Your Guide to Cyber Resilience

USERNAME

****

☑ Remember me   ■ Forgat password

LOGIN

AI

DATA

riskonnect.

Sophisticated hackers, relentless cybercriminals, and distracted employees have converged into an explosive landscape of cybercrime – with sobering success rates.

The cost to business is staggering. The global average cost of a data breach is currently estimated at $4.45 million, up 15% in just three years. The FBI's Internet Crime Complaint Center received more than 800,000 complaints last year, with a potential total loss of more than $10.2 billion.

If you haven't yet felt the sting of a cyberattack, ransomware scheme, or data breach, consider yourself lucky. Nearly 75% of organizations have experienced at least one cyberattack. You could be next.

Cybercriminals are continuously making their attacks more targeted, more disruptive, and more ingenious. Remote and hybrid workforces spread over a sprawling number of networks open the door wider to attackers. In a moment of distraction, even vigilant employees can let in an attacker. And with the help of generative AI, these attacks appear increasingly authentic, making them more difficult than ever to thwart.

Cybersecurity is certainly essential to block attacks from happening in the first place. But as criminals have demonstrated an uncanny ability to adapt, these measures alone cannot protect your business. You need a comprehensive cyber resilience plan to help you quickly get back on track if an attack is successful.

This ebook will help you understand cyber resilience, what's at stake, and how to strengthen your approach.

TABLE OF CONTENTS

WHAT IS CYBER RESILIENCE?

Cyber resilience refers to an organization's ability to anticipate, adapt, respond, and recover from a successful cyberattack, including malware, phishing and spam, social engineering, and insider threats. If you experience an incident, a cyber resilience plan is what will allow you to continue operations with minimal disruption.

Cybercrime is one of the biggest threats to business of any size and in any industry. Ransomware/ security breaches were cited as a top risk driver by nearly half of risk professionals recently surveyed by Riskonnect, with another 39% calling out state-sponsored cyberattacks. A separate survey revealed that more than three-quarters of organizations reported at least one ransomware attack in the past year – and more than a quarter of those were attacked at least four times.

Among the forces driving up both the amount of activity and the cost are:

Stiff regulatory fines and penalties.

Regulators around the world consider cyber-related threats as a serious danger to capital markets and are prioritizing cybersecurity with tougher rules around disclosures and safeguards. Those in the financial services industry are subject to some of the strictest rules, but regulators are extending their authority across industries and taking action to enforce compliance.

Massive financial and operational consequences.

Unauthorized cyberactivity of any kind can force companies to take systems offline, bring in cybersecurity experts, and shut down operations until the problem is resolved, all of which can make a significant dent in the bottom line. Case in point is The Clorox Company, which estimates it incurred $49 million in costs related to a recent cyberattack, including IT recovery and forensics work, as well as operating expenses accrued from system disruptions.

CYBER RESILIENCE REGULATIONS TO NOTE

U.S.'s Securities and Exchange Commission

EU's Digital Operational Resilience Act (DORA)

The European Cyber Resilience Act

New York Department of Financial Services Cybersecurity Requirements

Federal Trade Commission's Standards for Safeguarding Consumer Information

Australia's Security of Critical Infrastructure Act 2018

New Zealand's Federal Market Authority proposal

Savvy cybercriminals.

Bad actors are becoming increasingly clever in their attacks – and are even joining together to form sophisticated criminal gangs to advance their interests. They are leveraging technology like generative AI to stay a step ahead of cybersecurity protocols and eliminate telltale signs like phishing emails with misspellings. Instead of big, bold moves with instant rewards, criminals are starting to manipulate small bits of data to stay under the radar and wreak havoc over time. Attacks are also becoming more focused, targeting supply-chain partners four, five, or six degrees from the original source.

Ubiquitous technology.

The increasing reliance on technology to serve customers, engage workforces, optimize operations, and store data makes system availability non-negotiable. Indeed, accomplishing even the simplest tasks – for customers, employees, suppliers – usually requires technology. And PII, proprietary competitive strategy, and other stored sensitive data makes for a tempting target.

Internal threats.

Employees, partners, contractors, and suppliers with system access can compromise security, whether unintentionally or maliciously. Inside threats can range from accidental data exposure from improper handling to deliberate data theft and extortion.

What Gets in the Way of Cyber Resilience …	And What to Do about It
Labeling cyber resilience an IT issue	Incorporate cyber resilience into your broader business strategy.
Confusion between cybersecurity and cyber resilience	Educate decision-makers that these are complementary plans, with one aimed at prevention and the other aimed at recovery.
Communication gaps between boards/C-suites and CISOs, who often speak in technical terms	Speak in a language familiar to your audience – like real-world risk and likely damage.
A lack of ownership for a comprehensive cyber resilience plan	Prioritize cyber resilience by recognizing it as a critical source of value to the business.

riskonnect

ELEMENTS OF A CYBER RESILIENCE PLAN

Even the best cybersecurity measures can't always stop an attack. In the event of a cyber incident, cyber resilience is your comprehensive strategy to withstand, adapt, and recover quickly.

Businesses that are proactive in assessing risks and defining mitigation strategies are well-positioned to protect sensitive data, continue operations, and preserve their reputation. Evaluate all available sources of information to gain insight into something bad that might happen and what its impact may be. AI and machine learning – plus human analysis – can help you sift through mountains of information as efficiently as possible.

Identify critical business services. What are your most important systems and services that would cause significant damage to the business or greater market if disrupted?

Map dependencies. What people, processes, technology, and data are connected to your critical business services?

Assess your controls. What measures and policies do you have in place to protect your technology assets? Do you have reliable back-up procedures for your infrastructure and critical data and systems?

Build a response plan. What specific steps are needed to prevent further damage and recover systems and operations? Who needs to know what and when? Who is responsible for each step?

Test your plan. How well does your plan perform when tested with severe but plausible scenarios? Do you need to make adjustments?

Cyber Insurance: Today's Necessity

Escalating digital exposures – from data breaches, ransomware, phishing emails, and more – are making cyber insurance an essential investment for businesses of all sizes and in all industries.

Cyber insurance offers financial protection for damage caused by cyber incidents, such as expenses for investigations, credit monitoring, legal support, and other associated costs. It also can provide financial compensation for business interruption, loss of revenue, and system restoration. Cyber insurance can impart a sense of security by allowing the business to concentrate on continuing operations amid an incident.

While insurers have made great strides in clarifying policy coverage and exclusions, costs are soaring. In response, many are reducing coverage limits and increasing premiums, which are rising by some 30%.

Demonstrating a comprehensive, tested cyber resilience plan can help optimize coverage and minimize premium costs.

riskonnect.

HOW CYBER RESILIENCE INTERSECTS WITH OTHER RESILIENCE PLANS

Cyber resilience, cybersecurity, operational resilience, business continuity, crisis management, disaster recovery are often used interchangeably, but they each represent different facets of a business continuity and resilience strategy.

Operational resilience is often linked to financial services regulatory requirements such as those introduced by Prudential Regulation Authority in the U.K. It focuses on the ability to continue providing important business services to the market and customers when experiencing severe disruption.

Business continuity focuses on preventing, responding to, and recovering activities and operations following the onset of a disruption.

Disaster recovery focuses on the recovery of IT services, applications, and data needed by the organization to perform business activities and deliver products and services.

Crisis management mobilizes at the onset of a disruptive incident and helps leaders manage the response to minimize impact through communications and recovery.

Cyber resilience focuses on continuing and recovering operations when affected by a cyberattack caused by malware, ransomware, or inappropriate/unauthorized access leading to a data breach or downtime.

Business Resilience

Operational disruptions	Life safety events	Cyberattacks	Supply chain risks

PREPARE				RESPOND	
Operational resilience	Business continuity	Disaster recovery	Cyber resilience	Crisis management	Emergency notification

HOW TO ASSESS YOUR CYBER RESILIENCE MATURITY

Using a maturity model to assess your cyber resilience program is an excellent way to identify where you are now, compare that to where you want to be, and determine what it will take to get there.

Apply the analysis on your current maturity level to weigh the value of a cyber resilience program, the cost of failure, and the investment required. The more mature your program, the more effective your program will be. Even the most mature programs, however, require continuous upkeep to stay ahead in a constantly changing world.

5
OPTIMIZED

4
INTEGRATED

3
DEFINED

2
PRELIMINARY

1
AD HOC
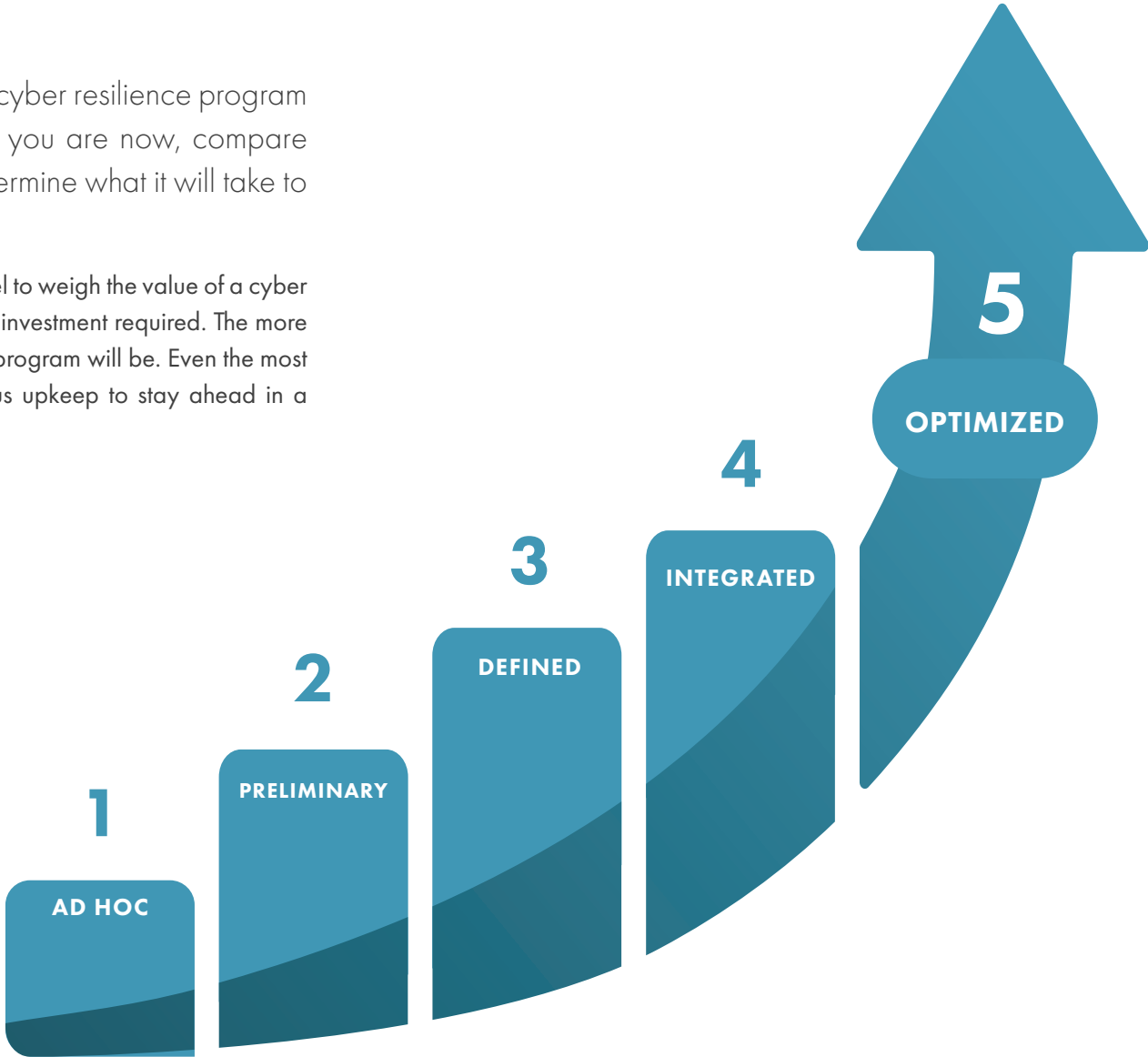
1 AD HOC

The management of cyber resilience is undocumented, in flux, reactive, and depends on individual heroics. Roles, responsibilities, processes, and plans are not clearly defined. Cyber resilience efforts mainly focus on technical controls and understate a broader organizational approach.

2 PRELIMINARY

Cyber resilience is defined in different ways and managed in silos. Efforts predominately focus on prevention and security rather than preparedness and response. Prevention and security overemphasize technical solutions and tools. Process discipline is unlikely to be rigorous and is only lightly defined. Roles and responsibilities are limited to program administrators or technical staff.

3 DEFINED

A common cyber resilience framework is in place and connected to key risk disciplines, such as the business continuity program, operational risk, and third-party risk management. An organization-wide view of cyber resilience is provided to executive leadership and the board. Efforts include a combination of technical, administrative, and physical controls. Roles, responsibilities, and response plans are defined, documented, and practiced. Plans are not limited to technical response and recovery.

4 INTEGRATED

Cyber resilience activities are coordinated across the organization, including relevant risk disciplines and business/operational areas. Risk disciplines share practices and resources, such as using common business continuity management tools and processes to enable enterprise-wide cyber-risk monitoring, measurement, and reporting. The organization has considered which threat scenarios would be most impactful, and these have been incorporated into scenario planning and other techniques, such as exercising. Recovery processes, including alternate processes and manual capabilities, are tested regularly and coordinated to help manage the consequences associated with a cyber disruption. Discussion of cyber resilience at executive committee and board levels is separate from the discussion of strategy and performance.

5 OPTIMIZED

Cyber resilience concepts are integrated into the broader enterprise strategy, including balancing cyber resilience with organizational initiatives, product or service development, and the strategic direction of the organization. Cyber and operational risk has moved beyond consideration as solely a cost center and is embedded in strategic planning, capital allocation, and other processes. The organization has a culture of resilience that is embedded in tactical decision-making. Risks and vulnerabilities that threaten the ability to recover are actioned at the appropriate level and reported regularly to management and the board. The organization has early-warning systems in place – threat and controls monitoring – to not only identify technical attacks, but to alert decision-makers if KRIs or other risk indicators are breached. The organization considers the broader geopolitical and economic landscape to identify threats that could impact the enterprise or require additional planning or resourcing. Business continuity and cyber-response strategies and plans are validated at all levels of the organization.

HOW TO START BUILDING A CYBER RESILIENCE PLAN

For cyber resilience to be successful, it must be an enterprise-wide strategy, led by executives, and embedded into every level of the organization, as well as partners, customers, and suppliers.

No one is immune to cybercrime. But being properly prepared can significantly reduce the impact on your organization. Here's where to start.

Change the conversation. Cyber resilience is not simply an IT issue. CISOs, CTOs, COOs, and the like will naturally be involved. But knowledge, data, systems, and processes are increasingly integrated across the enterprise – and everyone from the C-suite on down needs to participate in limiting the impact of a disruption.

Getting support from the top is particularly important to drive strategy and secure investment. Leave the tech jargon behind and frame the issue in more familiar quantitative financial terms – like loss exposure and likelihood of occurrence – to illustrate the size of the issue and inform strategy discussions.

Formalize the cyber resilience role. While still relatively rare, the position of chief cyber resilience officer is growing. The specific job title, however, is much less important than having someone dedicated to resilience who has the visibility and influence to ensure positive outcomes. Someone needs to be accountable for looking at the business as a whole – systems, third parties, locations, threats – and understanding the impact on humans, data, technology, and resources.

Develop your response plan. Create a step-by-step plan that specifies actions, responsibilities, and timing to contain the damage, avoid costly repairs, and protect customer trust.

- **Incident response.** The longer a cyber incident goes undetected, the more damaging it can be. Have a plan to quickly detect attacks and jump into action.

- **Communications.** Who should be notified, when, and with what information? Include all internal stakeholders, external suppliers/partners – and don't forget about regulatory reporting requirements and other legal obligations.

- **Restoration of critical business functions.** What do you need to do to return to normal operations after a breach/incident? This is a good opportunity to streamline and standardize processes across the organization and establish a strong governance structure.

Test and train. Put leadership, the technical team, and other stakeholders through severe but plausible scenarios to test the strength of your plan, identify opportunities for improvement, and develop muscle memory to speed response in the case of a real-life event. And feed those learnings back to continuously refine your plan.

But don't stop there. Achieving cyber resilience takes an all-hands-on-deck mentality. Just one vendor with weak security can expose you to substantial losses. Educate your employees, suppliers, contractors, and partners on what to do if they spot an irregularity. With more eyes and ears on the lookout for a problem, you are more likely to respond faster and contain the fallout.

Get going – now. Cyber risks are accelerating – and the ability of cybercriminals to evade strengthened defenses adds gasoline to the fire. Taking your eye off the ball even for a second can leave you vulnerable to devastating breaches and disruptions.

Protecting the business requires diligent planning, testing, training, investing, and allocating resources to stay a step ahead. Cyber resilience is now a board-level issue – and when done right can become a critical source of value to the business.

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,000 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 800 risk management experts in the Americas, Europe, and Asia.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

CONNECT NOW →

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

Risk Management Information System	Compliance
Claims Administration	Internal Audit
Third-Party Risk Management	Policy Management
Enterprise Risk Management	Project Risk
Environmental, Social, Governance	Health & Safety
Business Continuity & Resilience	Healthcare