Barracuda
Your journey, secured.

APRIL 2024

The CIO report: Leading your business through cyber risk

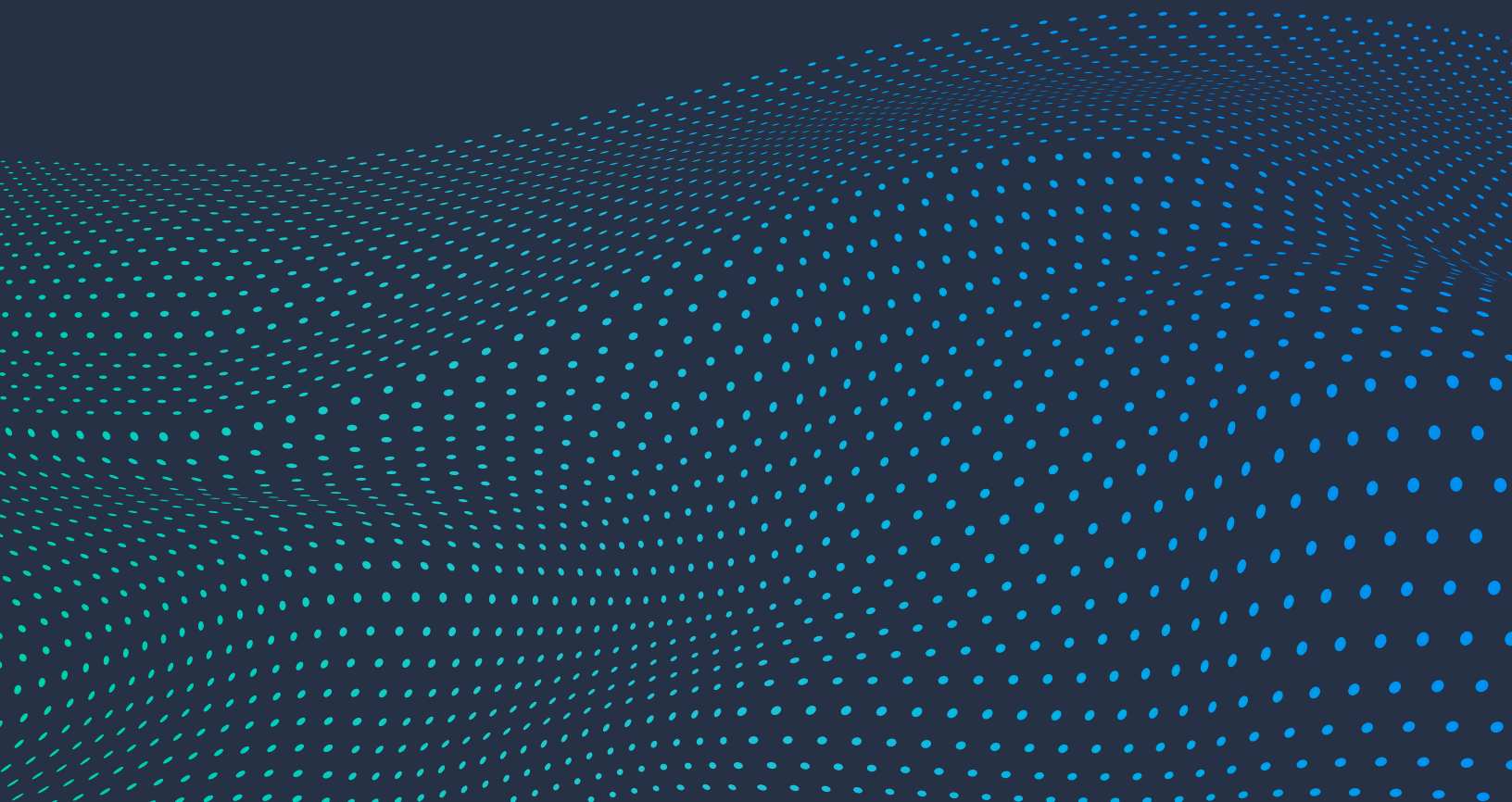


Table of contents

Introduction

The growing business use of emerging technologies such as artificial intelligence (AI) has made it more important than ever that business leaders understand how to manage their implementation effectively and securely.

For many businesses this can be a challenging journey. The cyber-risk landscape is complex and continuously evolving. The language of cyberthreats can be deeply technical, jargon-rich, and opaque. Organizations also have different appetites for risk; what is an acceptable level of exposure to one may be anathema to another. And in the face of competing priorities for business resources, compromises often need to be made.

The security end goal for all organizations is cyber resilience. Effective prevention and detection measures remain a critical cornerstone of security strategies, but companies shouldn't stop there. The evidence suggests that the likelihood of being affected by a security incident is almost inevitable. Many organizations fall victim repeatedly, particularly if they have not addressed the root cause of the first incident or the factors that allowed it to unfold.

What matters is how you prepare for, withstand, respond to, and recover from an incident. This is cyber resilience.

And while advanced, defense-in-depth security solutions will take you most of the way there, security success ultimately depends on people — the business leadership, the IT security professionals, and general employees.

Our Cybernomics 101 research, undertaken together with Ponemon Institute, shows how people-related security challenges, such as a lack of board-level support or security leadership, skills and staffing shortages, and the inconsistent implementation of security polices across the company can undermine cyber resilience. Many businesses worry about their supply chain security and who outside the organization might have access to their sensitive or confidential data — both areas of significant risk and prime targets for cyberattack.

Most organizations appreciate how exposed they are. Just 43% rate their security posture as very effective. However, this may not be as worrying as it seems — a belief that you could be doing more to enhance protection can help to focus attention and resources in areas that need them and ultimately make you more secure.

In this report we look deeper into the research findings related to cyber resilience and offer guidance on how to navigate your way to a stronger, more resilient future that works for you.

Siroui Mushegian, CIO, Barracuda Networks Inc

Methodology

Ponemon Institute surveyed a total of 1,917 IT security practitioners in the United States (522), the United Kingdom (372), France (329), Germany (425), and Australia (269) in September 2023. The final sample of respondents represented organizations with between 100 and 5,000 employees. All respondents are involved in the management of their organization's IT security functions or activities.

This report explores the findings by company headcount and for a number of industry verticals, consolidated for all the countries surveyed.

How organizations rate their security posture

We asked respondents how confident they feel about their ability to deal effectively with cyber risks, vulnerabilities, and attacks — using a scale of 1 to 10, where 1 is very ineffective and 10 is completely effective.

By a considerable margin, financial services organizations are the most confident about their ability to cope, with more than half (55%) rating their security posture as highly effective. The smallest companies surveyed were the least optimistic, with around half (48%) rating their security posture at the lower end of the scale.

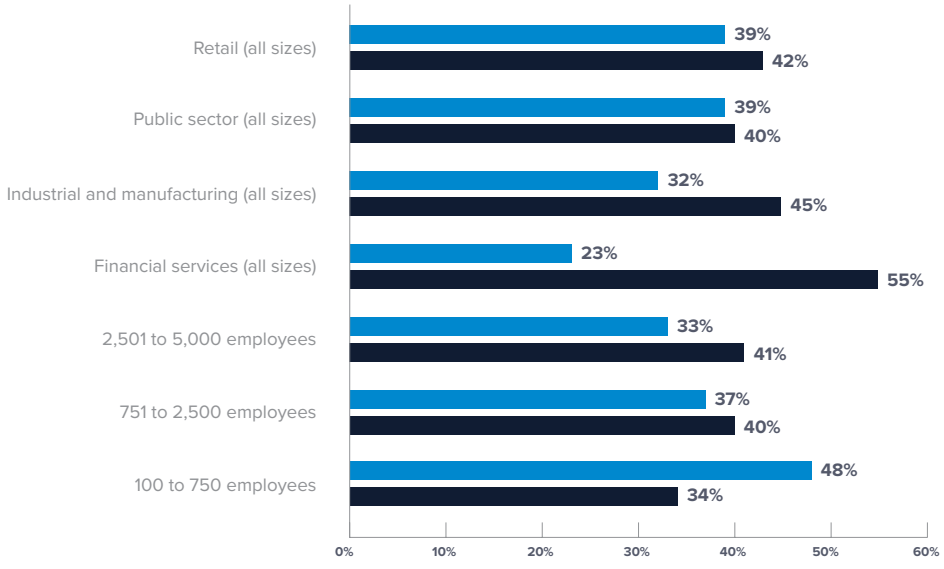


FIGURE 1

How would you rate your organization's security posture in terms of its effectiveness at mitigating risks, vulnerabilities, and attacks on a scale of 1 to 10?

Not very effective (1 to 4)

Highly effective (7 to 10)

n=1,917

The 'moderately effective' category (scale 5 – 6) is not included in the table.

Governance challenges

Lack of consistent company-wide security

For smaller and mid-sized organizations, the main governance challenge is a lack of consistent enterprise-wide security policies and programs, with half (48% and 50% respectively) choosing this as one of their top challenges, compared to just a quarter (27%) of companies with 2,501 to 5,000 employees. This is also the top challenge for financial services (49%), retail (49%), and the public sector (40%).

Implementing consistent policies can be an organizational headache for security teams. Business leaders can be reluctant to enforce security practices that appear inconvenient or restrictive. Some employees might resist controls such as 'just-in-time' or 'least privilege' access to certain applications or data, especially if they've had open access before.

Some employees might not be aware of security policies, unsure whether they apply to their systems or roles, or believe that their area should be an exception.

Such misunderstandings can lead to confusion and resistance and ultimately get in the way of effective implementation, increasing organizational risk.

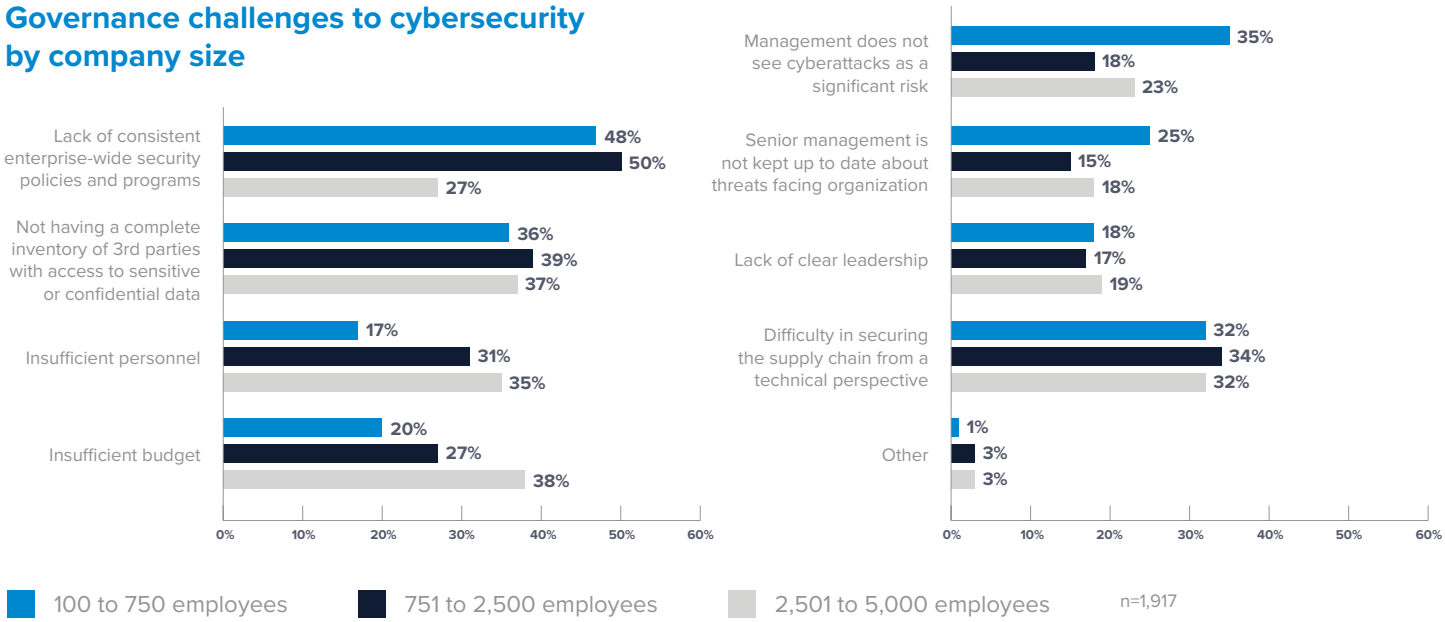
The more open and transparent you can be with employees about what the policies are, who they apply to, and why they matter, the easier it will be. These conversations promote understanding and cooperation, especially if they are supported by regular training. It is important to be responsive to change and to regularly review and update security policies, so they are aligned with evolving threats and business requirements.

Lack of leadership support and understanding

The smaller firms surveyed worry a lot about management challenges. Just over a third (35%) report that management doesn't see cyberattacks as a significant risk. This is not a question of management failure. It is hard to be interested in or care about something you don't understand. A quarter of the smaller firms admit that senior managers aren't kept up to date about threats facing the organization. The onus is on security professionals to speak in a language that business leaders understand. They need to be storytellers and be able to explain how to protect brand reputation through proactive, multifaceted defense programs.

FIGURE 2

Governance challenges to cybersecurity by company size



The risk management menu

A useful tool to help executives understand the risk and security choices they face is to present a simple menu of options. This approach can help you understand which risks need priority attention and your overall appetite for risk.

The following four-step methodology can help you to understand the risks currently facing your organization:

1. **Threats:** The circumstances or events that could harm organizational operations, assets, individuals, or other organizations
2. **Vulnerabilities:** The weaknesses that expose the organization or asset to exploitation
3. **Likelihood:** The probability that a risk scenario will occur
4. **Risk:** The potential for an adverse outcome

Once you understand the level of risk, you can decide on the level of protection you want and need:

- For example, 'high protection' involves locking almost everything down. This offers near total security but can come with restrictions that could lead to complexity, delays, and friction.
- At the other end of the scale, 'low protection' means access is largely unrestricted, open, and convenient — and also highly exposed.

Not every company has all the security resources, tools, and processes it needs on day one. By looking at security as a menu, you can build a roadmap of how to get there and the risks you need to manage along the way.

The menu can help you understand which risks need priority attention. A centralized risk register will help you keep track of your organization's risks and enable informed decision-making about managing or mitigating them.

A lack of skills and third-party visibility and control

The largest companies surveyed worry most about a lack of budget and skilled security professionals, at 38% and 35% respectively.

Supply chain risks represent a significant challenge for everyone, regardless of size. This includes not having a complete inventory of third parties with access to sensitive or confidential data and the technical challenge of securing the supply chain — around a third named each of these a top challenge.

This concern likely stems from the fact that much of the supply chain is beyond a company's security perimeter, and the further you move from your control, the more risk is introduced — especially if it includes vendors in markets with fewer security regulations.

Shadow IT has become a major concern. The unmanaged use of software applications creates a security risk as they often fall outside IT policies. Even approved software tools can introduce risk as many have evolved into platforms that offer marketplaces for third-party apps and plug-ins. These additions may provide unapproved fourth parties with access to sensitive data beyond the company's security perimeter.

Further, open-source generative AI tools can be valuable for innovation and productivity, but they also store and train their models on data shared with them. The unmanaged use of generative AI tools can expose company data beyond the corporate security perimeter.

Industry snapshot: Financial services

Financial services organizations have faith in the strength of their security posture. Just 3% don't have an incident response plan in place.

This is not surprising. The finance industry is highly regulated, with strict compliance rules and penalties for infringements. Employees accept the need to work within rules, processes, and procedures. Board and executive approval for security measures, combined with sufficient funding, means that business continuity planning (BCP) and disaster recovery (DR) strategies are in place to help organizations recover quickly from an incident.

However, the industry faces some security challenges. Many finance companies are huge. They've grown by acquisition into tremendous global organizations that exist in silos. Implementing globally resilient security processes across them all is immensely difficult.

Industry snapshot: Retail

Retailers are not as confident as financial services when it comes to their overall security posture, with 39% rating it as relatively ineffective. However, 42% rate their security posture as highly effective, and this underscores the complex, bifurcated nature of the industry when it comes to security.

On the corporate side, there's the head office, with the latest equipment, enterprise software, data centers, and protection. On the other side are the distribution and shipping centers, the production supply chains, and the actual retail stores. They could be using completely different sets of technology. A lot of this could be legacy equipment that is difficult or expensive to strip out, and IT teams are left trying to pull it all together as best they can.

Retail organizations were the most likely to cite a lack of inventory of third parties with access to sensitive and confidential data as a top governance challenge (46%) and difficulty in securing the supply chain from a technical perspective (35%).

Industry snapshot: Public sector

Public sector organizations are also more likely to lack confidence in their security posture, with 39% rating it as relatively ineffective. Insufficient budget (39%) is the top governance challenge after a lack of consistent, organization-wide security policies and programs (40%). Just over one in 10 (12%) doesn't have an incident response plan in place.

The public sector is hard to protect. There are many offices and employees to secure, budgets are invariably tight, and the attention of leaders, especially political ones, may be focused elsewhere. Many public sector organizations face shape-shifting budgets and funding that can change quickly according to the party in office. Planning for long-term security can be tough in these circumstances.

Incident response readiness

The good news is that around half of all the organizations surveyed, regardless of industry or number of employees, have an incident response plan that is applied consistently across the organization — and more than half say the plan is formally tested at least once a year.

Unfortunately, the good news ends there. Around a quarter (23%) of the largest companies have never tested their incident response plan, possibly because doing so in a large business can be a complex, time-consuming, and disruptive process. It can also be expensive to set up a business BCP/DR process if it must rely on significant volumes of data or system backups.

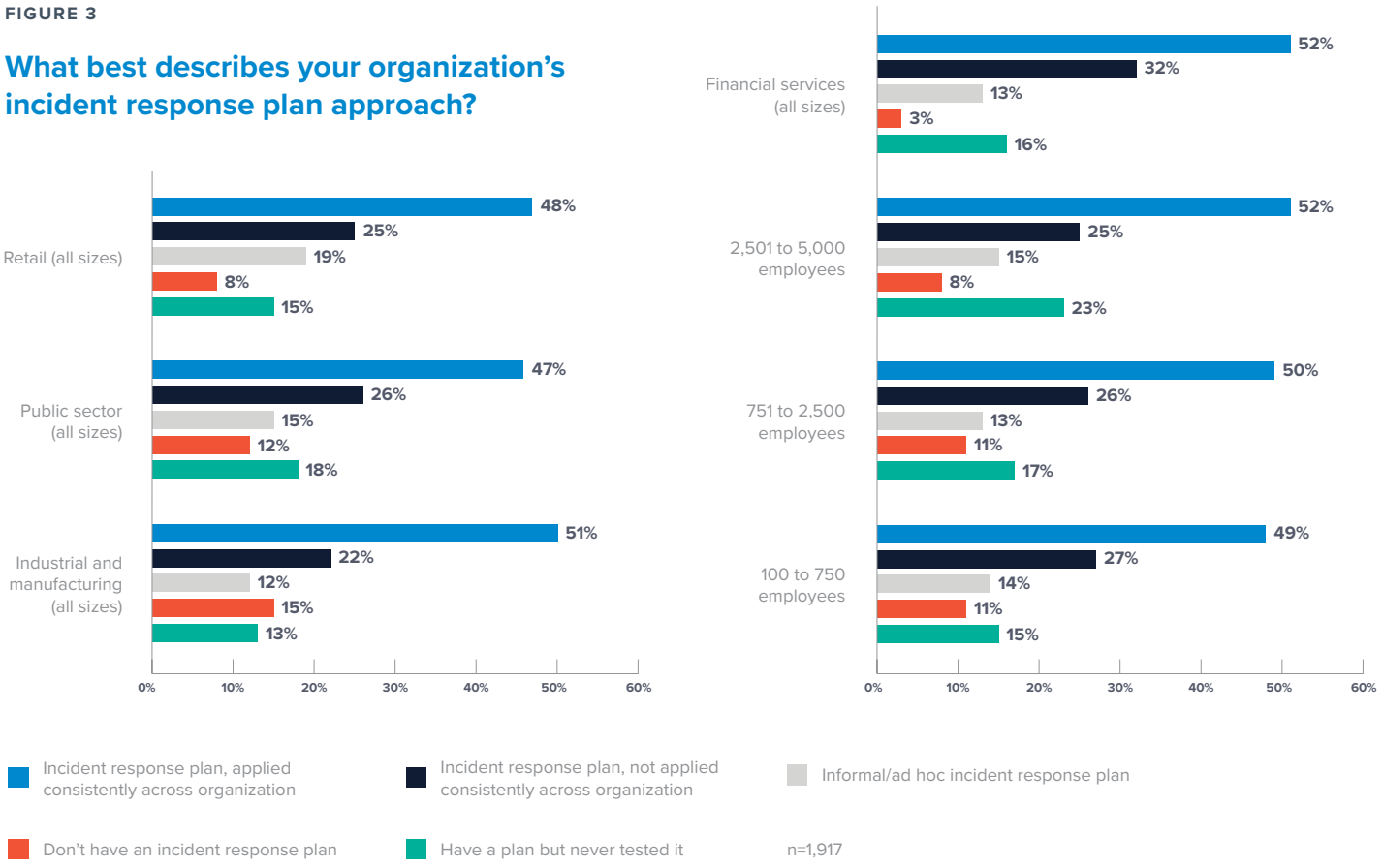
Further, around one in 10 overall admit they don't have an incident response plan in place.

If an organization doesn't have a plan about what to do if a security incident takes place, they risk finding themselves in the precarious position of not knowing how to react to events, and consequently doing nothing or the wrong thing.

A 'purple team' approach can help strengthen a company's readiness to respond. Purple teams manage and coordinate incident response simulations, creating scenarios where a 'red team' can launch a mock incident to which a 'blue team' then responds. Such simulations help companies to improve their ability to detect, respond to, mitigate, and learn from security incidents.

FIGURE 3

What best describes your organization's incident response plan approach?



Cyber resilience checklist

The following cyber resilience checklist draws on the U.S. National Institute of Standards and Technologies (NIST) Cybersecurity Framework.

GOAL	STRATEGIC FOCUS FOR BUSINESS LEADERS — WHAT YOU NEED TO KNOW	PROGRESS
PREPARE	**Organize** • Regulatory compliance What are your legislation and compliance obligations in each of the markets you operate in? • Management involvement and remit Who in the leadership team needs to be involved in cyber resilience and risk decisions? • Cyber insurance What kind of insurance do you need/are you willing or able to invest in?	☐ ☐ ☐
	Identify • Asset management What assets do you have, where are they, who has access to them? What are your most important assets for maintaining business continuity and operations? • Risk management and strategy What are your most exposed assets? What risks do they face? What is the potential impact of an attack in terms of damage, disruption, or loss?	☐ ☐
WITHSTAND	**Protect** • Security processes, policies, and technologies How can you best protect assets, infrastructure, and people within your available resources? • Cybersecurity awareness training How do you train and support employees? • Maintenance and control — patching, etc. Are your security basics in place? Patching, robust authentication, and access controls (multifactor authentication/Zero Trust), etc.?	☐ ☐ ☐
	Detect • Detection technologies and processes Can your security systems detect and block new and emerging threats? • Security operations center Is your security monitoring reliable and continuous? Can you oversee and manage the entire IT estate 24/7? Do you have access to the tools, skills, and staffing to investigate red flags and anomalies?	☐ ☐
RESPOND	**Mitigate** • Incident response planning and process Do you have an incident response plan that applies across the business? Is it regularly tested and up to date? How do you contain and neutralize incidents? How much downtime can your critical systems sustain? Can you revert to manual processes if needed? If your customers will be impacted, what is the service level that has been agreed to? Is your system on premises or in the cloud? (Is it a security-as-a-service (SaaS) enterprise, business system, etc.) In terms of regulatory compliance, who do you need to inform, and when? • Internal and external communications • Incident analysis and mitigation	☐ ☐ ☐
RECOVER	**Restore** • Recovery planning Do you have a business continuity plan/disaster recovery plan? Do you have a 'high availability' set up with your cloud provider? Do you need third-party support to uncover and close all gaps? • Internal and external communications • Improvements What lessons did you learn? What steps are you taking/should you take to harden your security?	☐ ☐ ☐

Conclusion

Cyber resilience is everyone's responsibility, but the main burden is shouldered by the security professionals. There is help available to support you, including fundamental and practical ways of ensuring you are meeting a minimum baseline of compliance.

Using the above template checklist is a great way of keeping your team and your organization on track and accountable. Adapt the document to the reality of your business environment and turn it into a roadmap and a plan with milestones, deliverables, and responsible parties.

For further information

There are many helpful tools, frameworks, and guidance notes available to help you navigate your way to cyber resilience. Here are a few to get you started:

- Cyber Governance Code of Practice (UK)
- National Association of Corporate Directors (U.S.)
- Australian Institute of Company Directors (Australia)
- Cybersecurity Framework 2.0 (U.S.)

About Barracuda

At Barracuda, we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Barracuda
Your journey, secured.