



Cyber  GRX + ProcessUnity 

**A STUDY ON THE BUSINESS VALUE
OF A RISK-BASED APPROACH TO
CYBERSECURITY**

The Transformation of Cybersecurity from Cost Center to Business Enabler



405245.50
639807.00
348029.00
405245.50
639807.00

Table of Contents

Introduction	3
The State of Cybersecurity	5
Building a Compelling Business Case	8
The Future of Third Party Risk Management	11
Conclusion	13
Methodology	14
Survey Questions & Responses	18
About CyberGRX & ProcessUnity	24



Introduction

Businesses increasingly rely on technology to streamline operations, enhance customer experiences, and gain a competitive edge. Digital transformation has brought unprecedented opportunities for growth and innovation. However, it has also exposed organizations to many cybersecurity risks that threaten the foundation of their existence.

Historically, cybersecurity was viewed as a necessary cost center where resources were allocated primarily to safeguard the organization's sensitive data and infrastructure. Organizations would invest in defensive measures to protect themselves against cyber threats, reacting to incidents and breaches as they occur. While this approach was essential for mitigating risks, it often led to people thinking of cybersecurity as an impediment to business growth and agility.

In recent years, some organizations have changed their approach regarding the perception and strategic importance of cybersecurity. More forward-thinking organizations realize that cybersecurity can transform from a mere cost center into a powerful business enabler that drives growth, innovation, and competitive advantage. This transformation hinges on adopting a comprehensive third-party risk management (TPRM) approach to cybersecurity.

The TPRM approach recognizes that businesses increasingly rely on external partners, vendors, and suppliers to perform critical functions and provide essential services. While these third parties offer numerous advantages, they also introduce a significant cyber risk because their vulnerabilities can easily become an entry point for malicious actors seeking to breach an organization's security defenses. As such, it becomes imperative to extend the scope of cybersecurity beyond internal networks and systems to encompass the entire supply chain and partner ecosystem.

“TPRM has become dramatically more complex for global organizations. You can no longer have one standardized provider, such as one payroll provider, because they may not cover all geographies. Now, we have multiple providers for the same service based on location and local regulations. As a result, we're often assessing companies we've never heard of.”

A Global Head of Cyber Assurance and Monitoring

In this paper, we delve into the paradigm shift that is reshaping the way organizations approach cybersecurity, and we also evaluate the following points:



The Current State of Cybersecurity. Understanding the strengths and weaknesses of most organizations' approach to cybersecurity is marred by focusing on reactive measures and piecemeal security solutions, leading to significant downsides and gaps in protecting organizations from cyber threats.



Building a Compelling Business Case for Adopting a Risk-Based Approach to Cybersecurity. By proactively identifying and managing risks that third-party partners, vendors, and suppliers pose, organizations can enhance their overall security posture and minimize the potential impact of cyber incidents.



TPRM is the Future. TPRM is set to become a cornerstone of cybersecurity strategies as businesses recognize its potential to drive growth, foster innovation, and instill a culture of cybersecurity awareness across all levels of the organization.

By understanding and embracing the transformative potential of cybersecurity through third-party risk management, organizations can position themselves at the forefront of secure digital innovation, enabling growth and resilience in an era when cyber threats continue to escalate.



The Current State of Cybersecurity

Traditionally, cybersecurity was approached as a reactive and siloed practice primarily focused on protecting internal networks and systems. As organizations became more connected to the Internet (and connected to other organizations via APIs and constant VPNs), the organization's network and security teams used firewalls, advanced routers, and Data Loss Prevention (DLP) solutions to protect company networks and data.

However, this legacy, siloed approach has significant downsides, leaving businesses vulnerable to emerging threats, lacking comprehensive visibility into their entire risk landscape, and expending valuable resources on incident response and recovery. In contrast, a transformative TPRM approach to cybersecurity offers a proactive and integrated solution to the ever-changing cyber threat landscape.

“The threat landscape constantly changes. The last few years, it was all about ransomware, but now ransomware is taking a backseat to AI. AI has become an enabler of fraud, used for writing better phishing emails with no language hiccups and writing exploit code on known systemic weaknesses or CVE.”

A Chief Information Security Officer

This section critically compares the legacy approach to cybersecurity with the TPRM approach, shedding light on the fundamental differences, advantages, and benefits organizations can derive from embracing a risk-based strategy. By delving into the strengths and weaknesses of each approach, this comparison aims to emphasize the importance of adopting TPRM as a strategic business enabler, elevating cybersecurity beyond a mere cost center to safeguard organizations in the digital age.



Some of the critical challenges of the current approach to cybersecurity compared to a third-party risk management approach include:

A Legacy Approach is Reactive by Nature.

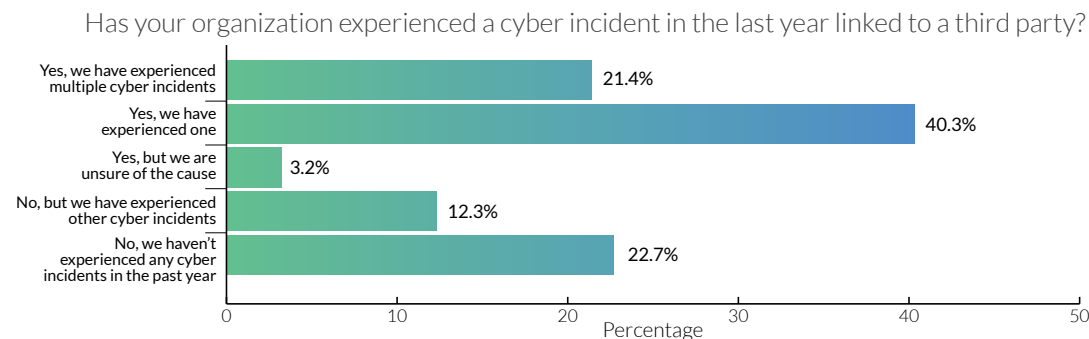
The current approach to cybersecurity often revolves around a reactive stance, focusing on incident response after a breach or cyberattack occurs. This approach leaves organizations vulnerable to emerging threats because they are caught off guard and may struggle to mitigate damages effectively.

Lack of Business Alignment and Siloed Practice.

Many organizations maintain separate security silos for departments or business units, resulting in fragmented security efforts. This compartmentalization hinders a holistic understanding of the organization's risk landscape and weakens the ability to respond cohesively to cyber threats. Also, many cybersecurity organizations lack business integration and alignment, leading to a perception of the security team as the team that says "no" instead of a business enabler.

An Antiquated View of Exposure and Scope.

Traditional cybersecurity practices concentrate on protecting the organization's internal networks and systems. However, with the increasing reliance on external vendors and partners, this limited scope fails to address potential risks that may originate from third-party relationships, leaving critical security gaps. In a recent survey, over 60% of those organizations surveyed experienced a cyber incident linked to a third party, and the number jumps to nearly 80% when asked if the organization experienced a cyber incident of any kind.



Resource Intensive.

The current approach to cybersecurity can be resource-intensive, requiring significant investments in reactive measures, incident response capabilities, and recovery efforts. This expenditure diverts resources from proactive risk management and innovative security initiatives.

Compliance Focus.

While compliance is crucial, a compliance-centric approach may not address all relevant risks. Organizations may prioritize meeting specific regulatory requirements without fully understanding the broader cybersecurity risks and vulnerabilities they face.



On the other hand, a TPRM approach addresses these downsides by:

Proactive Risk Management.

TPRM emphasizes proactive risk identification and management, allowing organizations to anticipate and mitigate potential threats before they escalate.

Modern View of Risk and Scope.

TPRM encompasses the entire partner ecosystem, enabling organizations to evaluate and address risks originating from external vendors, suppliers, and other third parties.

Automatic Organizational Alignment.

TPRM promotes an integrated and collaborative approach to cybersecurity, fostering communication and alignment across different departments and stakeholders throughout the organization.

Security as a Strategic Value to the Organization.

Adopting a TPRM approach can position cybersecurity as a strategic enabler rather than a mere cost center, driving business growth and enhancing competitive advantage through secure and trusted partnerships.

Risk-Based Focus.

TPRM is inherently risk-based, aligning security efforts with the organization's specific risk tolerance and business objectives. This approach ensures that resources are allocated where they are most needed.

Overall, a TPRM approach addresses the shortcomings of the current cybersecurity method and empowers organizations to stay ahead of the ever-evolving cyber threat landscape.

Building a Compelling Business Case

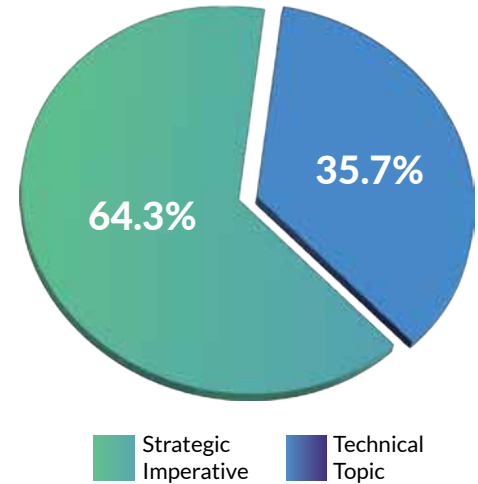
The case for a TPRM approach to an organization’s cybersecurity strategy highlights fundamental business values while also demonstrating security benefits. And the organization’s leadership realizes this is not just another IT/security project among all the other IT and security priorities. When polled, 64% stated that TPRM was viewed as an organizational strategic imperative by their boards of directors and executive teams.

Aligning the business values with the security benefits can be realized in three areas:

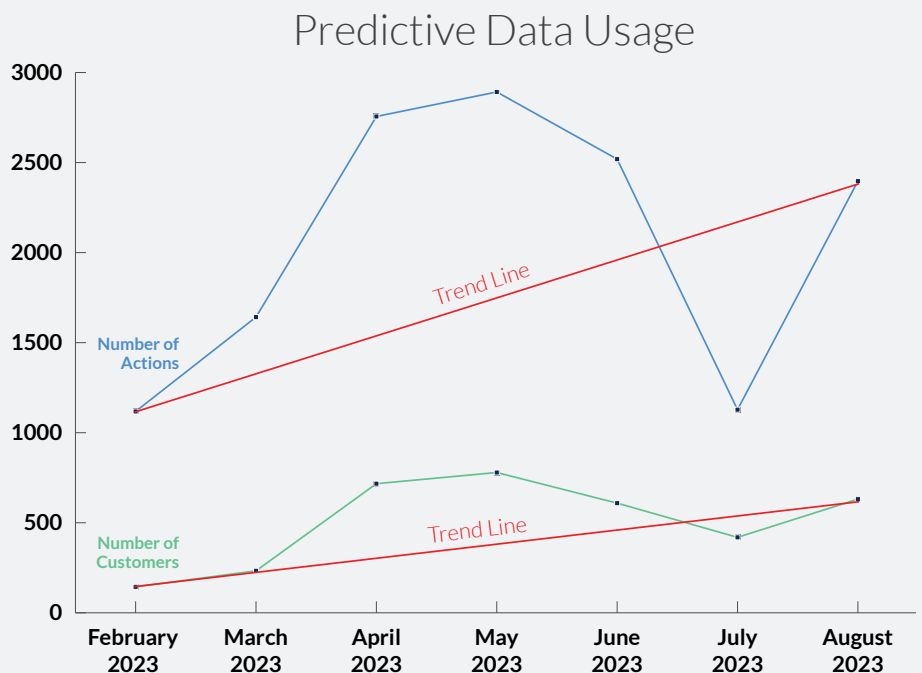
1. Process Improvement.

Adopting a TPRM approach streamlines and enhances various cybersecurity processes throughout the organization. Businesses can identify potential vulnerabilities and gaps within their extended supply chains by conducting thorough risk assessments of third-party partners. This heightened awareness includes implementing targeted security controls and risk mitigation strategies. Moreover, TPRM fosters a culture of continuous improvement, encouraging proactive monitoring and periodic reassessment of third-party security practices in addition to regular assessments. As a result, organizations can maintain a dynamic cybersecurity posture that adapts to emerging threats and ever-changing business requirements.

Is TPRM Viewed as a Technical Topic or an Organizational Strategic Imperative at the Board / C-Suite Level?



Data from the CyberGRX Exchange supports the survey findings, revealing an upward trend of customers who are viewing their third-party risks and identifying control gaps across their portfolio, using both predictive and assessment data. This graph highlights the month-over-month adoption rate and usage of **Portfolio Risk Findings** since its launch in February 2023.

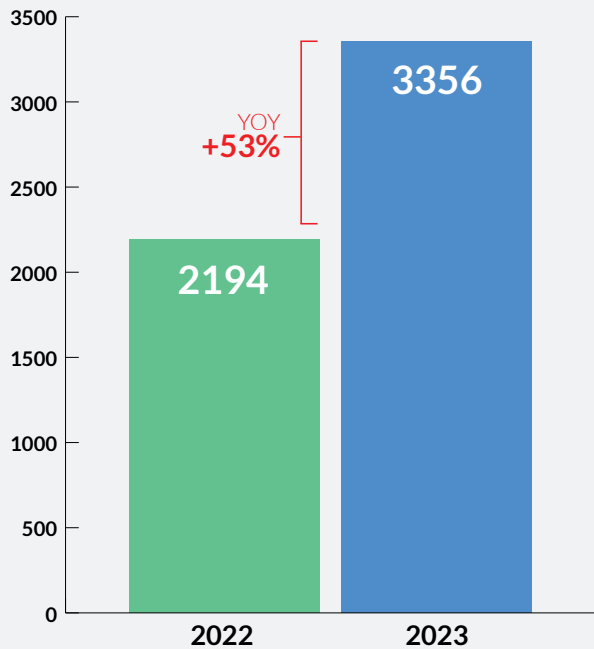


2. Cost Reduction.

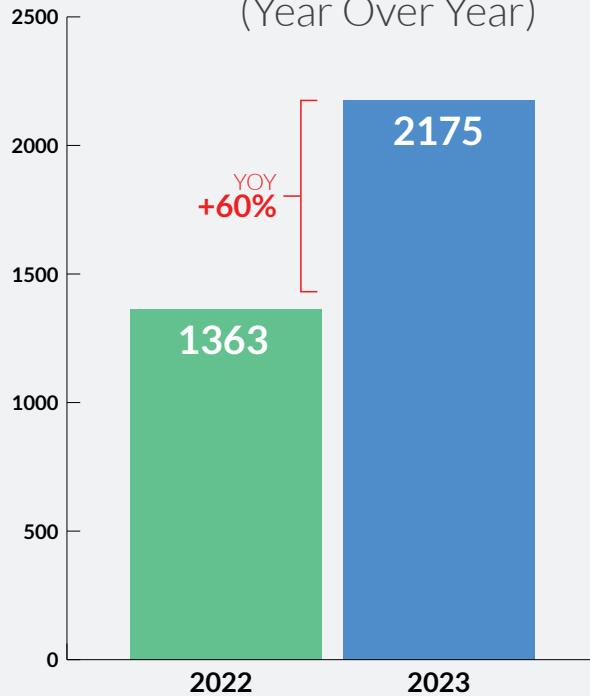
While investing in robust cybersecurity measures is essential, a TPRM approach can lead to more effective resource allocation and cost reduction. Reactive incident response and recovery can be costly and disruptive to business operations. By proactively managing risks and preventing incidents through TPRM, organizations can minimize the financial and reputational impact of cyberattacks. Moreover, TPRM helps organizations avoid potential legal and regulatory penalties resulting from third-party breaches, which can lead to significant financial consequences. By mitigating risks before they materialize, businesses can achieve cost savings and redirect resources to strategic security initiatives.



New Shared Assessments (Year Over Year)



New Accepted Assessments (Year Over Year)

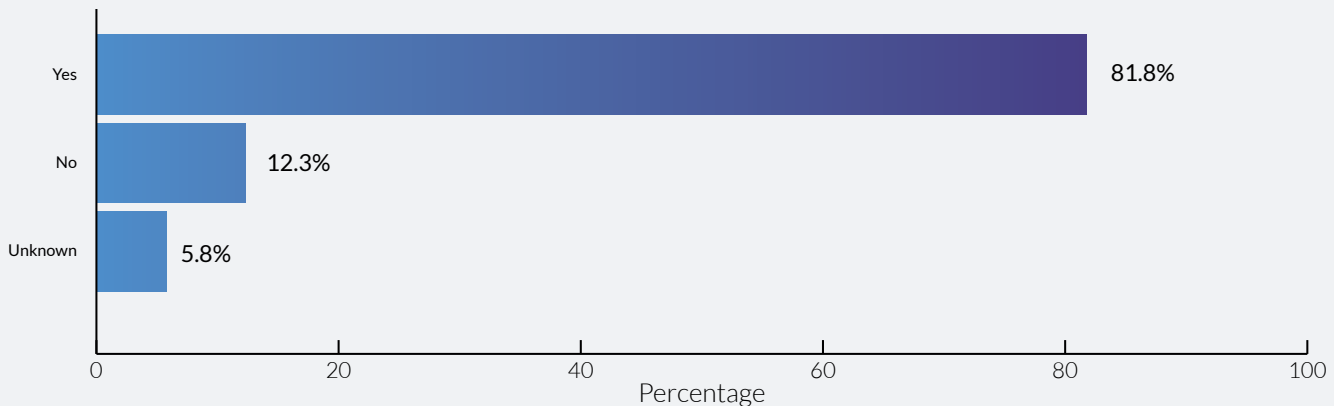


Data from the CyberGRX Exchange shows more companies are realizing the value of a Risk Exchange and the “complete an assessment once, share it infinite times” model to eliminate redundancies in the process. As evidence, in H1 2023, new assessment shares increased by 53% compared to the same period the prior year, and the customer acceptance rate averaged 60%, with some third parties reporting an acceptance rate of 70% or greater. The time savings and efficiency gains are substantial—an assessment questionnaire that used to take weeks or even months to complete can now be shared instantaneously, reducing internal costs and accelerating business decisions for all parties involved.

3. Business Alignment.

A TPRM approach aligns cybersecurity efforts with broader business goals, emphasizing risk-based decision-making that considers the organization’s specific risk appetite and objectives. TPRM enables organizations to prioritize their security efforts based on the potential impact on critical business functions and sensitive data. This alignment enhances cybersecurity’s effectiveness and fosters a deeper understanding of the business value of security initiatives. Cybersecurity becomes integral to strategic planning and decision-making by demonstrating how TPRM can safeguard key business processes and protect the organization’s reputation. Furthermore, TPRM helps build trust with stakeholders, including customers, investors, and partners. Demonstrating a commitment to robust cybersecurity practices in the extended supply chain instills confidence and reinforces the organization’s brand reputation. This enhanced trust can open new business opportunities and strengthen existing relationships, translating into a competitive advantage in the market.

Are You Able to Quantify and Communicate the Value of Your TPRM Program?



The business case for adopting a TPRM approach to cybersecurity is evident. In fact, among organizations surveyed, over 81% were able to quantify and communicate the value of their TPRM program to business leaders and stakeholders. With process improvement, cost reduction, and business alignment at its core, TPRM empowers organizations to proactively manage cyber risks, fortify their resilience, and achieve better business outcomes. As the digital landscape continues to evolve, embracing TPRM is not just a prudent choice but an essential step toward securing a successful and sustainable future for organizations in the digital age.

“We quantify the value of our risk management program in several ways: managing the risks associated with exposure to our various business units; regulatory compliance, which, because compliance isn’t optional, we don’t put a price tag on it; and the likelihood and potential financial impact to the organization based on various scenarios should an incident occur.”

A Global CISO

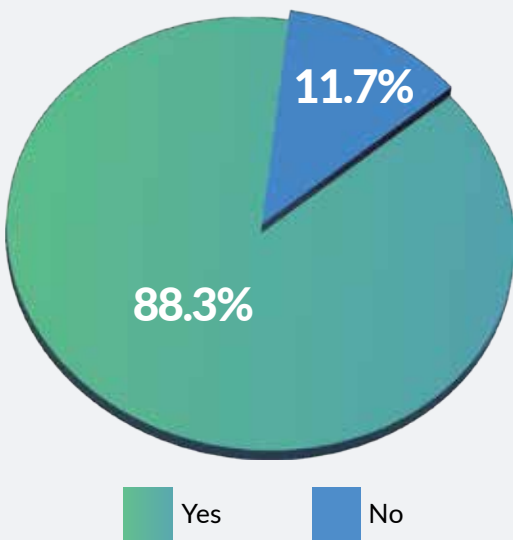
The Future of Third-Party Risk Management

The future of third-party risk management holds immense promise in reshaping the role of security within the organization, including the role of the Chief Information Security Officer (CISO) as a business enabler, while also enhancing organizational efficiency through reduced resources, automation adoption, and a heightened focus on core business objectives.

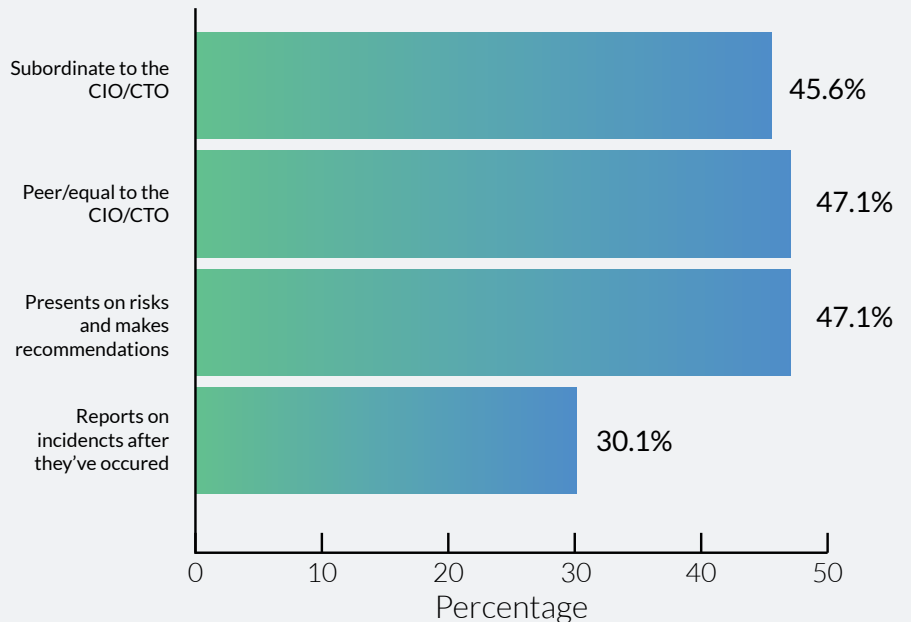
The Evolving Role of the CISO.

Traditionally seen as the “chief nerd” and the technical expert responsible for safeguarding an organization’s digital assets, the CISO’s role is set to advance with the widespread adoption of TPRM. Recent SEC rules brought the role of security chief as a critical member of the business leadership, and their place as a business leader will continue to expand and evolve. As cyber risks increasingly impact business operations and stakeholder trust, the CISO is empowered to assume a more strategic position within the organization. By actively engaging with the executive leadership and the board, the CISO can influence business decisions and ensure that cybersecurity is embedded in all aspects of the organization’s operations. This heightened visibility enables the CISO to champion cybersecurity as a business enabler, aligning security initiatives with overarching organizational goals and elevating the overall security posture.

Does your organization have a Chief Information Security Officer (CISO)?



You indicated that your organization has a Chief Information Security Officer (CISO). What role does the Chief Information Security Officer (CISO) hold within company leadership/Board of Directors?



Increased Organizational Efficiencies.

By implementing a comprehensive TPRM strategy, organizations can gain significant operational and organizational efficiencies. Proactively managing third-party risks minimizes the need for reactive incident response and recovery, resulting in reduced resource allocation to remediation efforts. TPRM enables businesses to focus on prevention and early intervention to generate cost savings and optimize resource utilization. Furthermore, as TPRM emphasizes a risk-based approach, cybersecurity efforts become more targeted and purpose-driven, which allows organizations to allocate resources to the most critical areas and reduce unnecessary expenditures.

Adoption of the Latest Technologies, Including Automation.

TPRM will embrace automation and other technological advances in the future, enabling organizations to streamline risk assessments, continuous monitoring, and compliance tracking processes. Automation reduces the manual effort required in managing third-party risks to enhance the speed and accuracy of risk evaluations. Moreover, automated risk scoring and reporting facilitate more informed decision-making, which allows the CISO and other business leaders to prioritize actions and allocate resources more effectively. As automation becomes integral to TPRM, organizations will gain greater agility in managing cyber risks and responding to emerging threats swiftly.

Greater Focus on Organizational Goals.

TPRM's risk-based approach directly aligns cybersecurity efforts with an organization's overarching objectives. By understanding the potential impact of third-party risks on business functions, the CISO and security teams can proactively tailor their strategies to protect core business processes and sensitive data. As a result, TPRM fosters a deeper integration of cybersecurity into the organization's DNA, instilling a culture of security awareness and responsibility among all employees. With TPRM supporting the achievement of organizational goals, cybersecurity is elevated from a cost center to a strategic enabler of growth and innovation.

Employee awareness training and developing the cybersecurity maturity of your employees is the most efficient and effective control you can have. Nothing is more valuable than an employee who thinks twice before clicking on a malicious link or disclosing information that they shouldn't.

A Global CISO

Conclusion

The transformation of cybersecurity from a cost center to a strategic business enabler through a third-party risk management approach holds significant potential for organizations seeking to thrive in the digital age. The current state of cybersecurity, with its reactive and siloed nature, leaves businesses vulnerable to emerging threats. Organizations lack comprehensive visibility into their risk landscape. However, by embracing TPRM, organizations can proactively manage cyber risks that external partners and suppliers pose, fortifying their resilience and aligning cybersecurity efforts with core business objectives.

The business case for TPRM highlights the advantages of process improvement, cost reduction, and business alignment. By streamlining cybersecurity processes, proactively managing risks, and demonstrating a commitment to robust security practices, organizations can achieve cost savings, enhance stakeholder trust, and unlock new growth opportunities.

Looking to the future, TPRM is poised to revolutionize the role of the CISO, empowering them as business leaders who actively influence strategic decisions and ensure cybersecurity is a foundational aspect of the organization. As TPRM increasingly adopts automation and aligns with broader business goals, organizations will achieve greater efficiencies, optimize resource allocation, and maintain a dynamic security posture.

By fostering a culture of security awareness, mitigating risks before they materialize, and capitalizing on emerging opportunities, businesses can thrive amidst uncertainty and ensure a successful and secure future in the face of evolving cyber threats. As the interconnectedness of an organization grows, the importance of TPRM will continue to rise, making it an indispensable component of a comprehensive cybersecurity strategy.

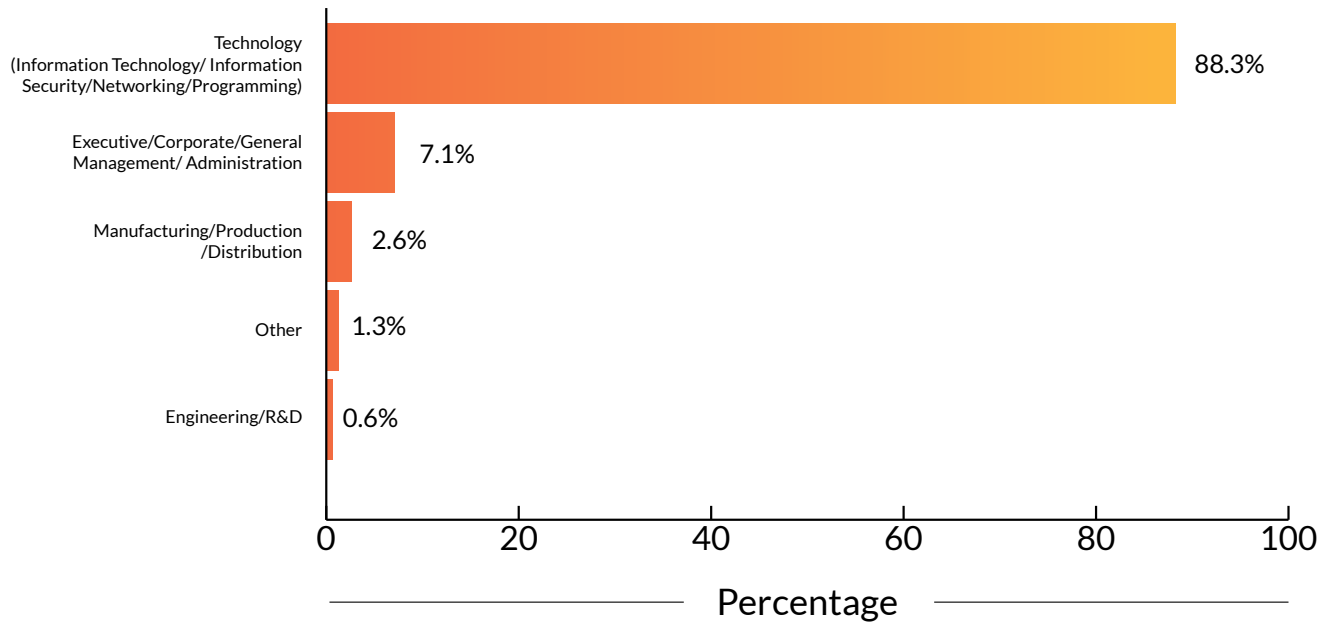


Methodology

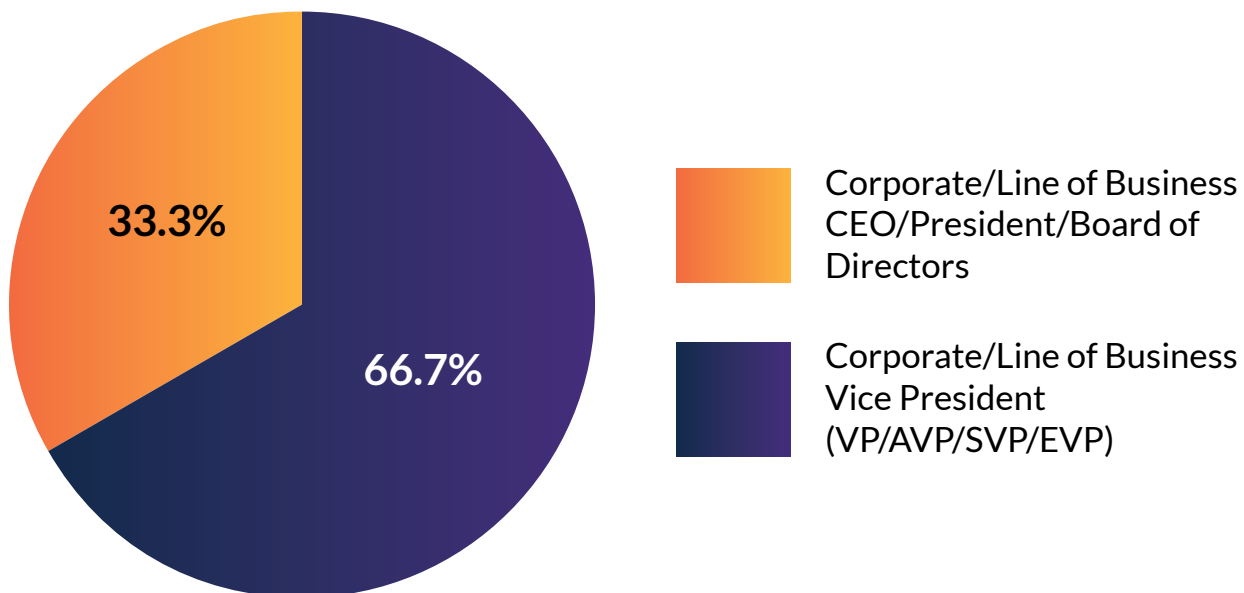
This survey was conducted in June 2023 by Enterprise Management Associates (EMA) on behalf of CyberGRX and ProcessUnity. 154 business professionals working in Information Technology, Information Security, Networking, and Programming participated in the survey, with a select group also participating in in-depth phone interviews. Participants were from organizations with at least 500 employees; 99% were in North America and 1% in EMEA.

A breakdown of the survey participants is as follows:

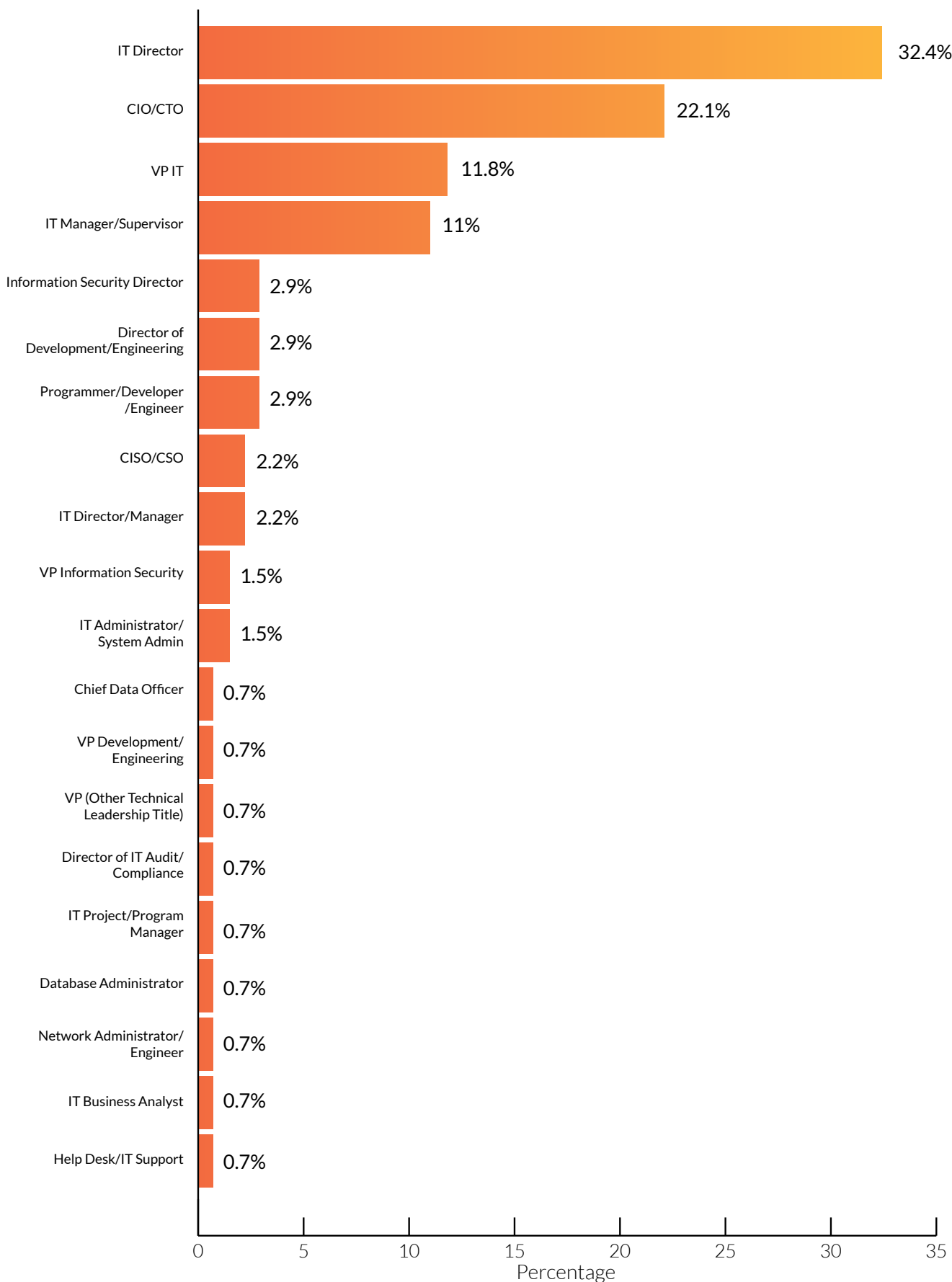
Department or functional area:



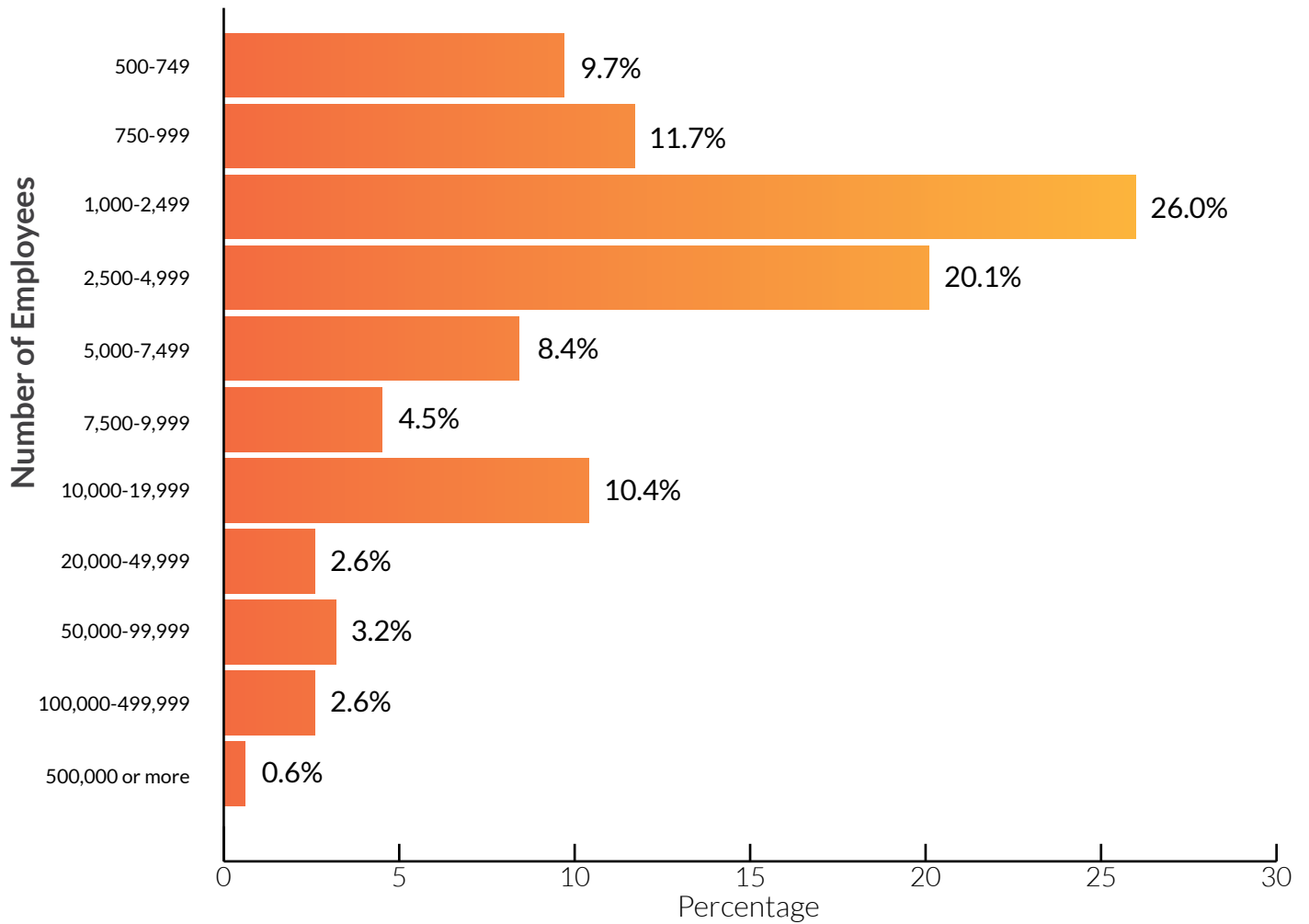
Functional role:



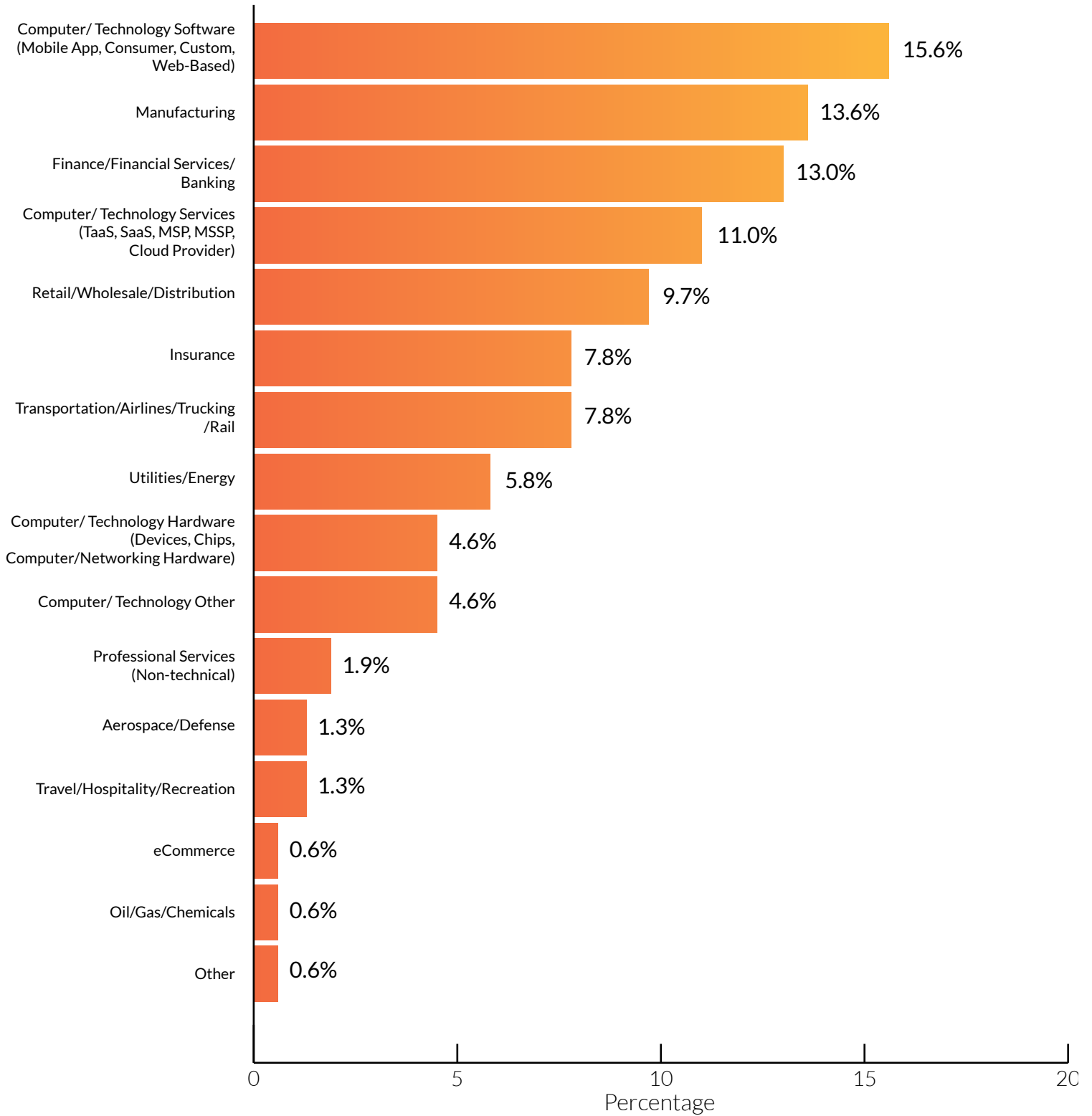
Specific Title:



Number of employees in the organization:

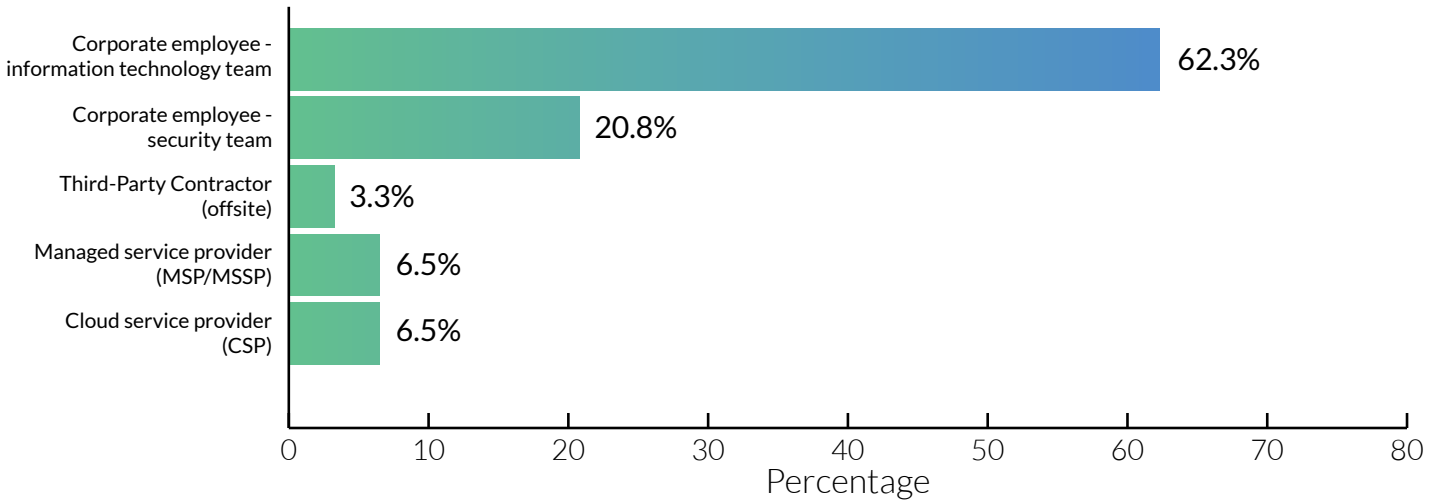


Industry:

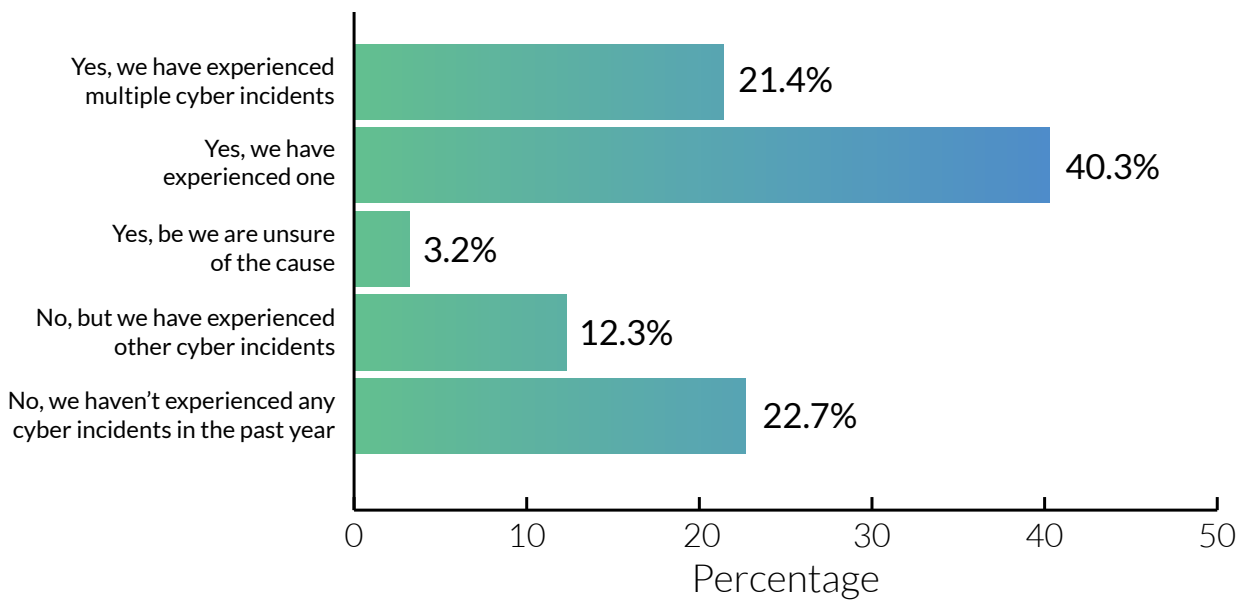


Survey Questions and Responses

Who Provides Security Administration for Your Organization?



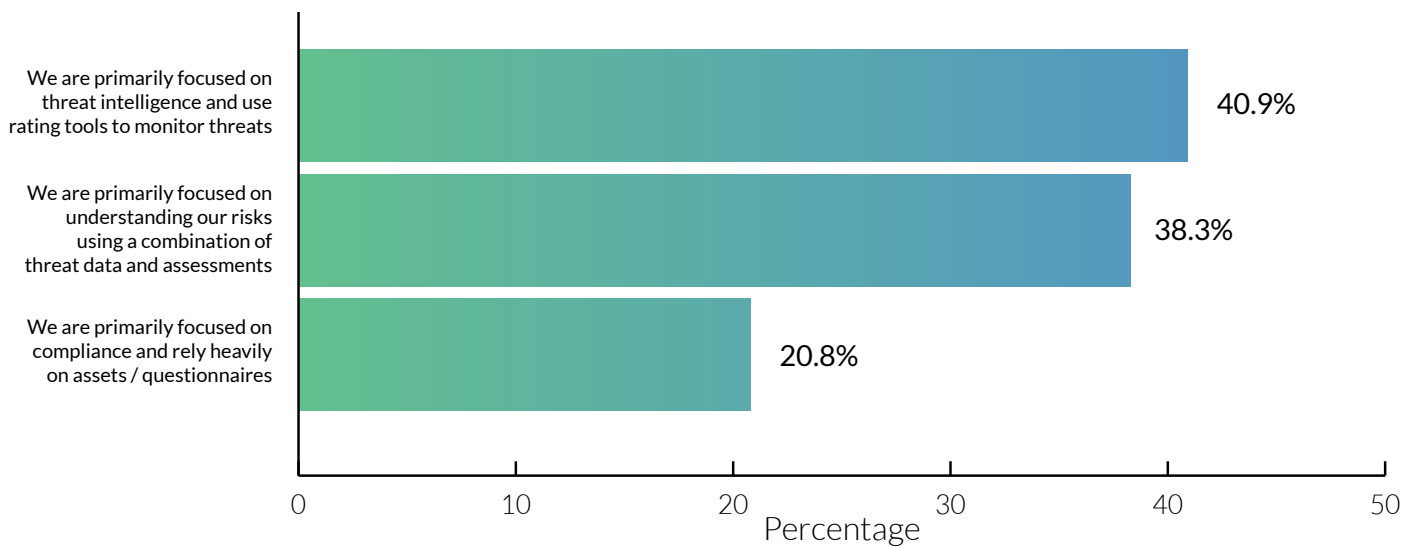
Has Your Organization Experienced a Cyber Incident in the Last Year Linked to a Third Party?



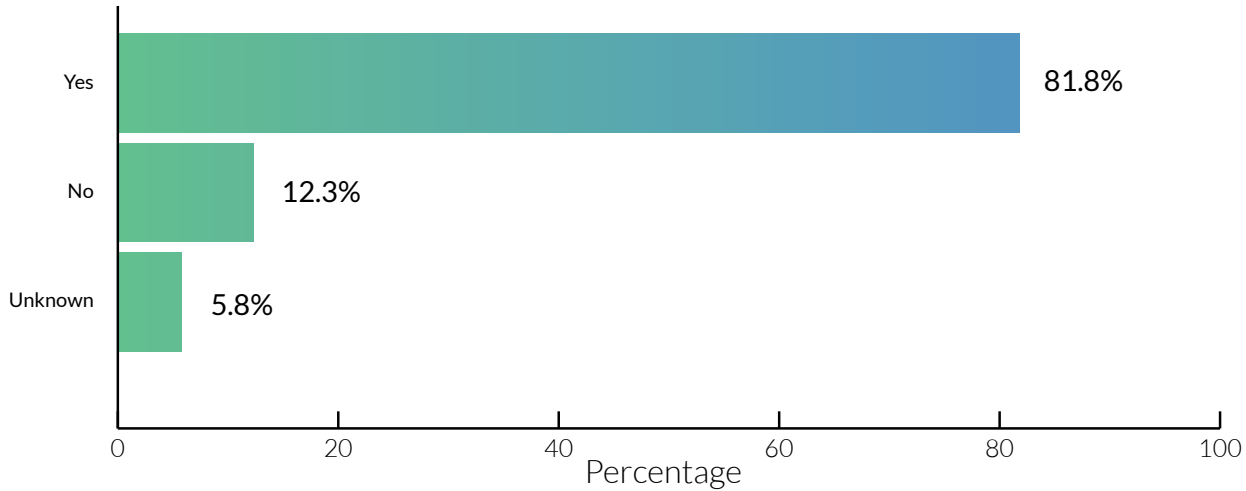
True or False Statements regarding TPRM Processes

	True	False	Unknown
My organization has identified and maintains a list of critical information assets (repositories)	94.8%	3.9%	1.3%
My organization has identified and maintains a list of critical people, business processes, and technology (including databases and code)	91.6%	7.1%	1.3%
My organization consistently measures dependencies on key suppliers, including the geographies in which they operate	85.7%	12.3%	1.9%
My organization conducts a regular assessment of our third-party vendors	90.9%	5.8%	3.2%
Customers require my organization to complete a regular assessment of our operations and security controls and procedures	79.2%	20.8%	0.0%
My organization uses a third party to conduct assessments/audits/evaluations on our behalf of our third-party vendors	80.5%	18.2%	1.3%
My organization participates in assessments/audits/evaluations by a third party for our customers	84.4%	13.6%	1.9%

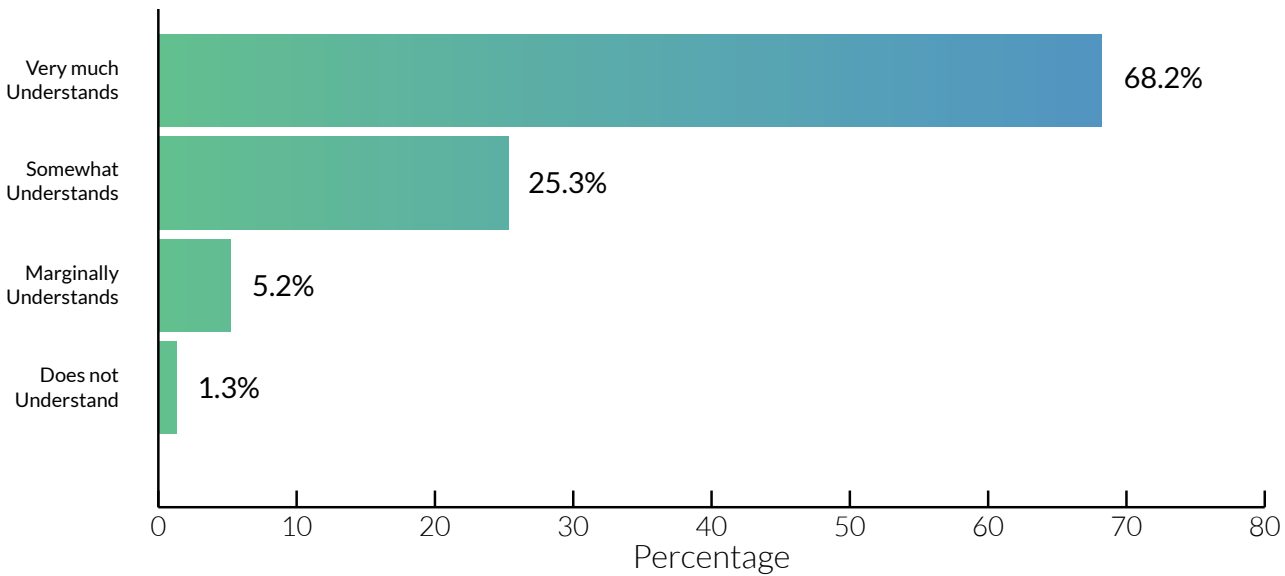
What is the Main Function of Your Third-Party Risk Management (TPRM) Program?



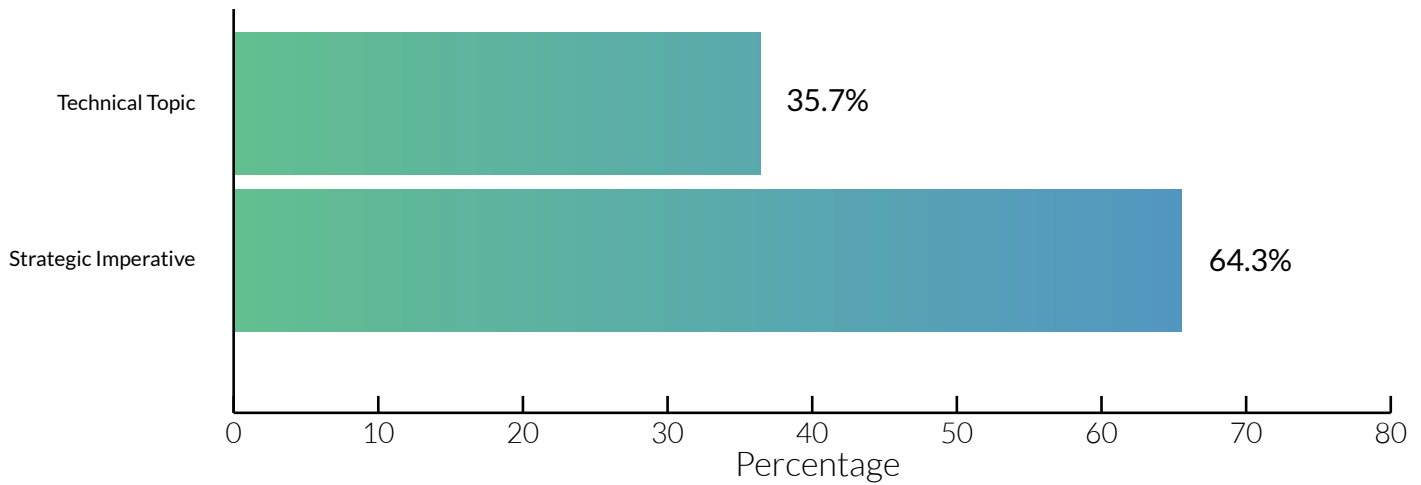
Are You Able to Quantify and Communicate the Value of Your TPRM Program?



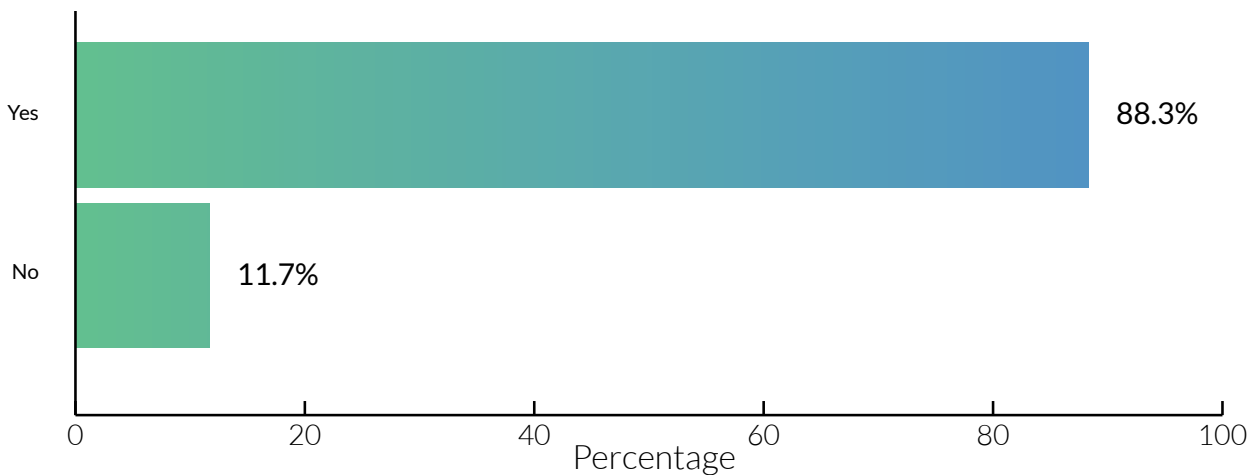
Do you feel that the Executive Management/Board of Directors of Your Organization Understands the Importance of Information Security?



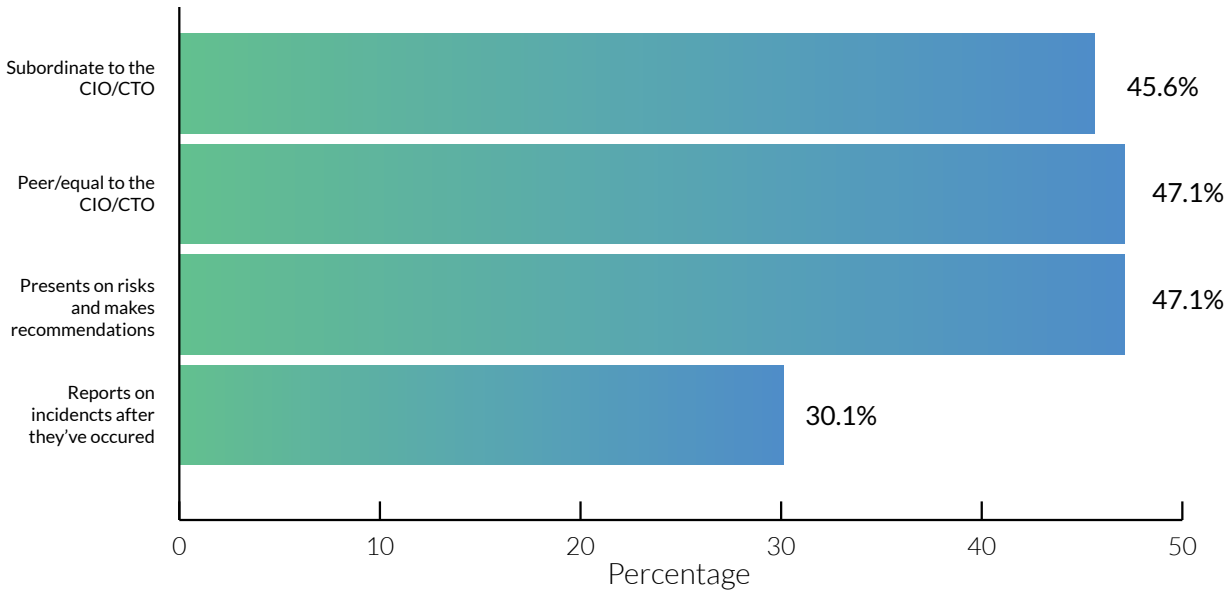
Is TPRM Viewed as a Technical Topic or an Organizational Strategic Imperative at the Board/C-Suite Level?



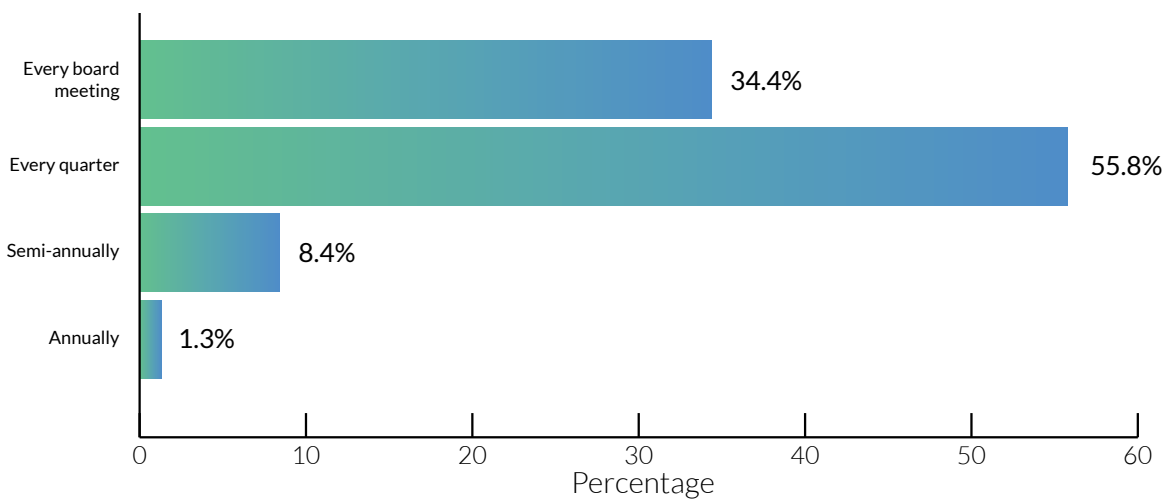
Does Your Organization have a Chief Information Security Officer (CISO)?



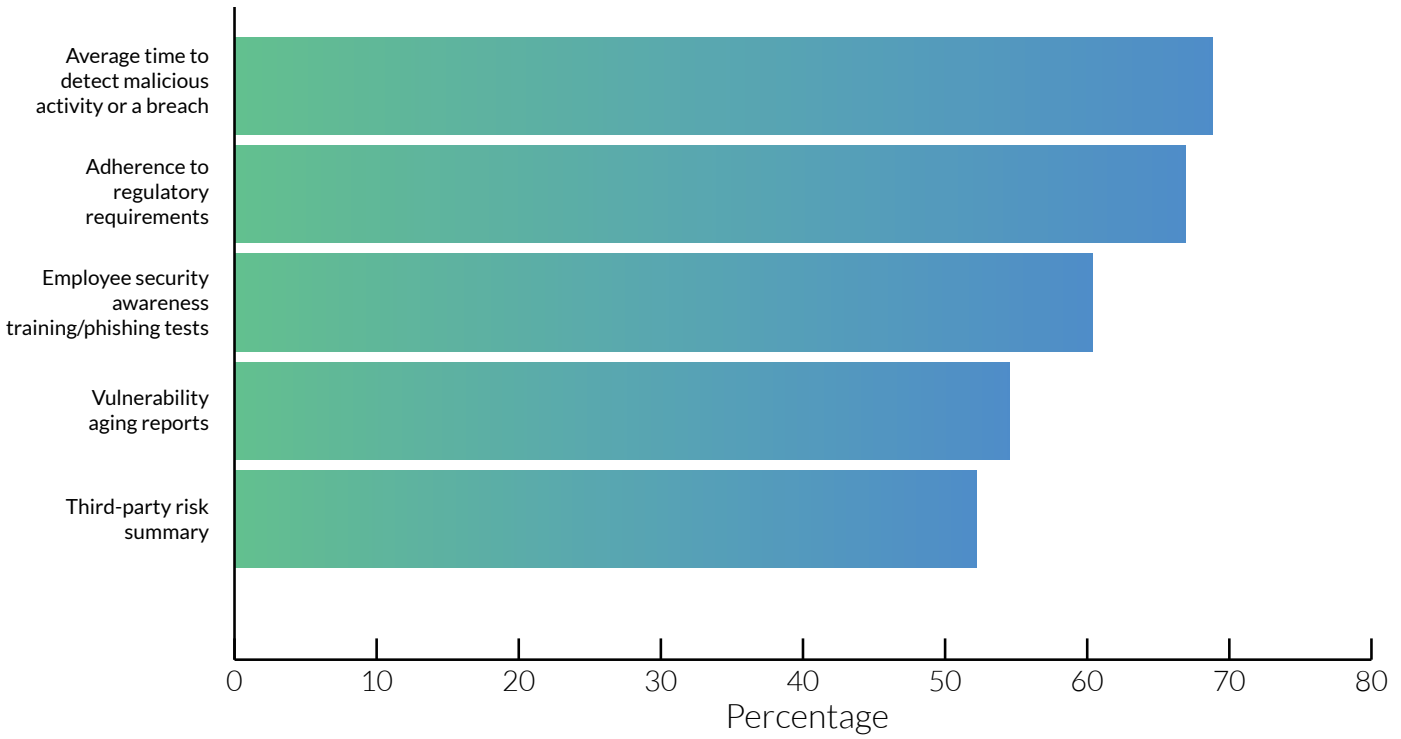
You Indicated that Your Organization has a Chief Information Security Officer (CISO). What Role Does the Chief Information Security Officer (CISO) Hold Within Company Leadership/Board of Directors



How Often Does Your Executive Team/Board of Directors Receive a Report on Security and Risk Management Program?



What are the Most Common Questions that Executive Management or the Board of Directors are Asking in Regards to Cybersecurity?





About CyberGRX + ProcessUnity

CyberGRX and ProcessUnity provides leading enterprises with comprehensive end-to-end cybersecurity and third-party risk management solutions. Fueled by the world's largest cyber risk exchange database, best-in-class workflow software, artificial intelligence, predictive analytics, and threat intelligence, CyberGRX and ProcessUnity enables organizations to quickly identify security gaps, reduce vendor onboarding and offboarding time, and proactively mitigate first- and third-party risks. As a result, organizations can more effectively safeguard their critical assets while lowering program costs. CyberGRX and ProcessUnity is trusted by major brands around the globe and is backed by Marlin Equity Partners. Learn more at [CyberGRX.com](https://www.CyberGRX.com) & [ProcessUnity.com](https://www.ProcessUnity.com).