INFO~TECH RESEARCH GROUP | PRIORITIES REPORTS 2024

# SECURITY PRIORITIES 2024

# Responding to an evolving threat landscape

## With the constant shift in the threat landscape, it's important to ensure organizations are equipped with the necessary measures to proactively respond to changes.

As the security world continues to respond to the various changes in the threat landscape and the advancement of new technologies, organizations are focusing on improving their security posture to prepare for the future. The threat landscape has been exacerbated with the various attack vectors emerging, such as the increase in credential-compromise attacks and cloud exploitation. The increase in supply chain risks and rise in deepfakes also showcase the shift of threat actors to improve the sophistication of their attacks. Furthermore, the rising costs of ransomware and cyber insurance premiums coupled with the continuous talent shortage depicts the challenges of efficiently fighting against these threats. This adds to the growing complexities of the current threat landscape, which has been identified by cybersecurity professionals as the most challenging within the past five years.

The emergence of advanced technologies has also welcomed opportunities for organizations to explore unique approaches to respond to these challenges while also enhancing existing capabilities to better equip themselves with the right people, process, and technology. This includes assessing the ability to address the talent shortage through upskilling, establishing a foundation to implement AI technologies, and evaluating an organization's security risk management with respect to integrating with the enterprise. Furthermore, the increased interest in zero trust adoption, coupled with the need for improving process efficiencies through automation, depicts the importance of continuous improvements through operationalization. This report explores the five priorities, along with the drivers and recommended actions, to help organizations be prepared to confidently address these security risks for 2024 and the years to come.

The average cost of a data breach in 2023 was USD 4.35M. Up 2% from 2022 and an increase of 15% from 2020.

Source: IBM, 2023

75% of cybersecurity professionals are viewing the current threat landscape as the most challenging within the past five years.

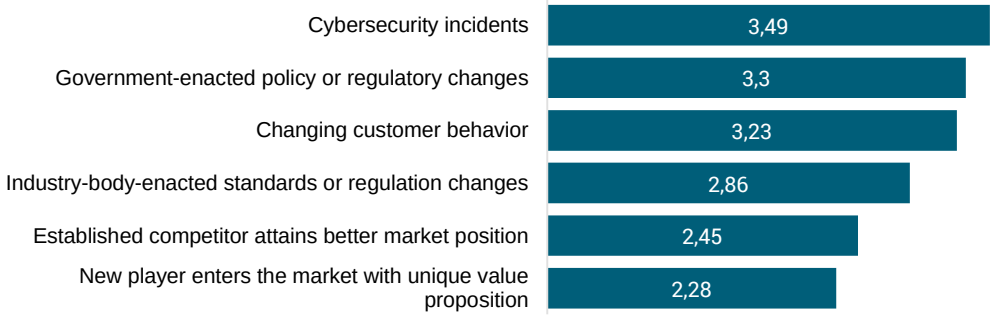
Source: ISC2, 2023; *N*=14,865

# Cybersecurity continues to disrupt the business

## Investment on cybersecurity is increasing due to its potential impact to the organization.

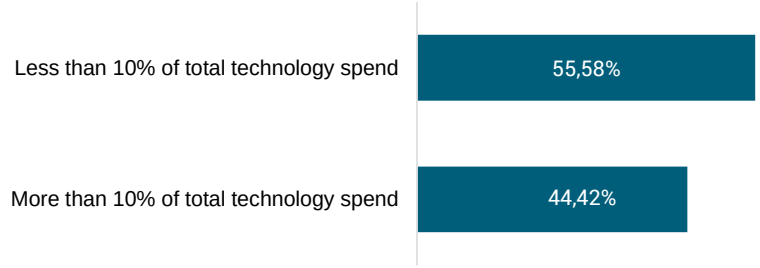
As part of our research process for the *Security Priorities 2024 Report*, we used the results from our Future of IT Survey, which collected responses between May 23 and August 22, 2023 (total *N*=894, with *n*=496 completed surveys). The survey highlights important technology trends and how organizations are addressing their opportunities and risks as well as their strategies for implementing the different technologies.

### FACTORS THAT WOULD DISRUPT THE BUSINESS WITHIN THE NEXT 12 MONTHS




Survey respondents (*n*=667) were asked what factors they anticipated would disrupt their organization within the next 12 months, ranging from 1 (smallest disruptor) to 5 (biggest disruptor). The number one disruptor was **cybersecurity incidents,** which was ahead of government-enacted policies or regulations and changing customer behavior. This indicates the growing importance organizations are placing on improving their security maturity, which would prepare them for any potential cybersecurity incidents.

### PERCENTAGE OF ORGANIZATION'S IT BUDGET SPENT ON CYBERSECURITY




Survey respondents *(n*=448) were asked about the percentage allocation of their IT budget spent on cybersecurity during the past fiscal year. **Fifty-five percent** of organizations indicated an allocation of less than 10%, while **44%** of organizations spent more than 10% of their IT budget on cybersecurity. Furthermore, **7%** of organizations indicated an allocation of more than 20% of their technology spend was on cybersecurity.

# Organizations understand the importance of adopting AI

## But what is the overall perceived impact to the organization?

The evolution of AI during the past few years has resulted in organizations learning more about the technology, its capability, and the importance of assessing its potential impact to the business. This notion was posed in a question in the Future of IT Survey, where organizations were asked what potential overall impact they expect AI to have.

### OVERALL IMPACT OF AI TO THE ORGANIZATION


Source: Future of IT Survey, *n*=500

Over **55%** of organizations expect a **positive** impact from AI and were more optimistic in the benefits it will bring to the business. Likewise, only **5%** of organizations expect a negative impact from AI and consider how it could be challenging and pose a threat to their business model. Irrespective of the impact, it's evident that the evolution of AI will continue to grow, and organizations should be prepared to secure the evolution through efficient investment in people, process, and technology.

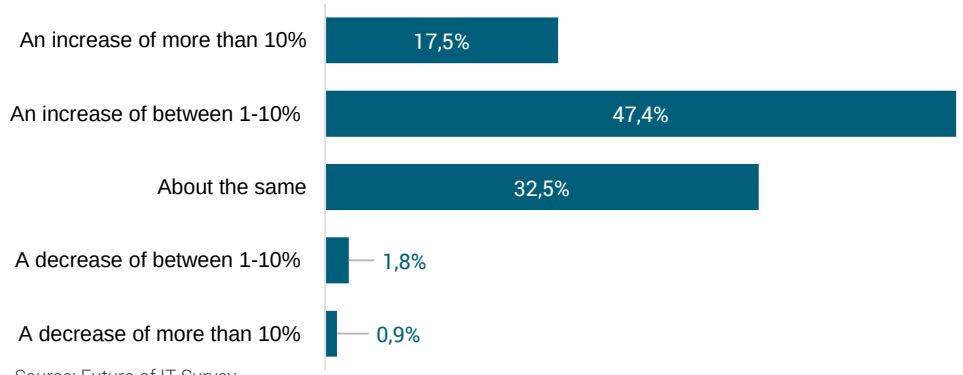
30% of organizations are currently leveraging AI to help automate repetitive, low-level tasks, and 37% are planning to use AI in 2024.

Source: Future of IT Survey, n=333

# Increase in investments to combat the growing threat landscape

Although a recession was anticipated in 2023, organizations are still looking into increasing their investments for the coming year and ensuring they have the resources to securely grow their business.

## EXPECTED ORGANIZATIONAL SPENDING ON CYBERSECURITY COMPARED TO THE PREVIOUS FISCAL YEAR

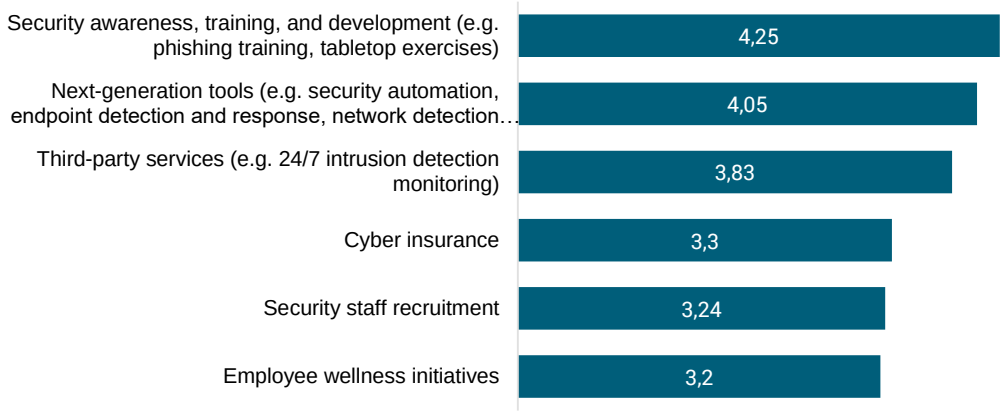



Source: Future of IT Survey

Survey respondents (*n*=452) were asked how they anticipated their organization's spending on cybersecurity will change compared to the previous year. Over **60%** of organizations anticipate an increase in their cybersecurity spending for next year, which was a ten-point increase from last year's response (53.4%).

Furthermore, only **32%** of organizations anticipate a similar budget to last year, which was a nine-point decrease from last year's response. This depicts how organizations are realizing the importance of cybersecurity spend and the need for increased investments that will allow them to stay competitive within their industry.

## CYBERSECURITY SPENDING PRIORITIES




Source: Future of IT Survey

Survey respondents (*n*=449) were asked how important the six cybersecurity initiatives were in terms of spending priorities. The number one priority was **security awareness and training**, followed by **next-generation tools** and **third-party services**. This shows the growing need and importance for investments in upskilling employees as well as technologies and services to assist organizations in maturing their security posture.

# THE FIVE SECURITY PRIORITIES FOR 2024

The evolving threat landscape and technology evolution has created a diverse set of security priorities your organization should focus on for the upcoming year.

| | | DRIVERS | |
|---|---|---|---|
| 01 | Develop and Optimize Your Cybersecurity Workforce | Talent shortage and cost of homegrown capabilities | Investment in long-term cost-saving initiatives |
| 02 | Secure the AI Revolution | Increased regulatory and market pressures for data security | Rising threat of deepfakes on organizations and their customers |
| 03 | Embed Security Risk Management With the Enterprise | Rising cost of cyber insurance | Increased supply chain risks |
| 04 | Operationalize Your Zero Trust Strategy | Continued rise of cloud exploitation | Increase in credential compromise-based attacks |
| 05 | Automate and Autonomize Your Security Processes | Rapid evolution of AI technologies | Increased frequency of ransomware attacks |

PRIORITY

01

# DEVELOP AND OPTIMIZE YOUR CYBERSECURITY WORKFORCE

How to strategically tackle the worker shortage gap through upskilling.

# Executive summary

## BACKGROUND

With the proliferation of technologies such as AI emerging in the security space and the constant changes to the threat landscape, many organizations are looking for different approaches to improve their security posture and prepare for the challenges to come. This includes developing a cybersecurity workforce that possesses the necessary competencies to meet organizational and industry demands. However, as the global workforce gap continues to increase by almost 13% from 2022, it is evident that the challenges of the talent shortage will remain eminent and that new approaches should be explored to meet demands (ISC2, 2023; *N*=14,865).

The opportunity to leverage in-house talent to develop your cybersecurity workforce would provide many benefits to the team and organization as a whole. The learning curve for a technical professional to transition into cybersecurity is low, hence they will possess the ability to be trained on and acquire key cybersecurity skills faster, relative to non-technical professionals. Furthermore, organizations upskilling their employees would avoid potential issues of new employees adapting to a new culture, since their current employees have assimilated into the organization and align with their mission and goals. Given the changes in the threat landscape and the demand for security professionals, optimizing your workforce through upskilling would provide not only immediate relief to the security demands but also a sustainable approach to grow and retain your in-house talent.

## CURRENT SITUATION (DRIVERS)

Talent shortage/cost of homegrown capabilities: Increase in talent shortage over the year exacerbates the issue of finding talent. **92%** of organizations report having a cybersecurity skills gap (ISC2, 2023; *N*=14,865).

Investment in long-term cost-saving initiatives: Investments in long-term cost-saving initiatives span into upskilling your employees to fill in the competency gaps. **58%** of worker shortages can be mitigated by upskilling key competency gaps (ISC2, 2023; *N*=14,865).

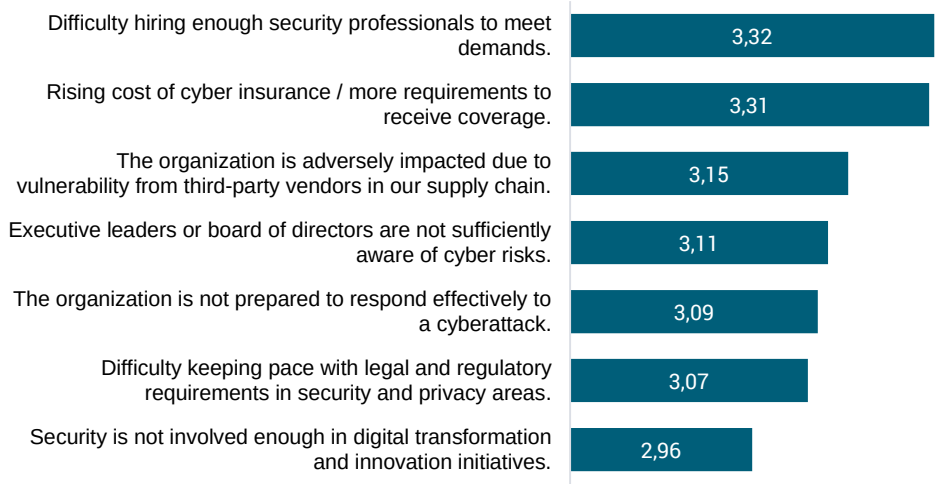
92% of organizations report having a cybersecurity skills gap, with 67% of the organizations indicating a skills gap as a greater threat than a worker shortage gap.

Source: ISC2, 2023

# Talent shortage is still a concern for organizations

Concerns may correspond to the increased demand in cybersecurity talent to combat the growing threat landscape.

## TOP CYBERSECURITY CONCERNS




Source: Future of IT Survey

Survey respondents (*n*=573) were asked how concerned they are about certain cybersecurity issues from 1 (not concerned at all) to 5 (very concerned). The number one concern was talent shortages. Other issues with similar concerns included the rising cost of cyber insurance and the impact of third-party risk.

Talent shortage is still the leading cybersecurity issue for the third year in a row in Info-Tech's Future of IT Survey, which shows the growing and continuous need for finding the right talent and building an innovative approach to bridging the gap. Although there has been some progress made during the past years in finding the right security talent, the constant concern indicates the need for an innovative approach that organizations should adopt to assist in mitigating the talent shortage gap. Finding the right talent could be closer than you think, as many organizations have employees whose skills and interest equips them with the necessary competencies to develop themselves into a cybersecurity professional.

**Fifty-two percent** of cybersecurity professionals began their career in a non-cybersecurity IT position (ISC2, 2023; *N*=14,865). This indicates an opportunity to leverage those transferable skills in a security role, which would enable organizations to stay competitive while also enabling continuous personal development for their employees.

Use this template to explain the priorities you need your stakeholders to know about.

# Develop and Optimize Your Cybersecurity Workforce

Provide a brief value statement for the initiative.

## Develop a strong cybersecurity workforce through optimizing your security team.

Description must include what organization will undertake to complete the initiative.

### INITIATIVE DESCRIPTION

- Define the competencies your organization needs to support the security program.
- Assess employees' current proficiency levels across defined competencies.
- Prioritize competencies against known organizational priorities.
- Acquire competencies through available learning and development tools and resources.
- Enable continuous improvement of employee proficiency by periodically reviewing your competency gaps.

List initiative drivers.

### DRIVERS

- Increase in talent shortage over the year exacerbates the issue of finding talent, as 92% of organizations report having a cybersecurity skills gap.
- Investments in long-term cost-saving initiatives span into upskilling your employees to fill in the competency gaps. 58% of worker shortages can be mitigated by upskilling competency gaps.

List initiative risks and impacts.

### RISKS

- Potential learning curve for employees in being upskilled to possess a competency that supports an organization's priorities and goals.
- Might not have employees who possess all of the desired competencies for an organization, so outsourcing and hiring would be an option.

List initiative benefits and align to business benefits or benefits for the stakeholder groups that it impacts.

### BENEFITS

- Reduce time and effort spent training new staff by leveraging the opportunity to upskill your existing technical staff.
- Acquire a diverse set of competencies that will give your organization a competitive edge as it navigates through the evolving threat landscape.

### RELATED INFO-TECH RESEARCH

- *Build a Plan to Close Your Cybersecurity Competency Gaps*
- *Build a Service-Based Security Resourcing Plan*
- Cybersecurity Workforce Development

# Recommended actions

## 1 IDENTIFY YOUR CURRENT COMPETENCY GAP AND ORGANIZATIONAL NEEDS

- Define the competencies your organization needs to support the security program.
- Assess employees' current proficiency levels across defined competencies.

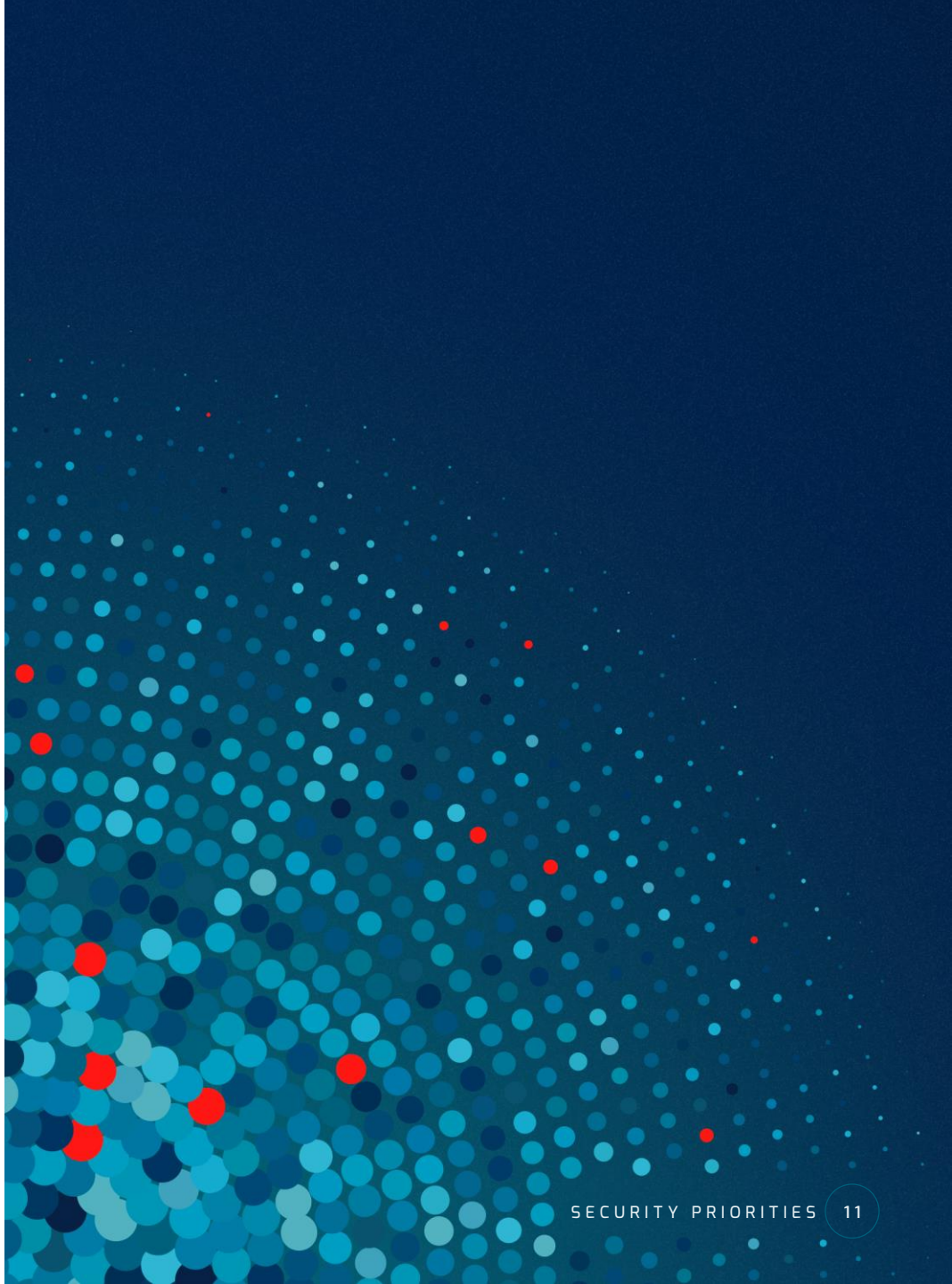
## 2 DEFINE YOUR CURRENT SECURITY RESOURCING PLAN

- Prioritize competencies against known organizational priorities.

## 3 DEFINE YOUR APPROACH FOR ACQUIRING THE COMPETENCIES

- Acquire competencies through available learning and development tools and resources.
- Enable continuous improvement of employee proficiency by periodically reviewing your competency gaps.

Source: *Build a Plan to Close Your Cybersecurity Competency Gaps*



PRIORITY

02

# SECURE THE AI REVOLUTION

Establish the right AI foundation to fight against AI-based threats.

# Executive summary

The rapid evolution of AI over the past few years has resulted in organizations assessing both the benefits of adopting the technology and the potential risks. These assessments have come at a time where government agencies are mandating responsible use of AI, such as the executive order by the US government on the safe, secure, and trustworthy use of AI. In addition to understanding the potential impact of the technology and the various stakeholders involved, it's important to ensure security is ingrained throughout the AI lifecycle, which will enable the efficient use of these technologies while also protecting against AI-based threats.

One of the first initiatives an organization should focus on when embarking on its AI journey is to develop the AI strategy and governance and make its alignment to the business' goals clear. Having a defined roadmap, which includes the people, process, technology, and security implications, in place would enable the development of a framework to build a responsible AI. This will allow organizations that are adopting AI technologies to have a structure in place to ensure the technologies leveraged are supporting the business goals and to assess the ethical and risk implications of their use.

## CURRENT SITUATION (DRIVERS)

**Rapid evolution of AI technologies:** The emergence of various AI technologies has enabled organizations to assess their ability to adopt these technologies, which will provide benefit to their business. **80%** of Fortune 500 companies have opened ChatGPT accounts within the first nine month of its launch (OpenAI).

**Increased regulatory and market pressures for data security:** Since the fuel for AI technologies is the data that is fed into it, organizations are doing their due diligence to ensure their data is secure while also assessing the opportunities to create further business by monetizing their data.

**Rising threat of deepfakes on organizations and their customers:** The creation of deepfakes through AI-generated content, coupled with the continued rise of social engineering attacks, depicts the potential threat of attackers becoming more sophisticated with their techniques to infiltrate an organization's systems and networks.

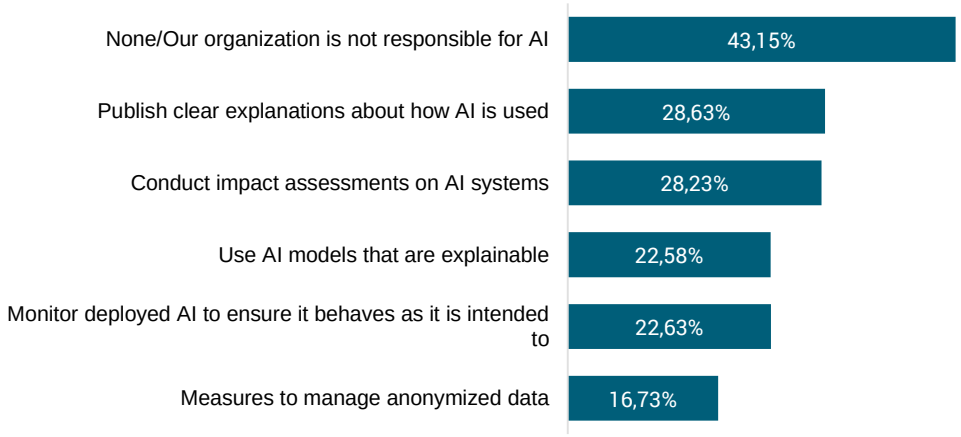
55% of organizations are already leveraging AI or are planning to use AI in 2024 to assist in identifying risks and improve their overall security posture.

Source: Info-Tech, Future of IT Survey

# Securing your organization's AI journey begins with establishing the right foundation

## Securing your AI revolution begins with careful management of the AI lifecycle to ensure the effective implementation of AI systems.

### AI GOVERNANCE STEPS ORGANIZATIONS CURRENTLY HAVE IN PLACE




Source: Future of IT Survey

Survey respondents (*n*=573) were asked what AI governance steps they currently have in place within their organization. Over **40%** of organizations don't have AI governance in place. Over **28%** of organizations have published clear explanations of its intended use of AI, while **28%** and **22%** of organizations are conducting impact assessments on AI systems and monitoring deployed AI systems, respectively.

As many organizations are working to leverage the power of AI, measures must be in place to ensure an effective adoption of the technology. Hence, establishing AI governance should be one of the initial initiatives within an organization's AI roadmap, to ensure a strong and ethical risk management framework is in place. With more than 40% of organizations indicating they have not yet established AI governance, there is great potential to develop and scale AI within the business, which starts with creating a foundation to manage, monitor, and control AI within the organization.

Implementing an AI risk management framework would ensure that there is sufficient oversight on AI systems and it effectively challenges AI's proposed use. The framework would also ensure risks are being evaluated throughout the lifecycle and its production is being monitored through assessments and audits. Having this structure in place before embarking on securing your AI journey would enable the creation of a methodology with defined processes for protecting your organization during these rapid changes while also maintaining a competitive edge within your industry.

Use this template to explain the priorities you need your stakeholders to know about.

# Secure the AI revolution

Provide a brief value statement for the initiative.

## Prepare your organization's adoption of AI by assessing the potential impact from a security perspective.

Description must include what organization will undertake to complete the initiative.

### INITIATIVE DESCRIPTION

- Identify your organization's initiatives and goals for leveraging AI and AI's alignment to the business goals.
- Assess your current security maturity and gaps that could be exploited by advanced AI-based threats and mitigated by leveraging AI technologies.
- Build a roadmap that will depict your organization's strategic approach in implementing the initiatives to support your AI goals.
- Identify the people, processes, and technologies required for the effective development, deployment, and monitoring of your AI initiatives.
- Formalize your AI governance framework to help define accountability and responsibility for AI, define your AI risk management, and establish metrics and KPIs to measure the success of your framework implementation.

List initiative drivers.

### DRIVERS

- The emergence of various AI technologies has enabled organizations to assess their ability to adopt these technologies, which will provide benefit to their business.
- There are increased regulatory and market pressures for data security to ensure their data is secure while also assessing the opportunities to create further business by monetizing their data.
- The threat of deepfakes on organizations and their customers is rising.

List initiative risks and impacts.

### RISKS

- Rapid changes in AI technologies require constant assessment of an organization's security posture and maturity to overcome potential challenges.

List initiative benefits and align to business benefits or benefits for the stakeholder groups that it impacts.

### BENEFITS

- Defined standards on how AI can be used and AI's alignment to business goals and compliance requirements.
- Improved understanding of AI-related risks and its applicability to your organization's use case.
- An established and iterative framework that will enable the management, monitoring, and control of all AI activities within an organization.

### RELATED INFO-TECH RESEARCH

- AI Research Center
- *AI Governance*
- *Address Security and Privacy Risks for Generative AI*

# Recommended actions

## 1 IDENTIFY YOUR ORGANIZATION'S AI GOALS

- Identify your organization's initiatives and goals for leveraging AI and AI's alignment to the business goals.

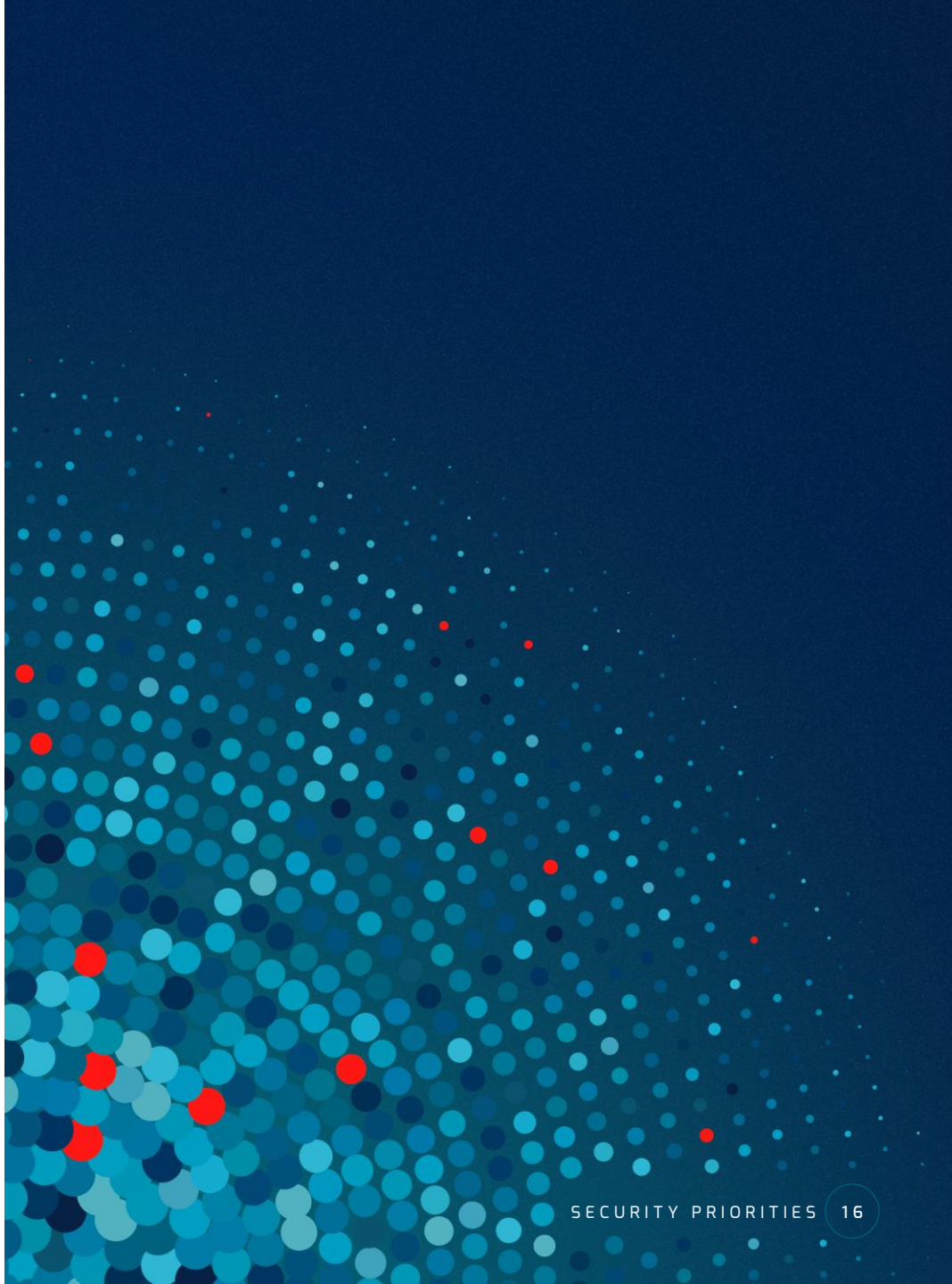
## 2 IDENTIFY YOUR SECURITY GAPS

- Assess your current security maturity and gaps that could be exploited by advanced AI-based threats and mitigated by leveraging AI technologies.

## 3 BUILD YOUR AI GOVERNANCE FRAMEWORK

- Build a roadmap that will depict your organization's strategic approach to implement the initiatives that will support your AI goals.
- Identify the people, processes, and technologies required for the effective development, deployment, and monitoring of your AI initiatives.
- Formalize your AI governance framework to help define accountability and responsibility for AI, define your AI risk management, and establish metrics and KPIs to measure the success of your framework implementation.

Sources: AI Research Center, *AI Governance*



PRIORITY

03

# EMBED SECURITY RISK MANAGEMENT WITH THE ENTERPRISE

Reframe both cybersecurity risk and vendor risk into a context that the enterprise can understand and appreciate.

# Executive summary

## BACKGROUND

Organizations are making increased use of cloud and third-party service providers. As the desire for the use of AI increases, reliance on third-party vendor platforms and capabilities will grow exponentially as the technology rapidly evolves. Reliance on vendors means information sharing between parties and greater CISO accountability for the protection of the organization's information assets. Information security risk management has not traditionally been elevated to the enterprise level. IT and information security leaders are inclined to manage security risks independently of enterprise risk management initiatives, which are primarily concerned with financial loss, service disruptions, and reputational damage. Reliance on third parties brings great value but can also pose great risk. Hence, it is time to elevate these risks to the enterprise level.

## CURRENT SITUATION (DRIVERS)

**Rising cost of cyber insurance:** Increased cost of cyber insurance has resulted in organizations identifying innovative approaches to better protect themselves from an attack. This could include outsourcing managed detection and response or leveraging AI capabilities to increase the organization's ability to automate cybersecurity defenses.

**Increased supply chain risks:** As many organizations are relying on third-party vendors to assist in the operationalization of their business, threat actors are finding ways to exploit the potential vulnerabilities of third-party vendors and attack their target through the weakest link first. **15%** of organizations identified a supply chain compromise as the source of their data breach. Furthermore, attacks caused by a supply chain compromise cost **11%** more and took **12%** longer to identify and contain than other breaches (IBM).

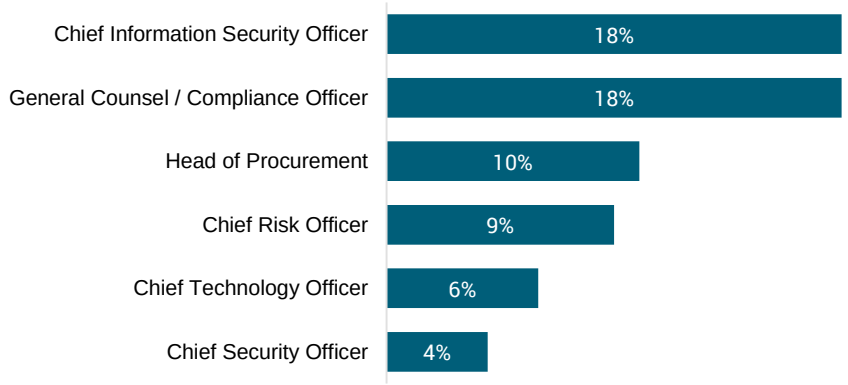
70% of organizations are carefully evaluating all third-party software on their network.

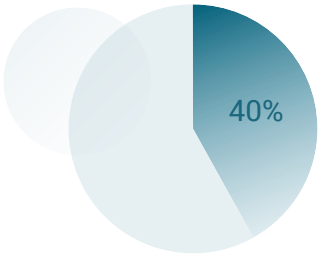
Source: ISC2, 2023

# Reliance on cloud and third-party vendors continues to increase

## And yet information security risk management continues to be managed in a vacuum.

### WHO IS MOST ACCOUNTABLE FOR THE CORRECT HANDLING OF THE ORGANIZATION'S THIRD-PARTY RISK MANAGEMENT PROGRAM?




Only **40%** of organizations report third-party risk to their board of directors.

Increasingly, organizations are leveraging cloud-based platforms and software-as-a-service solutions – all of which come with varying degrees of shared responsibility between provider and customer. In other capacities, they are outsourcing entire capabilities such as payroll, data processing, and managed IT and information security services to third parties. What's not happening to the same degree is a maturing of vendor risk management practices. In a September 2022 study by Ponemon Institute over half (**54%**) of the 1,164 surveyed IT professionals reported that they had experienced a data breach caused by a third-party vendor in the last 12 months. The same report also revealed that merely one third (**34%**) had confidence that they would be notified in the event that their vendor had experienced a breach.

In many organizations, the accountability of vendor risk seems to fall knowingly, or unknowingly, on the CISO, simply because of the role they play in the protection of the organization's sensitive information and assets. If this is to be the case, then information security risk management cannot afford to be managed in the same vacuum as conventional IT risk.

It's time to ensure that the information security risks are enterprise risks. It's time to elevate information security risk management to the enterprise level.

Source: Ponemon Institute, 2022;
*N*=1,164

Use this template to explain the priorities you need your stakeholders to know about.

# Embed security risk management within the enterprise

Provide a brief value statement for the initiative.

## Elevate your bolstered third-party risks and information security risks to the enterprise level.

Description must include what organization will undertake to complete the initiative.

### INITIATIVE DESCRIPTION

- Inventory all third parties with whom the organization shares important and sensitive information, and conduct an assessment of their security and data-handling practices.
- Implement a third-party policy review program.
- Confirm the contractual obligations for third parties to disclose security incidents and data breaches with their customers.
- Translate all vendor and information security risk reports into terms that are meaningful in an organizational context (disruption of service, loss of revenue, reputational damage, decrease in operational efficiency).

List initiative drivers.

### DRIVERS

- The increased use of cloud-based solutions and third-party vendor services increases information sharing between your organization and vendors.
- The organization's desire to leverage AI technologies to increasingly bolster its capability further increases the need to ensure that information-sharing risks are made visible at the highest level in the organization, not buried in the office of the CISO.

List initiative risks and impacts.

### RISKS

- The lack of access to a forum with which to present risk at an enterprise level is a common roadblock to this integration. The CISO must advocate for a voice or representation at the executive leadership or board level if this is not already a commonly accessed forum.

List initiative benefits and align to business benefits or benefits for the stakeholder groups that it impacts.

### BENEFITS

- Elevates the profile of information security risks, allowing for quicker action or mitigation strategies where needed.
- Ensures decisions about risk acceptance and mitigation are being made at the appropriate level.

### RELATED INFO-TECH RESEARCH

- *Proactively Identify and Mitigate Vendor Risk*
- *Build an IT Risk Management Program*
- *Combine Security Risk Management Into One Program*

# Recommended actions

## 1 ASSESS YOUR CURRENT THIRD-PARTY RISK MANAGEMENT

- Inventory all third parties with whom the organization shares important and sensitive information, and assess their security and data-handling practices.

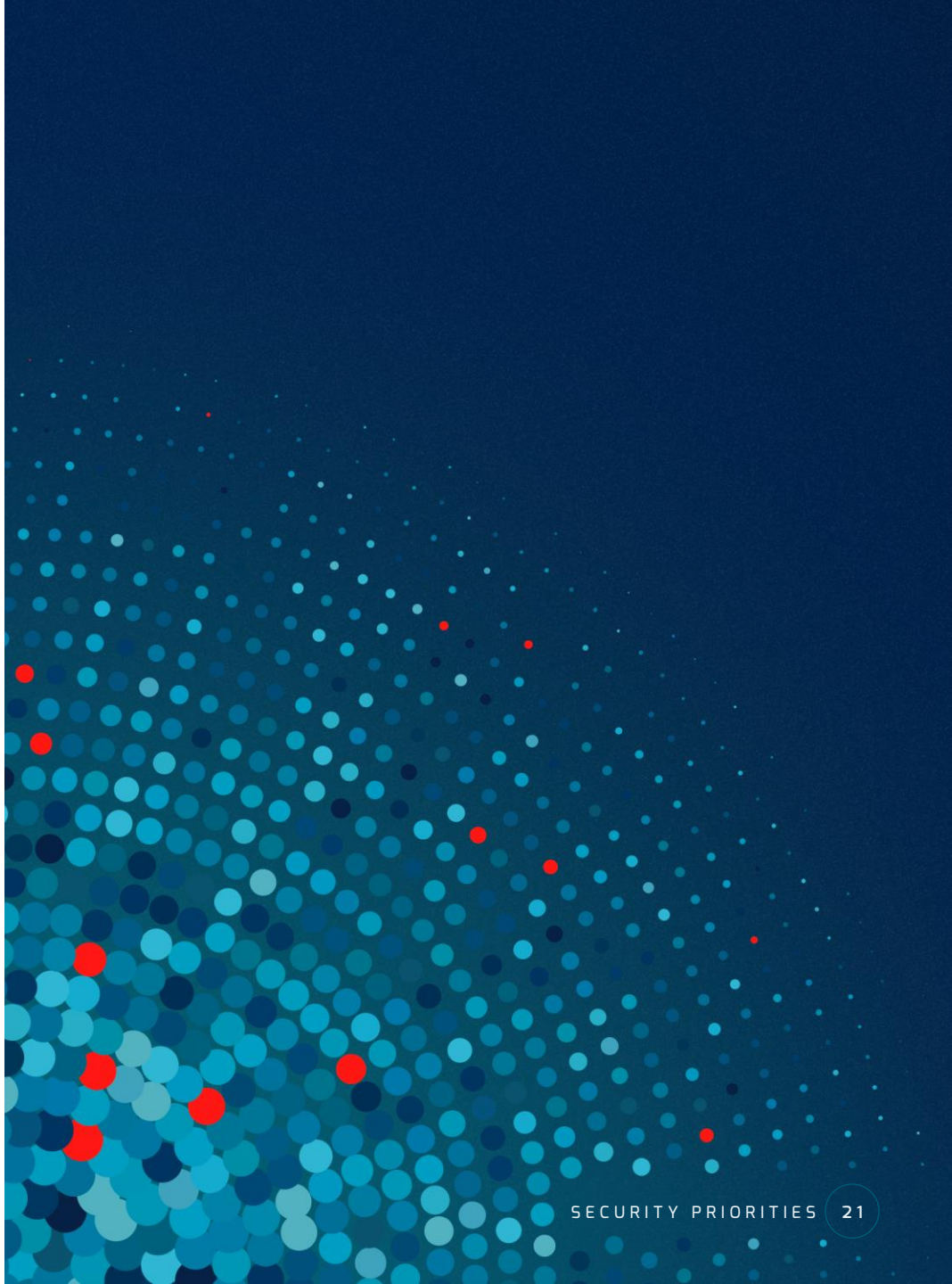
## 2 FORMALIZE POLICIES

- Implement a third-party policy review program.
- Confirm the contractual obligations for third parties to disclose security incidents and data breaches with their customers.

## 3 COMMUNICATE THIRD-PARTY RISK MANAGEMENT TO EXECUTIVE LEADERSHIP

- Translate all vendor and information security risk reports into terms that are meaningful in an organizational context (disruption of service, loss of revenue, reputational damage, decrease in operational efficiency).

Sources: *Combine Security Risk Management Components Into One Program*, *Exponential IT for Security and Privacy*



PRIORITY

04

# OPERATIONALIZE YOUR ZERO TRUST STRATEGY

Begin your journey by focusing on your most critical protect surfaces.

# Executive summary

## BACKGROUND

With the increase in sophisticated attacks through the advancement of technology and attack techniques, organizations are evaluating different strategies to protect their most critical assets. Adopting zero trust would improve an organization's security posture and support the business with its goals. Zero trust would assist in reducing an attacker's ability to move laterally within the environment, ensure least privilege access is enforced across critical resources, and reduce an enterprise's attack surface. Furthermore, the reduction in business and organizational risks along with compliance costs would ensure the organizational benefits of implementing this strategy.

However, as with any important security initiative, it is imperative to build a roadmap for implementing your strategies to ensure a process is in place to review your progress and identify opportunities for continuous improvement.

## CURRENT SITUATION (DRIVERS)

**Continued rise of cloud exploitation:** As many organizations continue to migrate their operations to a cloud environment, threat actors are becoming more "cloud-conscious" and expanding their threat vector to target cloud-based environments. **82%** of breaches involved data stored in the cloud or hybrid environment (IBM).

**Increase in credential compromise-based attacks:** The increasing shift away from malware-based attacks depicts the diversity and sophistication of methods attackers are using to infiltrate an organization's network assets. Over **70%** of incident detections were from malware-free activities (CrowdStrike).

15% of breaches occurred from stolen or compromised credentials, which was the second most common attack vector after phishing.

Source: IBM, 2023

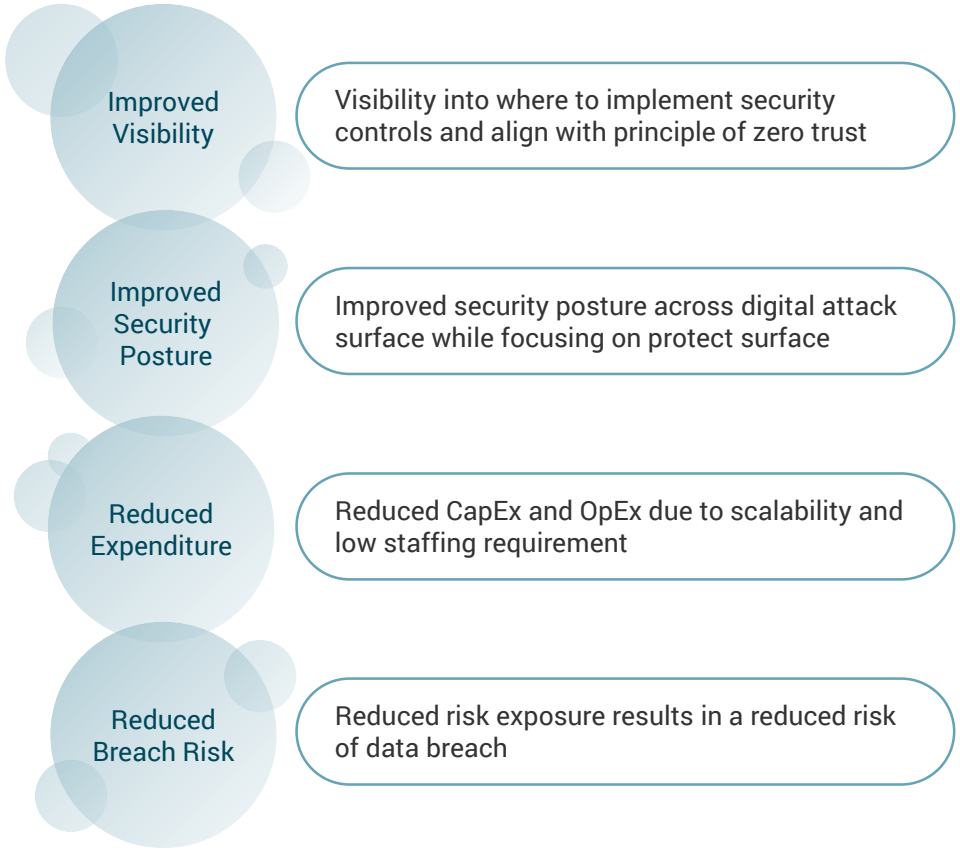
# Develop a roadmap to enable an iterative approach to your zero trust strategy

## Build an iterative and repeatable process for continuous improvement on your zero trust journey.

When building your zero trust roadmap, it's important to understand that the initiatives you are implementing should evolve through an iterative and repeatable process. This will ensure continuous improvement and an efficient deployment of your strategy, as you'll prioritize your most critical protect surfaces first. Implementing a set of principles such as least-privilege and per-request access enforcement will also minimize compromise to critical assets, which will reduce organizational risks and costs and enable compliance to regulatory standards. This will ensure organizations are obtaining the business benefits of this strategy while staying competitive and reducing their risk exposure.

Building your roadmap should begin by identifying your organization's objectives and how implementing your zero trust strategy will support the organization in achieving its goals. This includes defining your critical protect surfaces, which include your data, assets, applications, and services (DAAS) elements. By defining your protect surfaces and the alignment with your organization's objectives, you'll be able to effectively design your roadmap and develop and monitor the implementation of your strategy to ensure it is achieving your desired results. The changes in the threat landscape indicate the need for adopting a zero trust strategy and shifting our mindset from "when" we need to implement to "how" we can begin this journey. Given the sophistication of adopting this strategy, a step-by-step roadmap would assist organizations in developing an effective, measurable, and iterative strategy that would yield continuous improvement to the security posture and the organization's overall success.

### BENEFITS OF ZERO TRUST



Use this template to explain the priorities you need your stakeholders to know about.

# Operationalize your zero trust strategy

Provide a brief value statement for the initiative.

## Develop a practical zero trust roadmap that depicts the business value of a modernized security strategy.

Description must include what organization will undertake to complete the initiative.

### INITIATIVE DESCRIPTION

- Identify your business objectives and most critical protect surfaces, and map your protect surfaces to align with organizational goals.
- Design your roadmap by assessing key capabilities and identifying key processes and gaps to help build your strategy.
- Identify potential solutions and perform a cost/benefit analysis to prioritize your initiatives.
- Formulate your policies to ensure a secure path to access critical DAAS elements.
- Monitor the deployment of your zero trust roadmap through reporting, metrics, and collaboration with key stakeholders.

List initiative drivers.

### DRIVERS

- Stringent security requirements and the evolving threat landscape have resulted in an increased cost to cyber insurance premiums as well as a restriction in coverage.
- The increasing shift from malware-based attacks depicts the diversity and sophistication of methods attackers are using to infiltrate an organization's network assets.

List initiative risks and impacts.

### RISKS

- Potential steep learning curve in adopting the strategy, which would require a longer zero trust journey.

List initiative benefits and align to business benefits or benefits for the stakeholder groups that it impacts.

### BENEFITS

- Improved security posture across the digital attack surface.
- Reduced business risks through continuous verification of critical protect surfaces (identity, devices, network, applications, data).
- Achieves compliance with regulatory standards, which will improve audit results and reduce the risks of data breaches and other attacks.

### RELATED INFO-TECH RESEARCH

- *Build a Zero Trust Roadmap*
- Exponential IT Research Center

# Recommended actions

## 1 DEFINE YOUR ZERO TRUST STRATEGY

- Identify your business objectives and most critical protect surfaces, and map your protect surfaces to align with organizational goals.
- Design your roadmap by assessing key capabilities and identifying key processes and gaps to help build your strategy.

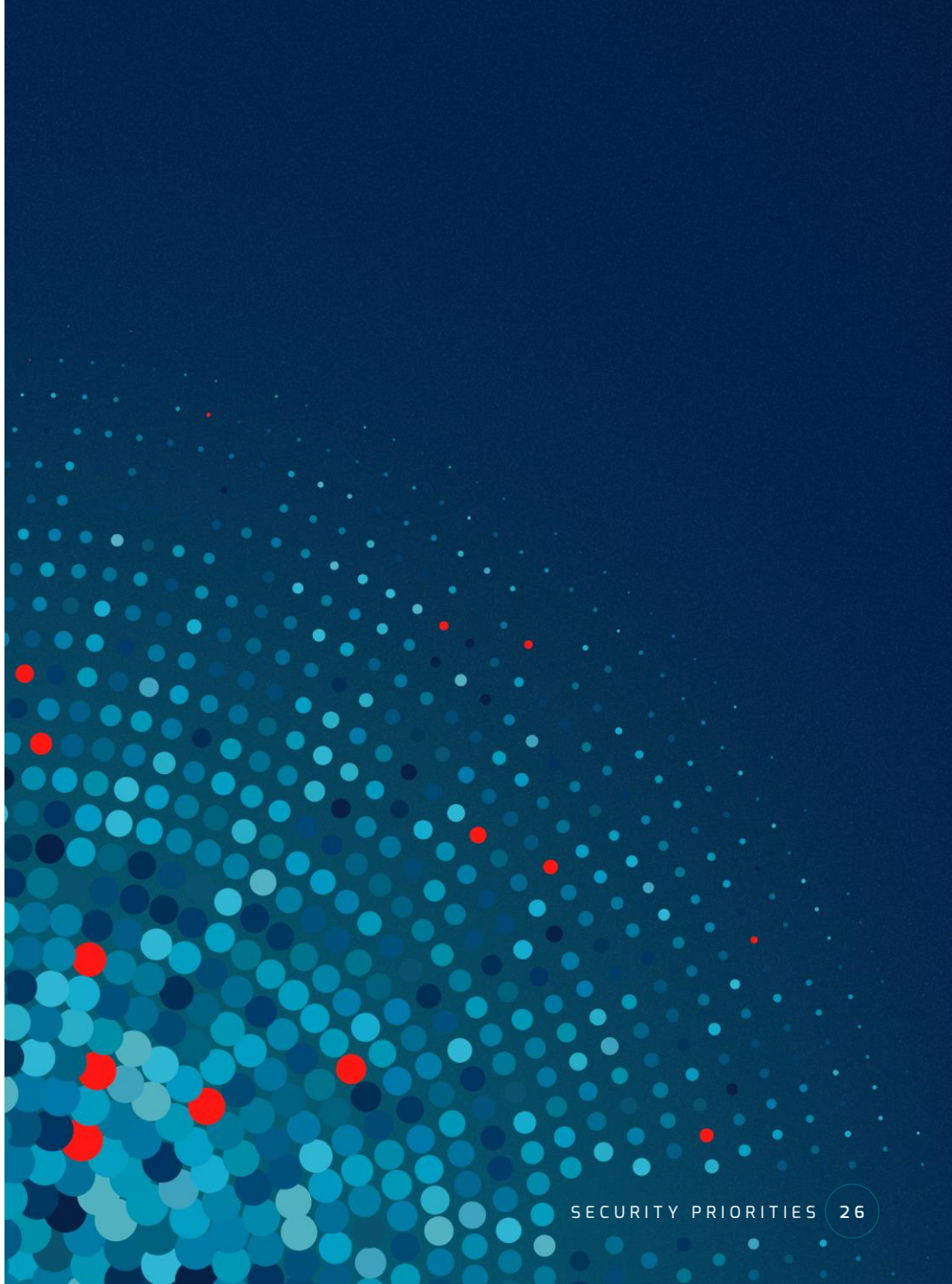
## 2 DEVELOP YOUR ROADMAP

- Identify potential solutions and perform a cost/benefit analysis to prioritize your initiatives.
- Formulate your policies to ensure a secure path to access critical DAAS elements.

## 3 MONITOR YOUR INITIATIVES TO IDENTIFY CONTINUOUS IMPROVEMENTS

- Monitor the deployment of your zero trust roadmap through reporting, metrics, and collaboration with key stakeholders.

Sources: *Build a Zero Trust Roadmap*



PRIORITY

05

# AUTOMATE AND AUTONOMIZE YOUR SECURITY PROCESSES

Prepare for an evolving threat landscape by streamlining your security process.

# Executive summary

## BACKGROUND

As the security landscape continues to evolve, organizations should assess their ability to streamline their security processes and efficiently defend against sophisticated threats while staying ahead of the technology curve. The need for security automation and autonomization will be more evident given the rise in automated and AI-based threats. Hence, identifying your automation initiatives requires the development of a roadmap to identify your automation goals, its value to the organization, and a strategy to achieve those goals. Having a solid management structure in place will ensure you have the right people, processes, and technology to achieve your automation goals.

Not all security processes need to be automated or autonomized, especially if there are potential risks involved with the streamlined process. Assessing your organizational needs and your security maturity level would help identify which initiatives can provide the most value while improving the efficiency, productivity, and quality of your security process.

## CURRENT SITUATION (DRIVERS)

**Rapid evolution of AI technologies:** The integration of AI capabilities within security solutions enables organizations to automate their security tasks, which will reduce costs and minimize time to identify and contain a breach.

**Investment in long-term cost-saving initiatives:** Investments in automation initiatives produces long-term cost savings given the sustainable return on investment it would provide from both a reduction in manual tasks and the mitigation of costs incurred from a cyberattack.

**Increased frequency of ransomware attacks:** The rise of ransomware as a service (RaaS) has made ransomware more accessible for threat actors, which still indicates the persistent threat of this attack vector.

61% of organizations are employing some level of security AI and automation, which delivered over USD 1.5 million in cost savings.

Source: IBM, 2023

# Begin by identifying the value of streamlining your security process

## It is important to identify which security processes should be automated or autonomized based on your organizational needs.

In a world where efficiency is of the utmost importance to stay competitive within an industry, automation is seen as an approach to improve efficiency across many areas while enabling continuous improvement. The enhanced protection provided through improved quality of alert triage, coupled with the reduction in compliance deficiency and improved cost efficiency, showcases the many benefits of this approach in protecting against an evolving threat landscape.

However, it is important to evaluate your organization's current security posture to assess your current state and define processes that would be streamlined through automation. This includes standardizing your processes through documentation and conducting a feasibility assessment to justify the resources required for these changes. This will ensure an organization is working toward reaching full automation across its various security processes to enhance security operations. An automation roadmap is an incremental journey where new challenges and opportunities might arise when automating a process. Ensuring continuous improvement within each process will allow for the efficient implementation of an automation roadmap, which will enable a more suitable, risk-free, and feasible strategy.

### AUTOMATION MATURITY STAGES

| MATURITY STATE | DEFINITION |
|---|---|
| Manual, Ad Hoc | Process is performed manually in an inconsistent manner |
| Manual, Standardized | Process is performed manually in a consistent manner because it was documented |
| Blended | Process is aided by some elements of automation |
| Automated | Process is fully automated, with human oversight for purpose of verification and orchestration |
| Autonomized | Process is fully autonomized, as there is no human interaction at all |

Sources: *Build an Automation Roadmap to Streamline Security Processes*

Use this template to explain the priorities you need your stakeholders to know about.

# Automate and autonomize your security processes

Provide a brief value statement for the initiative.

## Adopt recommended practices for streamlining your security processes.

Description must include what organization will undertake to complete the initiative.

### INITIATIVE DESCRIPTION

- Identify your automation goals and the current and target maturity states of your security process to identify gaps.
- Review your existing security process to identify which initiatives should be automated.
- Identify the suitability, value, and risks of each security process to prioritize initiatives to automate.
- Determine the feasibility of automating a security process by assessing the cost and benefits of each initiative.
- Develop your automation roadmap and ensure the initiatives are supporting your organizational goals.
- Communicate your automation roadmap to executive leadership to obtain support on your security automation objectives.

List initiative drivers.

### DRIVERS

- Integration of AI capabilities within security solutions enables organizations to automate their security tasks.
- Investment in automation initiatives enables cost savings, given the sustainable return on investment it would provide from both a process efficiency and cost mitigation perspective.
- Increased cyber insurance cost has resulted in organizations identifying different approaches to protect themselves, including automation.

List initiative risks and impacts.

### RISKS

- Potential increased reliance on automation, which might reduce critical domain knowledge.
- Potential process efficiency overload, where one solved process magnifies inefficiencies elsewhere.

List initiative benefits and align to business benefits or benefits for the stakeholder groups that it impacts.

### BENEFITS

- Increased process efficiency, which will improve response time to security incidents.
- Enhanced process quality, which will improve consistency and reduce errors.
- Increased process and staff productivity, which will increase throughput and free up resources to support critical initiatives.

### RELATED INFO-TECH RESEARCH

- *Build an Automation Roadmap to Streamline Security Processes*
- *Exponential IT for Security and Privacy*

# Recommended actions

## 1 ASSESS THE MATURITY OF YOUR SECURITY PROCESS

- Identify your automation goals and the current and target maturity states of your security process to identify gaps.
- Review your existing security process to identify which initiatives should be automated.

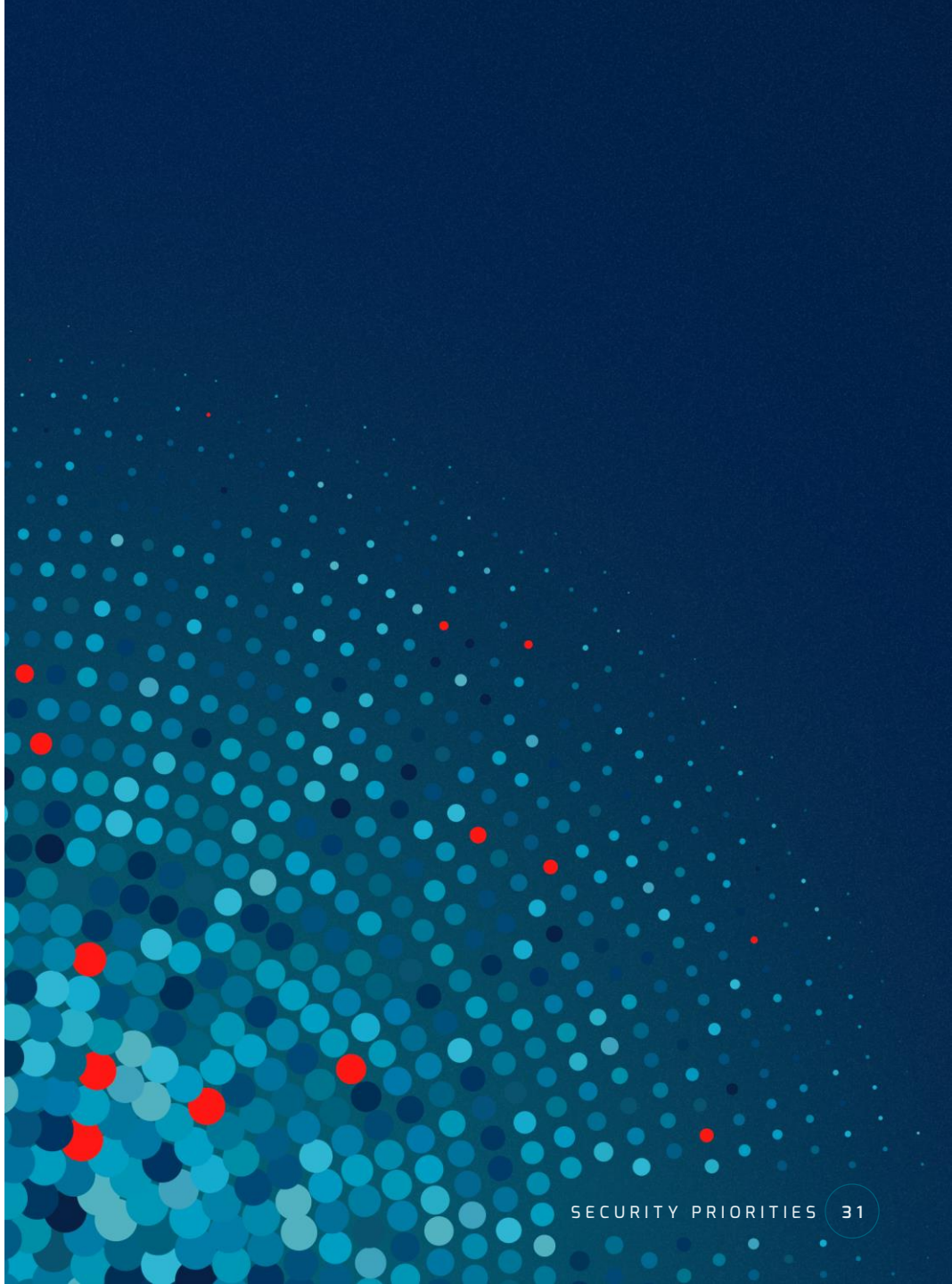
## 2 ASSESS THE VALUE, RISKS, AND FEASIBILITY OF THE AUTOMATION

- Identify the suitability, value, and risks of each security process to prioritize initiatives to automate.
- Determine the feasibility of automating a security process by assessing the cost and benefits of each initiative.

## 3 DEVELOP AND DELIVER YOUR AUTOMATION ROADMAP

- Develop your automation roadmap and ensure the initiatives are supporting your organizational goals.
- Communicate your automation roadmap to executive leadership to obtain support on your security automation objectives.

Sources: *Build an Automation Roadmap to Streamline Security Processes*



# Bibliography


"2023 Global Threat Report." *CrowdStrike*, 2023.

"Achieving Cybersecurity Success in Canada." *Bell*, Oct. 2023.

Beasley, Mark, Bruce Branson, and Bonnie Hancock. "The State of Risk Oversight." *AICPA*, April 2021.

"Cost of a Data Breach 2023." *IBM*, 2023.

"Cybersecurity Forecast 2024 Insights for Future Planning." *Google Cloud*, Nov. 2023.

"Executive Order on Improving the Nation's Cybersecurity." *The White House, The United States Government*, May 2021.

"Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." *The White House, The United States Government*, Oct. 2023.

"ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap." *ISC2*, Nov. 2023.

"Introducing ChatGPT Enterprise." *OpenAI*, Aug. 2023.

"Mandiant Cybersecurity Forecast 2023 Report." *Mandiant*, 2023.

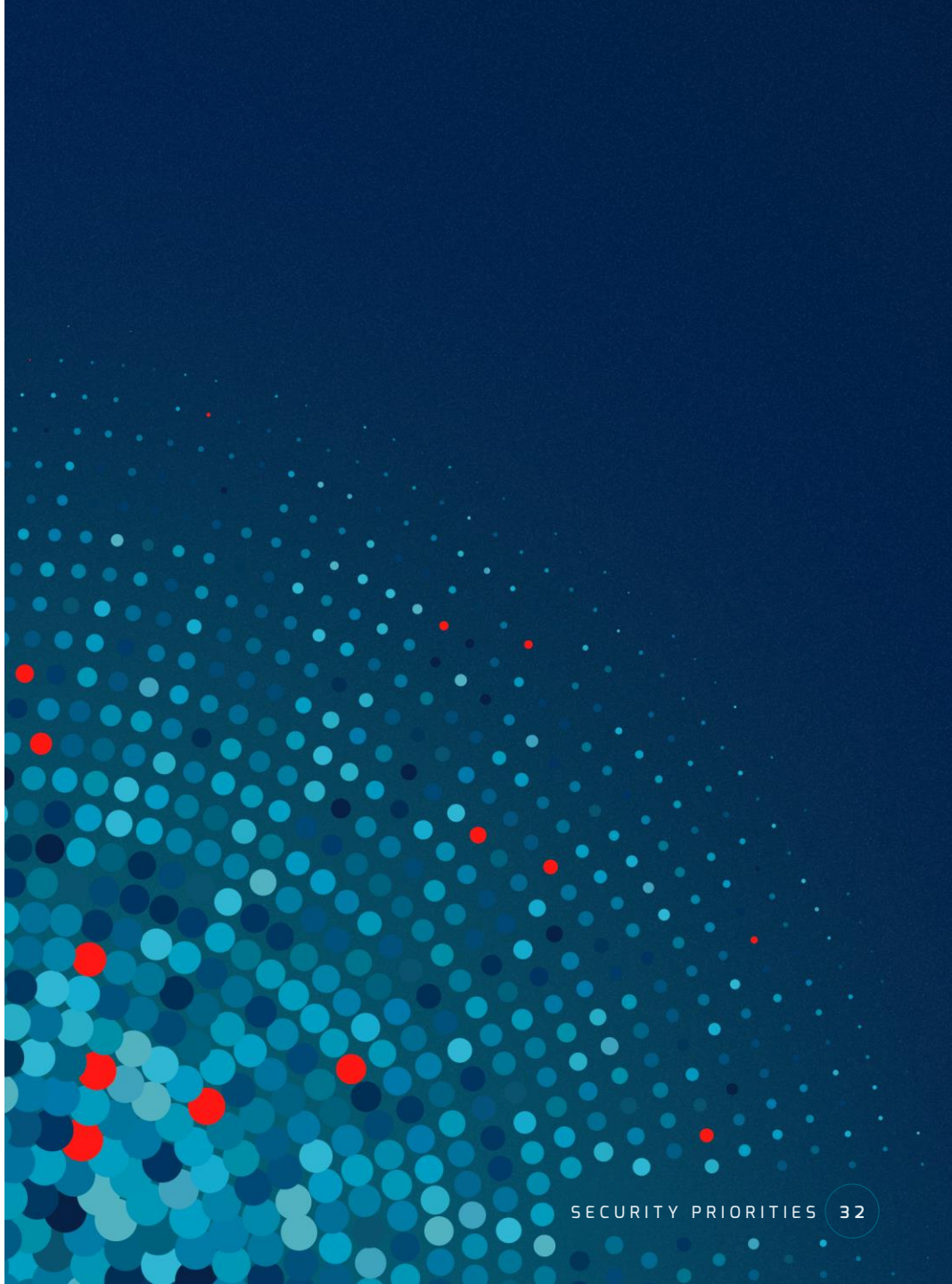
"National Cyber Threat Assessment 2023-2024." *Canadian Centre for Cyber Security*, Oct. 2022.

"Nine Surprising Stats about Vendor Risk Management." *Evantix Vendor Risk Management Blog*. Accessed 9 Nov. 2016.

"Ponemon Report: Data Risk in the Third-Party Ecosystem Study." *Ponemon*, 2022.

"Sophos 2023 Threat Report." *Sophos*, 2022.

"Threat Predictions." *Trellix*, Oct. 2023.

# Research contributors and experts

One anonymous contributor

894 respondents from Info-Tech's Future of IT Survey 2024