awareness of executive teams around the need for cybersecurity has grown, funding to execute cybersecurity initiatives remains insufficient. This is in part to the ever evolving cyber threat landscape. Executives face the challenge of how to best allocated the limited funds available towards IT and technology solutions, staffing, training and other mitigation resources.

RECOMMENDATIONS

- Quantifying cyber risk in financial terms can often help leadership teams better evaluate cybersecurity investments.
- Ongoing communication and cross company collaboration with executive teams and cybersecurity personnel will help senior leadership to identify budget support opportunities. This could include additional tailored trainings on cyber risk for senior leaders, adjusting the frequency of cyber risk program report updates, revising the content or format of reports, or other areas.
- Revised reporting and forecasting models will help better identify and prioritize cybersecurity investments by better illustrating business impacts in relation to strategic initiatives.
- Leveraging risk transfer solutions and insurance will allow organizations to place a fixed cost on cybersecurity and transfer the financial exposure from the P&L and into the financial markets.

OLD SYSTEM/NETWORK INFRASTRUCTURE

Legacy systems and outdated network infrastructure remain a challenge for organizations. While companies have many business centric reasons for keeping old system/network infrastructure in place, it is a growing area of vulnerability. If companies are not able to replace outdated legacy systems due to budgetary constraints, operational requirements or other reasons, they must find ways to ring fence these systems and harden defenses.

RECOMMENDATIONS

- Review the lifecycles of old systems and network infrastructure to identify ideal transition schedules.
- Review dependencies from third-parties (e.g. customers and business partners) that may require the use of old systems or network infrastructure to update transition schedules accordingly if needed.
- Prioritize transition needs for modern migration upgrades. Develop business cases for selected priorities.
- Determine the most suitable presentation format to senior leaders to establish an understanding of the needs and secure their support.
- Develop containment strategies to ensure legacy systems have limited if no access to the broader network.

INEFFECTIVE ORGANIZATIONAL STRUCTURE

Organizational structures remain very siloed while cyber risk has grown pervasive, impacting nearly every aspect of an organization's operations. Reporting lines for cybersecurity matters must be designed in a way to promote visibility, prioritization, accountability, and integration into enterprise risk management activities. In organizations with ineffective organizational structures, cybersecurity initiatives may not be receiving the appropriate attention and prioritization.

RECOMMENDATIONS

- Consider assessment options for organizational structure improvements by determining if this will be conducted by internal personnel or consultants.
- Conduct an assessment which relies upon internal personnel feedback, industry standards, and best practices to identify improvement opportunities.
- Present improvement opportunities to focus groups and senior leaders to determine a remediation roadmap.
- Execute the remediation roadmap accordingly to support the organizational structure improvement initiative. Develop a process to monitor the changes and re-evaluate any new challenges.

PATH FORWARD

Based on our analysis of the survey results, the survey partners make the following final recommendations on the path middle market organizations must take to stay ahead of the next threat.

Cyber has become the defining risk of the 12st century. Organizations across all industry verticals must contend with how to navigate the complex and shifting cyber threat landscape. As technology continues to advance, and organizations grow ever more interconnected, cybersecurity will continue to be a central pillar of any organizations business strategy. To successfully navigate a cyber attack with minimal loss and disruption, a proactive and agile cyber posture will be necessary. Investing in technology alone will not be sufficient, organizations must approach cybersecurity holistically, implementing technologies as well as education to achieve network resiliency and ensure business continuity.

EVALUATE NEW TRENDS FOR SECURITY AND COMPLIANCE IMPACTS

Cyber regulations continue to change as the cyber threat landscape grows more treacherous. It is therefore important to establish a process to remain up to date on all applicable regulations, standards, and framework changes. This is a s crucial step to avoiding non-compliance penalties. Organizations must now look beyond their operations when it comes to compliance. Ensuring that any third party providers or other vendors with access to key information are in compliance is a new development that firms must now comply with for certain regulations.

Despite considerable efforts from internal IT teams and external organization involvement, there may still be concerns about whether requirements for a framework, regulation, or standard have been completely satisfied or are sufficient. In such cases, consultants can be leveraged to provide a second review to validate compliance activities. Engaging with consultants can help to address ambiguity in compliance requirements, provide insight on industry best practices, and identify actions needed to work toward compliance.

LEVERAGE INFORMATION SHARING GROUPS

Information sharing remains a key step towards cyber resiliency. Where organizations once were apprehensive about sharing cyber related information, they are slowly seeing the value. Continued threat sharing and other Information Sharing Analysis Organizations (ISAOs), help establish an early warning system within industries. By alerting industry peers, it provides the majority of firms to better prepare their defenses and mitigate attacks. This type of collective risk sharing model is something that should be further explored and developed in a private-public type partnership. This enables the smaller and larger organizations to leverage similar levels of cyber defense while not able to expend the same type of budgets for security.

OBTAINING AND MAINTAINING CYBER INSURANCE

Unlike prior years, the cyber insurance market has now become more selective. Cyber insurance provides many benefits to organizations and can often enable a company to survive such an intrusion by transferring the financial losses away from its balance sheet and onto the insurer. Cyber insurance has proven very effective in this regards, with a large number of claims paid by carriers over the past several years. This has now resulted in underwriters growing more weary of this product class and therefore implementing more stringent underwriting requirements, higher rates for coverage and even coverage limitations on some of the leading loss drivers like phishing and ransomware attacks. This new operating reality means companies must work harder and smarter to both obtain and maintain their cyber coverage. Companies that cannot demonstrate cyber risk management policies in effect, such as multi-factor authentication, cyber response plans, and other critical policies are finding themselves uninsurable when it comes to cyber risk.

Cyber insurance has now grown to a well known and recognized insurance class by the majority of middle market firms. Yet many still opt to forgo this important coverage and rely only on their own funds to pay for associated losses from a cyber incident. This is largely due to the continued misconception that because a company does

not hold large numbers of digital records, that they are not a target for cyber criminals. The reality is that the majority of cyber attacks are ransomware attacks where cyber criminals hold an organization's business hostage until a ransom is paid, more often than not in the six to seven figure range. When this type of incident occurs, organizations find themselves in a precarious situation with little recourse. For this reason all companies of all sizes should conduct a cyber risk assessment to determine both their potential vulnerabilities as well as their financial resiliency to withstand a cyber attack of such a magnitude. If they are unable to afford such a large payout, then they should explore obtaining cyber insurance to offset the risk.

ADDITIONAL CYBER RESOURCES

- **Tear Sheets.** These material resources were developed to educate organizations on the basics for acquiring cyber insurance coverage. Because of the prevalence of cyber risk, it is among the most important coverages we recommend universally

  Cyber 101: Coverage Overview | Learn more about what coverages should be included in your policy, as well as notable exclusions.

  Cyber 101: Sample Technical Specs | To obtain cyber coverage, organizations must provide detailed information regarding their cybersecurity programs.

  Cyber 101: Minimum Cybersecurity Checklist | At a minimum, applicants must meet minimum standards in these six areas to be eligible for coverage.

- **Published Articles & Interviews.** This curated list of pieces serves to illustrate our current cyersecurity landscape, address myths, and demystify the ways organizations can mitgate cyber risk.

  Cyber Attacks Are Killing Small Businesses; Here's What They Can Do To Survive | Originally published on Risk & Insurance, this piece outlines tangible takeaways from previous cyber attacks.

  Executive Briefing on Cyber Insurance | Cybervista, a workforce development firm specializing in educating cybersecurity professionals, invited Risk Cooperative to participate in a subject matter expert interview on cyber insurance.

  Coronavirus and Telecommuting: How One Risk Is Giving Way to an Even Bigger Threat | Featured on the Society for Human Resource Management (SHRM), our team very quickly saw the downstream risks of our collective change to remote work in early 2020.

  CEO's Talk Cyber Risks & Resiliency | Dataprise is a highly esteemed managed security service provider (MSSP). Their CEO invited Risk Cooperative to join in a conversation about the complementary nature of cybersecurity and cyber insurance.

ABOUT RISK COOPERATIVE

Risk Cooperative is a specialized strategy, risk and insurance advisory firm licensed to originate, place and service innovative risk-transfer and insurance solutions in all 50 states, D.C. and Puerto Rico. Risk Cooperative helps organizations address risk, readiness and resilience through a comprehensive service and solution offering in partnership with leading insurance companies and value-adding partners.

For more information, visit **www.riskcooperative.com** or **contact our team** today.