Brought to you by:

Hitachi Vantara

Cyber Resilience

for dummies®

A Wiley Brand

Navigate threats and regulatory pressures

Build resilient, AI-ready architectures

Anticipate, recover, and improve fast

Hitachi Vantara Special Edition

Guy Hart-Davis

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., Hitachi Vantara provides the data foundation that world-leading innovators rely on. Through data storage, infrastructure systems, cloud management, and digital expertise, the company helps customers build the foundation for sustainable business growth. To learn more, visit hitachivantara.com.

Cyber Resilience

Hitachi Vantara Special Edition

by Guy Hart-Davis

for dummies®
A Wiley Brand

Cyber Resilience For Dummies®, Hitachi Vantara Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-394-30196-6 (pbk); ISBN: 978-1-394-30197-3 (ebk); ISBN: 978-1-394-30198-0 (ePub). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Traci Martin

Client Account Manager: Jeremith Coward

Table of Contents

Introduction

In today's hyperconnected world, a cyberattack occurs every six seconds on average. Until recently, well-configured defenses — such as firewalls, intrusion detection systems, and vigilant IT teams — were enough to repel most threats. But times have changed.

Today's businesses are always online, operating in the cloud, relying on mobile apps, and sharing data with third-party vendors and partners. All of this creates an increased attack surface, with more entry points for bad actors to exploit. Cybercriminals are also evolving. They now leverage artificial intelligence (AI) to automate attack methods, develop new attack methods, and probe for zero-day vulnerabilities. And with organizations now holding more sensitive data, the payoff for a successful attack is higher than ever.

In this new threat landscape, the question is no longer whether your organization *will* be attacked but *when.* The traditional cybersecurity paradigm of keeping out bad actors isn't sufficient. Instead, organizations must develop a mindset of and toolset for *cyber resilience* — the ability to withstand cyber attacks and recover quickly from them, which ensures business risk reduction and continuity with minimal disruption.

About This Book

Cyber Resilience For Dummies, Hitachi Vantara Special Edition, consists of seven chapters that cover the following:

- Identifying present-day security challenges and defining cyber resilience (Chapter 1)
- Implementing data governance and regulatory compliance in your organization (Chapter 2)
- Understanding what a resilient security posture is in the age of AI (Chapter 3)
- Moving from a reactive security posture to a posture of proactive cyber resilience (Chapter 4)

- Creating plans for resilient response and recovery to incidents (Chapter 5)
- Monitoring security, detecting and neutralizing threats, and driving continuous improvement (Chapter 6)
- Taking ten actionable steps to implement cyber resilience (Chapter 7)

Icons Used in This Book

This book displays icons in the margin to point you to three specific types of information:


REMEMBER

The Remember icon flags information you should make sure you don't forget.


TIP

The Tip icon points out practical advice and key information you're likely to find helpful.


WARNING

The Warning icon draws your attention to pitfalls you want to avoid.

Beyond the Book

This book explains what cyber resilience is and takes you through the major considerations in implementing cyber resilience. But there's only so much a short book can cover. If you find yourself hungering for more information about cyber resilience, follow these links:

- **htchivantara.is/4lqvT2q:** *Ensure Business Continuity Across the Enterprise* white paper
- **htchivantara.is/4eCxHCy:** *Boost Cyber Resilience with Superhero Powers* blog
- **htchivantara.is/44AVi22:** *Solutions for Data Resiliency and Compliance* e-book

IN THIS CHAPTER

- Facing up to present-day security challenges
- Understanding what cyber resilience is
- Grasping how culture is central to cyber resilience

Chapter 1
Reducing Business Risk with Cyber Resilience

In today's digital-first landscape, cyber threats pose a severe and growing risk to business continuity, reputation, and financial stability. To stay online and in business, you must move beyond traditional cybersecurity approaches and develop cyber resilience, an adaptive strategic framework for responding to threats and minimizing disruption.

In this chapter, you first identify present-day security challenges and the means of addressing them. You then dig into what cyber resilience means in the face of these threats and how it differs from traditional cybersecurity and disaster recovery. You also learn how culture is central to building cyber resilience into your organization and its employees.

Identifying and Addressing Present-Day Security Challenges

Never in its short history has cybersecurity been exactly easy, but security professionals now face a torrent of new security challenges and amplified threats. These include

- **Being online is vital:** These days, most every organization needs to be available online continuously for its customers. This online presence opens up an attack surface for bad actors.
- **Increased attack surface:** As IT environments become more complex and increase their use of cloud surfaces, they expose a larger and more dynamic attack surface for bad actors.
- **Tempting targets bring more threats:** Organizations storing large amounts of sensitive data make a tempting target for attackers.
- **More sophisticated attack techniques:** While security professionals harden their defenses, attackers continue to ramp up the sophistication of their attacks. For example, many security breaches require the exploitation of multiple vulnerabilities in a precise order. Other threats include ransomware as a service encrypting a breached data store and attacks through the software supply chain.
- **AI-driven attacks:** AI turbocharges attackers' capabilities, enabling them to probe large networks for vulnerabilities in seconds, use zero-day exploits, and perform automated attacks at machine speed.

At the same time as defending against threats such as these, businesses in regulated sectors need to comply with new regulations, such as the Digital Operational Resilience Act (DORA) in the European Union and Executive Order 14028, Improving the Nation's Cybersecurity, in the U.S. Compliance with such regulations involves far more than checking off items on a checklist once a year. Instead, you must demonstrate that your organization can recover from cyberattacks and disruptions while preserving forensic evidence cleanly for investigation.

REMEMBER

Cyber resilience helps you not only deal with these new security challenges but also comply with regulations.

Defining Cyber Resilience

Cyber resilience is a business-continuance strategy that enables your organization to keep operating effectively even when hit with successful cyberattacks or significant digital disruptions. Cyber resilience extends beyond preventing or averting attacks, focusing instead on developing the holistic ability to withstand and recover from cyber threats.

Cyber resilience involves not just creating robust responses to incidents but also preparing for swift and clean recovery from them. This preparation includes

- Preserving data for post-incident forensic analysis
- Meeting strict compliance, governance, and privacy regulations
- Ensuring clean restorable states by implementing measures like saving recovery points frequently to immutable storage
- Minimizing downtime by keeping systems updated and patched so that they have the latest software editions, which should have the fewest vulnerabilities
- Using virtualized systems to test updates and patches, simulate attacks and respond to them, and practice recovering systems and data

How cyber resilience differs from cybersecurity

Traditional cybersecurity focuses on preventing and detecting cyber threats — keeping the bad actors out of your network, systems, and data by using technologies such as firewalls and policies like encryption and access control. Keeping threats out used to be an effective approach to security, but nowadays it isn't adequate to the level of threats that organizations face.

By contrast, cyber resilience assumes that successful attacks and data breaches are inevitable, given the level of threats, the number of bad actors, and the technology available to them (such as AI). While cyber resilience aims to keep out attacks and avoid data breaches where possible, it also expects some attacks to be successful and emphasizes recovering from them.

How cyber resilience compares to data protection

Cyber resilience is a broader concept than data protection:

- **Cyber resilience** describes your organization's ability to prepare for cyberattacks, withstand them, respond to them, and recover from them.

- **Data protection** focuses on safeguarding data from loss, corruption, or unauthorized access. Data protection uses means such as encryption, access controls, and compliance with regulations to ensure the confidentiality, integrity, and availability of the data.

Data protection is an essential component of cyber resilience, but cyber resilience also includes various other components, including operational continuity, adaptability in the face of evolving threats, and rapid recovery from attacks.

How cyber resilience compares to resilience

In the context of business, resilience describes your organization's ability to bounce back when it experiences serious disruption. For example, a resilient organization would normally be able to recover from a natural disaster (such as an earthquake), an economic downturn, or a supply chain failure.

Cyber resilience, a subset of this general resilience, describes the organization's ability to respond to cyber disruptions — fending off attacks and malware as far as possible and getting systems back up and operations back online after a breach.

Recognizing the Importance of Culture to Achieving Cyber Resilience

To achieve and maintain cyber resilience in your organization, you need to make it a responsibility shared across all departments rather than letting people assume the responsibility falls on the IT department alone. This means fostering a culture of security awareness where every employee understands their role in protecting digital assets, from recognizing attempts at phishing and social engineering to complying with data handling policies. Develop regular training, cross-functional initiatives (see Chapter 4), and clear communication channels to build cybersecurity into your organization's workflows, ensuring that threats are identified and dealt with wherever they occur.

IN THIS CHAPTER

- Surveying the landscape
- Implementing best practices
- Including regulatory requirements in your budget

Chapter 2
Implementing Data Governance and Regulatory Compliance

Your first step in building cyber resilience in your organization should be to implement data governance and compliance with the relevant regulations. This is because, while data governance and regulatory compliance may appear isolated concepts, they're in fact integral parts of a holistic cyber resilience strategy. Governance and compliance provide the necessary framework for organizations to protect their data, meet legal requirements, and withstand cyberattacks.

In this chapter, you review the data governance and compliance landscape, examine how to implement best practices to become and stay compliant, and learn how to build regulatory requirements into your security budget.

Mapping the Data Governance and Compliance Landscape

Nowadays, most industries have regulations intended to protect consumers, ensure public health and safety, maintain financial stability and integrity, and hold businesses responsible for their actions.

You typically want to start by exploring the data governance and compliance landscape that applies to your organization. The regulations that apply depend on your organization's geographical locations, the countries or regions in which it operates, and the type of business it performs.

While the specifics of the regulations will vary, the three examples in this section should give you an idea of the types of requirements you may be facing.

GDPR

Enacted in 2018 by the European Union (EU), the General Data Protection Regulation (GDPR) is a wide-ranging data privacy and security law designed to protect EU citizens' personal data and apply standard data protection across all EU member states. GDPR reaches beyond the EU by applying to any organization worldwide that processes or targets the data of EU citizens.

GDPR sets limits on data collection; mandates lawful, fair, and transparent data processing; and requires data to be stored securely. Organizations must demonstrate accountability via documentation and data protection impact assessments; organizations that focus on monitoring data subjects or process sensitive personal data need to appoint data protection officers. Non-compliance with GDPR exposes an organization to significant fines.

DORA

The Digital Operational Resilience Act (DORA) is an EU regulation intended to strengthen the cyber resilience and digital security of the financial sector by requiring comprehensive ICT risk management, mandatory incident reporting, and resilience testing.

DORA applies to many types of global and regional financial entities that operate in the EU, from banks and payment companies

to crypto-asset services providers, and from investment firms to insurance companies. DORA also applies to critical third-party Information and Communication Technology (ICT) companies that provide services to those financial entities. DORA came into effect in January 2023, and full compliance was required by January 17, 2025.

DORA carries stringent penalties for non-compliance:

- Financial institutions face fines of up to €10 million or 2 percent of their total annual worldwide turnover, whichever is higher.
- Individuals such as executives face fines of up to €1 million.
- Designated critical ICT service providers face fines of up to €5 million or 1 percent of their average daily global turnover (whichever is higher) for each day of non-compliance, up to six months.

Apart from these monetary penalties, EU member states can require corrective and remedial measures from offenders or impose criminal penalties on them.

HIPAA

The 1996 Health Insurance Portability and Accountability Act (HIPAA) is a United States federal law that protects the privacy, security, and integrity of individuals' protected health information (PHI) both during transmission and in storage.

HIPAA applies to healthcare providers, insurers, and related organizations. Three of its key rules are the following:

- **Privacy Rule:** Specifies who can access and share health information.
- **Security Rule:** Mandates that organizations protect electronic health data using physical, technical, and administrative safeguards.
- **Breach Notification Rule:** Requires that a covered entity (such as a hospital) notify affected individuals, the U.S. Department of Health and Human Services (HHS), and the media if PHI is compromised. Requires that business associates (such as a third-party billing service) notify the covered entity (which must then notify affected individuals, HHS, and the media).

Non-compliance with HIPAA carries financial penalties for civil offences and jail time for criminal offenses knowingly obtaining or disclosing PHI in violation of HIPAA.

REMEMBER

Regulation is an ongoing process, so keep an eye open for regulatory changes that will affect your organization. For example, in 2025, the EU is expanding the role of the GDPR in AI governance to cover how AI systems process personal data. Similarly, the HHS is updating HIPAA to require encryption for electronic protected health information (ePHI), multi-factor authentication, regular security assessments, comprehensive risk analysis, and faster notification of breaches.

Developing Best Practices to Attain and Retain Compliance

Once you have identified the regulatory landscape in which your organization is operating, shift your focus to making your organization compliant with the regulations — and then keeping it compliant. Regulatory frameworks such as DORA and HIPAA require considerable effort to achieve initial compliance followed by sustained vigilance to stay compliant, but you can streamline compliance by developing best practices.

Developing the following best practices can help considerably with both achieving initial compliance and staying compliant:

- **Create a compliance-driven culture.** Make an organizational commitment to compliance by having leadership prioritize compliance and align it with business objectives. Embed compliance across workflows using cross-functional collaboration between IT, legal, risk, and operations teams. Issue compliance policies and procedures, and conduct regular training on the subject.
- **Perform risk-based assessments.** Identify the relevant compliance requirements and conduct risk-based assessments to pinpoint gaps in data protection, cyber resilience, and third-party management. For example, for DORA compliance, you need to assess ICT third-party risks and plan mitigation strategies for them.

- **Set up technical and organizational controls.** Implement technical controls — such as encryption, access management, and continuous monitoring — that will protect sensitive data and provide system resilience. Set up organizational controls, such as incident response plans and change management procedures, to support the technical controls. Align the technical controls and organizational controls with regulatory requirements. For example, to meet DORA detection and reporting requirements, you might deploy a Security Information and Event Management (SIEM) tool that provides real-time monitoring and alerting, supported by an incident response plan.
- **Automate your compliance processes.** Use automated tools for tracking compliance, scoring risk, and control testing to provide greater accuracy and lower costs than manual compliance processes. Monitor systems and vendors constantly to detect anomalies early and meet DORA's requirement for cyber resilience.
- **Keep an up-to-date compliance repository and audit trail.** Build a repository of policies, risk assessments, incident logs, and proof of control implementation so that you can face regulatory inspections and internal audits with confidence.

Building Regulatory Requirements into a Budget

Given the regulatory landscape discussed earlier in this chapter, compliance is no longer a box-ticking exercise; instead, it is a key element of your cyber resilience strategy. Regulatory mandates — such as DORA, GDPR, and HIPAA (all discussed earlier in this chapter) — impose strict requirements for operational continuity, data protection, and audit readiness. To meet these requirements, you must implement verifiable security controls. That means making mandatory investments in your security budget.

For example, DORA requires financial institutions that operate in the EU to be able to recover critical business services within 60 minutes of an operational disruption. This is a legal obligation rather than a guideline; to meet it, you need to invest in failover infrastructure and advanced recovery solutions and develop effective incident response capabilities. Ignoring these

legal requirements puts your organization at risk of penalties for non-compliance as well as suffering operational failures when crises occur.

DORA and similar regulations also require proof of continuous compliance, so when building your security budget, you must also make provision for keeping your organization ready for audits. You may need to allocate funds for tools and services such as the following:

- **Automated compliance monitoring:** Get tools or services that automatically evaluate your systems and processes for regulatory requirements, reducing the need for manual auditing and giving faster responses.
- **Security Information and Event Management (SIEM) platforms:** Systems that collect security data from your organization's systems, networks, and applications; analyze the data; and correlate it. SIEM platforms help you detect threats and respond to incidents.
- **Immutable storage systems:** Systems that lock your stored data in an unchangeable state for a defined period of time, thus preventing tampering, ensuring your data's integrity, and enabling its safe recovery. Immutable storage systems provide an audit trail for your data, supporting legal and regulatory compliance.

WARNING

Non-compliance with regulations can bring significant financial consequences. In 2020 (before DORA), the average regulatory fine for data breaches in the banking and financial services sector was over $500 million. Beyond the monetary penalties, a compliance failure may damage your reputation, driving down your stock price, diminishing the brand value, and destroying carefully nurtured customer trust.

When building compliance into your budgeting, work with other departments rather than trying to silo it in a single department such as IT or Security. Plan to work with your organization's legal, risk-management, and business-continuity teams to identify the relevant regulatory requirements, assess gaps in your coverage of them, and create a coordinated and fully-funded compliance plan.

Building regulatory requirements into your security budget like this increases your organization's overall cyber resilience as well as mitigating legal and financial risks. In this way, you turn compliance from a burden into a boon.

IN THIS CHAPTER

- Harnessing AI power to boost your security
- Identifying the challenges and threats AI poses
- Spotting AI security risks and warding them off

Chapter 3
Redefining Resilient Security Posture for the Age of AI

As artificial intelligence (AI) rapidly transforms the digital landscape, traditional security frameworks are being outgunned and outmaneuvered by ever more sophisticated and severe threats. In this chapter, you explore how organizations need to redefine their security posture to remain resilient in an AI-charged age. The chapter starts with the good news, examining how you can leverage AI to enhance aspects of your organization's security operations from threat detection to incident response. The chapter then moves along to the bad news, laying out the unique threats and challenges that AI introduces, before explaining practical approaches to identifying AI-enabled threats and defending your organization against them.

Leveraging AI to Augment Security

To counter cyber threats and to maintain a resilient security posture, you should leverage AI as fully as possible to augment your organization's security. AI can play multiple roles in security,

from turbocharging threat detection to automating responses to attacks:

- **Detecting and averting threats:** AI can analyze vast datasets rapidly and detect anomalies that may represent cyberattacks. Machine learning models can identify threats that rules-based systems miss, flagging suspicious behavior such as unusual login patterns, phishing messages, or malware activity.

  
  TIP

  AI significantly strengthens defenses against zero-day attacks — attacks using unknown vulnerabilities — by detecting behaviors that stray from normal patterns. AI can also create actionable threat intelligence by analyzing global threat data, allowing organizations to ramp up their defenses proactively before an attack occurs.
- **Responding automatically to threats:** AI can speed up response to threats by automating security workflows. AI-powered systems can prioritize alerts, minimize false alarms, and automatically trigger response measures. For example, they can quarantine affected devices, enforce access restrictions, or suggest necessary security updates. These automatic responses dramatically shorten the time between detecting threats and dealing with them.
- **Implementing behavioral analytics and continuous authentication:** AI can perform User and Entity Behavior Analytics (UEBA) to profile normal user activity and identify changes that may indicate insider threats or a compromised account. For example, an authorized user account logging in from a different location than usual or attempting to access areas of a system that account does not normally use may indicate a threat. UEBA adds a dynamic layer of security by validating users not just by their credentials but by their behavior patterns, thus enabling continuous authentication instead of authentication only at login.
- **Responding in real time to emerging threats:** Using AI, you can implement adaptive cybersecurity frameworks that continuously evolve to counter new threats. To keep defenses strong enough to ward off ever-changing cyberattacks, such systems can modify access rights, revise firewall settings, or activate multi-factor authentication in real time, based on ongoing risk evaluations.

- **Performing post-incident analysis:** Following a security breach, AI can swiftly analyze logs to help forensic teams identify the breach's cause. AI can also feed actionable insights back into detection systems, enabling continuous learning and strengthening defenses against future attacks.

All these AI capabilities are welcome additions to your security arsenal, but AI tools are not a replacement for your security staff members. Rather, AI tools lighten the load on your security staff by performing both security drudge work and advanced tasks beyond human abilities quickly and untiringly, referring incidents to human members when decisions beyond AI's remit are needed.

Recognizing the Challenges Posed by AI

As you saw in the previous section, AI brings powerful capabilities to organizational security, improving and speeding up threat detection and response. But as with much technology, AI brings challenges as well. This section examines how AI expands the attack surface, requires specialized skills to handle, and accelerates the evolution of cyber risks.

Managing increased data volume and complexity

AI systems not only rely on vast amounts of input data for both training and analysis but also generate large quantities of output data. Both input data and output data may include sensitive corporate information or personal data and need to be stored securely.

Storing large amounts of data creates a tempting target and a larger attack surface for attackers. More data means more potential entry points for attackers, more sensitive information to protect, and greater difficulty in maintaining data integrity and confidentiality, especially since AI data often uses diverse formats and decentralized storage. Protecting such information assets effectively requires complex data governance, robust encryption, and access controls throughout the entire data life cycle.

Bridging the AI skills gap

The second major challenge that AI brings is a skills gap: There aren't enough cybersecurity professionals who understand AI

security risks and mitigation strategies. This skills gap means that organizations will find it difficult to assess risks and so may overlook critical vulnerabilities introduced by AI systems.

To bridge this skills gap, organizations need to upskill their existing security staff in AI technologies and threats, recruit AI security talent, and encourage cross-functional collaboration between their security staff and AI developers.

Identifying AI-specific vulnerabilities and attack vectors

As if security teams didn't have plenty of traditional IT vulnerabilities to deal with, AI introduces new vulnerabilities and attack vectors, such as these:

- **Model inversion:** An attacker uses access to an AI model to infer sensitive information about the data used to train it.
- **Data poisoning:** An attacker corrupts an AI's training data to cause the AI to become biased or exploitable.
- **Adversarial attacks:** An attacker inputs subtly altered data to cause the AI to misclassify or misinterpret the output — for example, to bypass a facial-recognition security system.

Worse still, attackers can harness the power of AI to their own ends, as discussed next.

Identifying and Defending Against AI Security Risks

The wide availability of AI has driven the arms race between security professionals and threat actors to a new level. While white hats are deploying AI to strengthen cybersecurity, threat actors are eagerly leveraging AI to create sophisticated and wide-ranging new attacks. This section explains how threat actors are weaponizing AI and how organizations can develop resilient defenses to counter them.

Understanding how threat actors use AI

The following list explains three key ways in which attackers use AI:

- **Automating reconnaissance and exploiting vulnerabilities:** Using AI, an attacker can scan vast networks and identify vulnerabilities in seconds rather than the days or weeks such scanning would have taken without AI. Automated tools driven by AI can attempt to guess passwords based on information known about the target, run brute-force attacks (trying to find passwords), or perform credential stuffing (inserting stolen usernames and passwords into login fields) at machine speed.
- **Performing highly personalized social engineering:** Most people can recognize conventional phishing messages, but attackers using generative AI can now create not only targeted and contextually relevant phishing messages but also deepfake voice calls or videos. The results are convincing enough to fool even security-aware employees.
- **Creating polymorphic malware:** AI can create malicious software that changes its signature continually to evade traditional detection tools. Evasion techniques powered by AI enable malware to analyze security systems and adapt itself in real time to avoid detection.

Defending against AI security risks

Traditional cybersecurity isn't adequate to combat today's AI-powered threats, let alone the upscaled threats coming down the pike. Instead, you need to develop a security model that incorporates AI tools to operate at machine speed and scale.

TIP

Here are five central planks for beefing up your cybersecurity with AI:

- **Deploying AI-driven behavioral analytics:** These analytics can detect AI attacks that manifest as unusual patterns, such as spikes in network traffic or data access from atypical locations. After detecting a potential problem, the AI can contain it for evaluation.

- **Adding multi-factor authentication (MFA):** Passwords alone are little use against attackers who can use AI to guess, steal, or brute-force them. For effective security, add multi-factor authentication via authenticator apps, biometrics, or one-time passwords.
- **Deploying AI-enhanced incident response:** In today's machine-speed threat arena, responding instantly is key to cordoning off potential threats before they spread. Set up your AI defenses to contain problems by isolating compromised devices and applying access controls before involving human staff to take any further actions needed.
- **Training employees to recognize threats:** Your organization's employees should be one of its greatest strengths, but they also represent a key vulnerability. Implement regular training from onboarding onward to enable employees to recognize social engineering tactics and phishing attempts (both regular phishing and AI-enhanced phishing).
- **Integrating and monitoring AI tools:** For robust governance and risk management, incorporate AI-specific risk assessments and government frameworks. You will need to secure the data you use for training your AI systems, validate your AI outputs, and test your defenses regularly against simulations of AI-driven attacks.

IN THIS CHAPTER

- Improving your security posture
- Uncovering and triaging security issues
- Developing secure and compliant apps
- Nurturing a culture of resilience

Chapter 4
Making the Move to Proactive Cyber Resilience

With threat actors becoming more sophisticated and regulations tightening, defending your organization with reactive cybersecurity is no longer enough. Instead, you need to implement proactive cyber resilience that will not only protect data but also maintain trust, compliance, and operational continuity.

In this chapter, you explore four areas key to this transformation.

Moving from a Reactive Security Posture to a Proactive One

Until recently, many organizations have assumed a reactive security posture: They protected their networks, systems, and data by using tools such as firewalls, antivirus and antimalware, and encryption and generally concentrated on keeping bad actors out. When an attack occurred, they responded to it, investigating breaches, fixing vulnerabilities that were revealed, and informing stakeholders about the attack and the damage control.

REACTIVE SECURITY INCREASES DOWNTIME

Two incidents in Spring 2025 in the U.K. spotlight how a reactive security posture often results in serious downtime. First, the high-profile retailer Marks & Spencer suffered a phishing-based cyberattack over Easter 2025 that exposed customer data and disrupted its services for two months. Second, the Co-operative Group (Co-op) detected an attack in May 2025 that wreaked havoc on its stock ordering systems and supply chains for several weeks. Perhaps even worse, the attackers claimed to have been operating in the Co-op's network for a while before being detected.

The lengthy downtime from these cyberattacks highlights the value of a proactive security posture. Cyber resilience is expensive — but for many organizations, the cost of weeks of downtime and severe reputational damage is likely to be even higher.

Given the vastly increased level of threats that most organizations now face, and the heightened severity and sophistication of those threats, a reactive security posture is no longer adequate, especially for any organization that needs to ensure operational continuity. Instead, security experts recommend transitioning to a proactive security posture that reduces risk exposure and recovery costs while limiting reputational damage. A widely used framework for this posture is the Cybersecurity Framework (CSF) 2.0 from the National Institute of Standards and Technology (NIST).

NIST CSF 2.0, as the framework is commonly called, lays out a structured approach to cybersecurity. The framework identifies six core functions that help organizations to transition from reactive security to proactive security:

- **Govern:** Create cybersecurity policies, roles, and risk management strategies that align with the organization's business objectives.
- **Identify:** Identify risks by constantly surveying the threat landscape and internal vulnerabilities.
- **Protect:** Reduce risk exposure by training employees and implementing safeguards such as access controls and encryption.

- **Detect:** Spot threats in real time by using continuous monitoring and advanced tools.
- **Respond:** Contain and mitigate security breaches by using incident response plans.
- **Recover:** Be able to restore affected systems and operations with minimal impact on business operations.

Implementing these core functions moves an organization to a proactive security posture. For example, in implementing the Govern and Identify functions, an organization evaluates its risk environment, defines clear policies that tie in with its business objectives, and assigns roles and responsibilities for proactive cybersecurity.

Identifying Security Vulnerabilities and Prioritizing Their Remediation

To implement a resilient cybersecurity posture, you need not only to identify vulnerabilities in your organization but also prioritize them so you can remediate them strategically and efficiently. You need to go beyond checklists and patch cycles and really understand which risks pose the greatest threat to your organization.

Performing a comprehensive cyber assessment

Start by performing a full-spectrum audit of your organization's security posture. You need to assess the infrastructure, review IT policies, and audit layered defenses to uncover both technical and procedural weaknesses. While you may likely find various straightforward problems, such as ancient software that requires updating or removal and open ports that need closing, you're also looking to uncover how vulnerabilities interact with business operations, compliance obligations, and user behavior.


TIP

To perform this comprehensive cyber assessment, use automated scanning tools backed up by expert analysis. This one-two punch lets you not just identify the vulnerabilities but also tie them to the systems, workflows, and data they affect.

Simulating threats

After you've mapped out the current state of your organization's security environment, pressure-test the environment by running simulated attacks. Schedule controlled penetration tests and red team exercises for attacks such as these:

- **Distributed denial of service (DDoS) attacks:** Overwhelming a target system or network with a flood of internet traffic, either to disrupt business or to distract from other attacks.

  Perform the penetration testing on a digital twin environment, not on your organization's live environment. See the nearby sidebar for details on digital twins.

- **Social engineering:** Manipulating individuals into disclosing confidential information or taking actions that compromise security. For example, in the hack of the Co-op, the attackers posed as employees and used social engineering to get IT support staff to reset passwords or grant unauthorized access.
- **Privilege escalation:** After gaining low-level access to a system, exploiting vulnerabilities to get administrator-level privileges and take control of a system.
- **Code breaches:** Exploiting application code flaws, such as buffer overflows or insecure application programming interfaces (APIs), to get unauthorized access or manipulate data.
- **System exploits:** Attacking the operating system, such as exploiting vulnerabilities in the operating system's kernel, to execute code, elevate privileges, or gain unauthorized access.


REMEMBER

By running such attacks, you can discover how your systems hold up under attack and identify gaps in threat detection and response.


TIP

Evaluate the vulnerabilities holistically rather than in isolation, bearing in mind that attackers will often chain together multiple vulnerabilities to build effective attacks.

WHAT IS A DIGITAL TWIN?

A digital twin is a digital model of a real-world physical product, system, or process. You can use a digital twin for purposes such as simulation, integration, testing, monitoring, and maintenance. For example, you can test how a system or environment will behave and respond to cyberattacks or other problems. The digital twin provides a production-grade offline environment that simulates real-world conditions. By using a digital twin, you can test and improve your system's resilience without risking damage or downtime to the live system.

Because the digital twin is virtualized, you can easily roll it back to an earlier saved state (such as a snapshot). For example, you might use a digital twin to test a software update, and then roll back the digital twin to its pre-update state so that you could run further tests.

Developing a risk-based prioritization framework

After identifying vulnerabilities, build a prioritization framework that enables you to rank them by risk and potential impact so that you can clearly see which to remediate first. Link each vulnerability to your organization's business-critical assets and its regulatory exposure.

Focus on the systems that contain mission-critical data or are subject to legal and regulatory requirements such as data privacy or payment security. Use performance metrics such as mean time to detect (MTTD; see the nearby Remember paragraph) and mean time to respond (MTTR; likewise) to gauge how well your security efforts are working and where you need to invest more resources.

REMEMBER

MTTD is the average time your organization takes to detect a security problem that's occurred. Mean time to respond (MTTR) is the average time your organization takes to fix or contain the problem after detecting it.

Assessing your organization's security readiness

Assess the ability of your organization's teams and tools to detect threats, respond to them, and recover from them. Here are three key considerations:

- **A SIEM may improve security readiness.** A Security Information and Event Management (SIEM) platform integrates your security tools under a single pane of glass, giving easier and faster access to them.
- **DevSecOps integration is key.** Ideally, your development, security, and operations teams work together from the start to build security into your software rather than retrofitting security after development.
- **Patches and upgrades need thorough testing.** To keep your systems' software as secure as possible, you will want to apply patches and upgrades soon after they become available — but you will need to test them thoroughly first. See Chapter 6 for more on this topic.

Hardware and software are vital for effective security, but so is wetware. Train all your organization's staff to be security minded and to recognize and report suspicious activity. In your training classes, include the teams from different departments who will work together rather than training each department separately. To instructor-led classes, add tabletop exercises and live drills that will make team members work together and will highlight any coordination difficulties between the various teams.

Integrating Security and Compliance into Application Development

With regulators worldwide looking to secure the software development supply chain, development teams must make security and compliance core components of the development cycle rather than bolting them on at the end of development. Recent regulations, such as the U.S. Executive Order 14028 (EO 14028) and the EU's DORA, demand greater traceability, transparency, and risk reduction in application development.

Tracking increased scrutiny of the software supply chain

In recent years, vulnerabilities in third-party dependencies and open-source components have enabled high-profile attacks such as the Log4Shell vulnerability in 2021. To reduce the risk of such problems, regulators are increasingly looking to secure the software development supply chain.

For example, to strengthen the software supply chain for federal agencies, EO 14028 requires vendors to provide detailed Software Bills of Materials (SBOMs). An SBOM lists all open-source or custom components used in an application, thus simplifying risk assessment and vulnerability management.

Similarly, DORA imposes strict resilience requirements on software in the banking, financial services, and insurance (BFSI) sector. DORA's provisions include making code changes traceable and requiring organizations to define recovery timelines for ICT disruptions. For example, a bank may commit to a maximum tolerable downtime (MTD) of two hours for its online payments service, meaning it must restore the service to full operation within that time after an outage.

Automating trust with DevSecOps practices

In the traditional programming model, developers first coded applications, and then added security and compliance at the final review stage. This approach created bottlenecks that slowed down development.

To avoid this slowdown, DevSecOps uses a model that embeds security and compliance checks in the development process, automating trust by building security controls into workflows. In this model, security scans, policy validations, and access control happen in real time, contributing to speedy development.

Tracking application actions with logging and telemetry

To demonstrate compliance, an application may also require immutable logging, writing critical application actions to tamper-proof logs that can provide a trustworthy trail of activity usable in a compliance audit or an investigation. As well as providing a

record of what has happened, telemetry — the real-time collection of metrics, events, and performance data — also helps organizations to detect anomalies in real time as they occur.

Developing a Culture of Resilience Through Cross-Functional Initiatives

In the olden days of the previous millennium, security was often largely if not wholly the responsibility of the IT department. Now that threats have multiplied and grown far more potent, security has become a responsibility shared by all staff in the organization. When all that's needed to trigger a security disaster is for one member of staff to open a phishing message or an email attachment without thinking, you need everybody alert and working together.

Similarly, to create resilient defenses, you need to foster a culture of resilience throughout your organization. Often, the best way to do this is by implementing cross-functional initiatives that bring together members of different departments to collaborate on ways to enhance organizational resilience. For example, you might create a team that draws people from the HR, Finance, and Operations departments as well as from the IT department.

Here are three examples of cross-functional initiatives you may explore for boosting the resilience of your organization:

- **Resilience and Anti-Phishing Onboarding Program:** Ensure your organization's new employees understand their importance in resilience from the get-go. At the same time, train employees to recognize phishing techniques and social engineering gambits.
- **Business Continuity Planning Team:** Develop a continuity plan, test it, and maintain it. Make the team cross-functional to ensure the plan is connected across departments rather than siloed within them.
- **Cyberattack Response Workshop:** Walk through a cyberattack simulation and assess how effectively each department would respond. Pinpoint communication problems and identify resources needed for business continuity and messaging.

IN THIS CHAPTER

- Changing focus from disaster recovery to cyber resilience
- Creating a response and recovery plan
- Minimizing downtime and data loss
- Implementing a cyber vault

Chapter 5
Developing Plans for Effective Response and Recovery

To implement cyber resilience in your organization, you need to develop plans to respond effectively to cyberattacks and recover from them. In this chapter, you first explore why you should change from a mindset based on disaster recovery to a mindset based on cyber resilience. You then look at how to create a response and recovery plan and how to approach minimizing downtime and data loss. You also learn about the advantages of storing your critical data and backup snapshots in a cyber vault.

Shifting Your Mindset from Disaster Recovery to Cyber Resilience

Disaster recovery (DR) has long been the paradigm organizations use to prepare for and deal with IT disruptions. As the name says, the focus is on recovering after disaster strikes; for example, if your organization suffers a cyberattack, you activate your data protection plan to restore its systems and data as quickly

as possible. The present-day landscape of fast-evolving cyber threats renders this type of reactive approach obsolete. Instead of disaster recovery, you need to adopt a mindset of cyber resilience.

Rather than just bouncing back after an attack or outage, cyber resilience involves continuing to operate during the incident. To this end, you need to integrate security, risk management, and business continuity into your organization's daily operations rather than treating them as isolated areas.

To make this mindset shift, you need to follow four steps:

1. **Move from an approach of reacting to problems to an approach of anticipating problems.**

   That means understanding your organization's critical assets, identifying potential means of attacks, and continuously evaluating weaknesses in your security.

2. **Change your goal from restoring data or systems to maintaining business continuity even when under attack.**

   Design your systems to provide redundancy and fault tolerance and to be easy to isolate when trouble hits. Plan for your organization's essential services to continue to run, even if at reduced capacity.

3. **Require all departments to contribute to cyber resilience.**

   Responsibility for disaster recovery has traditionally fallen on IT departments, and IT still retains a key role, but the legal department should help with regulatory compliance, HR should provide security awareness training for all employees, the facilities department should ensure physical security, and so on.

4. **Change from static planning for disaster recovery to a mindset of dynamic adaptation to an ever-evolving threat landscape.**

   To be resilient, you need to monitor your organization's systems continuously, learn from attacks on them and those of your competitors, and adapt your defenses to deal with new threats that emerge.

Architecting a Response and Recovery Plan

Now that cyberattacks are a real and persistent threat, creating a response and recovery plan has become a core business function rather than the IT exercise it might have been in the past.

REMEMBER

Cyber resilience is an elevated conversation in the boardroom because the vast majority of modern companies derive their value from data rather than from the physical products they create. This means that data protection is everyone's responsibility.

Creating the plan should be a team effort involving not just the chief privacy officer, the chief data officer, and the IT department but also other departments such as legal, communications, and human resources. The team should add accountability to the plan by specifying who owns the plan and is responsible for executing it.

Prioritizing risks

To start creating your plan, list the assets you're protecting and prioritize their recovery:

- **Identify your critical assets.** Prioritize the recovery of the data, systems, and processes vital to your organization. Depending on its line of business, these might be financial systems, manufacturing control systems, customer databases, or intellectual property.
- **Identify the leading threats.** List the types of attacks bad actors are most likely to use on your organization — for example, denial-of-service attacks, ransomware encryption, or straightforward data theft. Understanding the threat landscape should help you anticipate attackers' tactics and arm your organization with effective countermeasures.
- **Quantify the impact of downtime.** For each critical system, assess the cost of downtime and estimate how much data loss you can tolerate. Set concrete targets for your response and recovery plan by assigning Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Designing a response with fast action and smart decisions

When a cyberattack breaches its defenses, your organization needs to respond fast to limit damage. Create clearly documented response procedures for what is to happen, including who will lead the response, which systems must be taken offline, and what measures need to be taken to contain and eradicate the threat.

Your response and recovery plan must preserve evidence that will enable breach forensics to evaluate the incident. You need the forensic analysis not only for grasping what went wrong but also for compliance with regulations and for legal defense.

REMEMBER

Include in your plan full details of which regulators your organization must notify of breaches and of how and when to inform them.

Testing your plan and improving it

To make sure your plan works properly, test it by using drills and simulations. Most likely the first iteration of the plan will reveal gaps in coverage, coordination, and understanding. This is normal, so conduct "post-mortem" analyses to identify what additions and improvements are needed. Then test again and repeat the cycle of analysis and improvement.

By using the feedback from testing, you can turn your response and recovery plan into a continuous quality process. Evolve your plan to keep up with changes to your organization's business and the threats it faces.

Constructing a Modern Approach to Minimizing Downtime and Data Loss

Implementing cyber resilience means maintaining system uptime and protecting data integrity even when cyberattacks break through your organization's defenses. Taking a proactive, modern approach enables you to minimize downtime and data loss in ways that traditional disaster recovery plans do not.

Eliminating outdated infrastructure

Legacy systems often demonstrate impressive survival skills, but you should look seriously at removing them from your systems, as they typically lack the speed, flexibility, and security to deal with present-day threats and operational demands. As a result, your legacy systems may act as bottlenecks during recovery operations, extending downtime and making data loss more likely. Look to upgrade your legacy systems to cloud-based, scalable platforms that support automation and provide greater resilience and rapid response to incidents.

Creating snapshots for faster restoration

Daily or weekly backups may have been enough for traditional data recovery, but for cyber resilience, you will need to create backups that give near-continuous data protection for your critical systems and that enable you to restore data swiftly. This means, instead of taking standard backups, capturing snapshots that reduce potential data loss to minutes rather than hours and that you can restore rapidly and reliably, preferably via automated procedures.


TIP

Test your recovery processes regularly to make sure they are effective. As usual, test using a digital twin environment, not your live system. Work with cross-functional teams to set Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) that meet your organization's business needs.

Incorporating immutability and forensics

Recovering fast is crucial to cyber resilience, but you also need to recover cleanly and confidently. That means protecting your data and integrating forensics with the response and recovery process.

To protect your snapshots from threats such as ransomware encryption and insider attacks, make the snapshots immutable, so that they cannot be altered or deleted for a specified period of time. You may want to store the snapshots in a cyber vault.

TIP

To help your organization investigate, understand, and respond to cyberattacks, integrate forensics into your data protection and recovery strategy. With forensics, you can analyze the root cause of an attack and work out how the attacker gained access. You can also identify which of your systems or data sets were affected and validate the integrity of your snapshots, making sure that your restore points contain clean and uncompromised data.

Service-level agreements and the Cyber Resilience Guarantee

To formalize your expectations for data protection, recovery, and response to security incidents, implement service level agreements (SLAs). An SLA can be either internal to your organization or with a third-party provider whose services you use. Either way, an SLA ensures that all the stakeholders agree on recovery priorities.

TIP

When you're evaluating SLAs, look at the Cyber Resilience Guarantee, a kind of super-SLA that combines contractual assurances with technical capabilities including real-time threat detection, guaranteed immutability, and full recovery support. This agreement guarantees the recovery of clean data quickly to the nearest recovery point using immutable snapshots instead of backups, enabling swift recovery from attacks and providing effective cyber resilience.

Understanding the life cycle and value of your data

A key element in shifting from a reactive security posture to a proactive security posture is understanding the life cycle and value of your data.

REMEMBER

The data life cycle describes the data's journey from start (creation or collection) to finish (archiving or destruction). Between those start and end points, the life cycle includes the data's storage, processing and usage, and sharing with or transfer to other departments or organization.

Understanding the life cycle enables you to implement proactive security on the data. You can

- Apply targeted controls to different stages of the life cycle, such as encrypting the data strongly during transit and implementing robust access controls during processing.
- Map potential vulnerabilities in your data's transit paths and storage.
- Ensure compliance with the Digital Operational Resilience Act (DORA) and other regulations by mapping compliance requirements for each stage of the data life cycle.
- Reduce the attack surface by minimizing data collection and retention.

It's also crucial to understand the data's value — not just the monetary value or competitive value that the data's loss might represent, but also the reputation cost of a data breach, the data's importance to your organization's daily operations, and the potential for fines or legal repercussions of non-compliance with regulations.

Understanding the data's value helps you implement proactive security in several ways. You can

- Prioritize your resources to protect your most valuable and critical data. For example, such data might require multiple layers of encryption, stricter access control, and continuous monitoring rather than standard protections you might apply to less sensitive data.
- Assess the risk that the data's loss would represent.
- Prioritize your restore operations. For example, you would normally want to recover your data that is critical to core operations before less vital data.

Securing data in a cyber vault

A *cyber vault* is secure and isolated storage in which you keep your mission-critical information and snapshots safe from threats such as malware, ransomware, and insider attacks. You might think of a cyber vault as a digital safe that physically or logically separate sensitive data copies from the production environment, ensuring that even if your main system is compromised, your clean data remains safe and recoverable.

The cyber vault is protected by being air-gapped (physically disconnected or logically separated) from the main network. Access is tightly controlled using role-based permissions and multifactor authentication (MFA). To protect snapshots from tampering or ransomware encryption, the data stored in the vault is immutable for a defined retention period — once the data has been written, it can't be altered or deleted.

A cyber vault enables you to recover clean data rapidly after an attack or outage, even during ongoing investigations. The cyber vault's isolation from the main network enables IT to analyze and cleanse data before reintegrating it. IT may also run AI-powered anomaly detection on snapshots to ensure they are not corrupted or otherwise compromised.

As well as enabling swift restoration of clean data, a cyber vault's immutable and auditable snapshots help an organization demonstrate compliance with regulatory requirements for data protection and retention.


TIP

In your cyber vault, use snapshots rather than backups. Snapshots provide a nearer recovery point for your data than backups, enabling you to recover data more quickly and to reduce data loss.

IN THIS CHAPTER

- Recognizing why security monitoring is key
- Catching threats — and crushing them
- Assessing the benefits of managed security
- Applying patches and upgrades securely
- Creating a virtuous circle of continuous improvement

Chapter 6
Monitoring Security and Driving Continuous Improvement

In this chapter, you explore why security monitoring is essential to implementing effective cyber resilience. You then move on to detecting and neutralizing threats, consider the benefits of security as a managed service, and learn best practices for applying patches and upgrades safely to your systems. Finally, you examine how to create a virtuous circle of continuous improvement in your organization's resilience.

Grasping the Importance of Security Monitoring

In the past, a traditional cybersecurity model — putting defenses in place and responding after incidents occurred (reactive) — was sufficient, but today's elevated threat landscape and relentless AI-driven cyberattacks require a proactive approach.

Security monitoring is vital for the following reasons:

- **Detecting threats early:** Monitoring using automated tools can identify anomalies or malicious activity in real time. By taking action immediately, you can prevent a small incident from developing into a major breach.
- **Reducing damage and downtime:** Automated tools can respond instantly to incidents, quarantining compromised or suspect systems to prevent malware from spreading. Isolating problem systems like this should reduce downtime resulting from incidents.
- **Adjusting defensive strategies to meet threats:** Constant security monitoring of data from networks, systems, and endpoints builds a picture of current threat level, enabling you to adjust your defensive strategies.
- **Demonstrating regulatory compliance:** Security monitoring provides an audit trail that lets your organization demonstrate compliance with regulations.
- **Supporting recovery and remediation:** Security monitoring data enables you to perform critical analysis of incidents and identify their causes. This information helps you not only recover from incidents but also avoid them in the future.
- **Preventing future attacks:** Ongoing monitoring enables you to identify recurring attacks, gain insight into attackers' tactics, and predict threats.
- **Maintaining business continuity:** Security monitoring lets you quickly contain threats and prevent their spread, thus maintaining uptime and business continuity.

Detecting and Neutralizing Threats

After you've accepted that some cyberattacks succeed no matter how strong your organization's defenses are, your priority becomes detecting threats as early as possible and neutralizing them as soon after that as you can to avoid them developing into full-scale crises.

Detecting threats early

To detect threats early, you need to monitor the following four areas of your system:

- **Infrastructure:** Your IT infrastructure includes your physical servers, your virtual machines and containers, and your cloud instances. Scan these systems continuously for unusual behavior, such as spikes in CPU usage or network traffic; for unexpected modifications, such as changes to user accounts or permissions; or known indicators of compromise (IoCs), such as unusual login activity or connections to unknown domain names or IP addresses.
- **Endpoints:** Endpoints include devices such as smartphones, tablets, and laptops used for remote work or remote access. You can deploy endpoint detection and response (EDR) tools to identify suspicious behaviors, such as logins from new locations or attempts to escalate privileges, on endpoint devices.
- **Data stores:** Monitor your data stores to detect attacks from ransomware or malicious actors. Back up your data for near-instant restore by capturing snapshots rather than regular backups.

  Store your snapshot data on immutable storage, such as in a cyber vault (see Chapter 5) to prevent changes. Restrict access to that storage to only those administrators who actively need it. Even so, monitor access to the data storage so that you can detect unauthorized access (for example, from insiders).


TIP

- **Applications and network traffic:** Run real-time analysis of application and network to identify zero-day attacks or attackers moving laterally through the network to find targets. Scan your network traffic also for communications between malware and external command-and-control (C2 or C&C) servers used to exfiltrate your data, issue commands remotely, or update or expand the malware.

ANALYZING MONITORED DATA WITH SIEMS AND XDRS

Monitoring your system's infrastructure, endpoints, data stores, and traffic generates far more data than humans can realistically analyze. Instead, you will normally want to use either a Security Information and Event Management (SIEM) tool or an Extended Detection and Response (XDR) tool to analyze the data at machine speed, flagging anomalies and incidents for review by humans as needed.

A SIEM tool is a hub that collects log data from the monitored devices on your infrastructure, aggregates the data, and normalizes it. The SIEM identifies known attack patterns by using rule-based correlation and signature matching.

XDR provides a more advanced approach to monitoring than SIEM. Rather than focusing on log data, an XDR tool integrates and correlates security telemetry from a wider range of sources, including cloud, email, and identity data as well as endpoints and network systems. Using advanced analytics and threat intelligence, XDR can detect new threats (such as zero-day vulnerabilities) and multi-stage attacks that SIEM would likely miss.

Neutralizing threats

After you detect a threat, you need to neutralize it rapidly and intelligently. Typically, you want to take the following steps:

1. **Contain the threat.**

   Stop the attack from spreading. That may mean isolating a compromised system from the rest of your network, segmenting your network to prevent attackers from moving laterally through it, revoking compromised credentials used in an attack, or configuring your firewall to block suspect IP addresses. If you have an XDR system, you can configure it to take these types of actions for you automatically.

2. **Eradicate the threat.**

   Remove the threat by scouring infected systems, uninstalling malware, and patching vulnerabilities that the threat has exploited.

3. **Recover your systems and data.**

   After neutralizing the threat, you can restore your systems from clean backups — preferably snapshots, for faster restoration — held in immutable storage.

4. **Analyze the incident and apply lessons learned.**

   Review how the attack happened and determine vulnerabilities it used or exposed so that you can decide how to improve your organization's resilience. For example, you may need to beef up your authentication protocols for critical systems, bolster your employee security awareness training, or upgrade from SIEM to XDR.

Assessing the Benefits of Security as a Managed Service

If you're not already committed to an in-house cybersecurity operation, you may be better off outsourcing your cybersecurity to a Managed Security Service Provider (MSSP), a provider that offers security as a managed service. An MSSP can provide five major benefits over an in-house security operation:

- **24/7 monitoring and response:** Given that cyberattacks can strike at any time, having around-the-clock security vigilance from an MSSP is far better than having an in-house operation working business hours.
- **Immediate access to cutting-edge security expertise:** MSSPs have teams of experienced analysts, engineers, and threat intelligence professionals available to handle every aspect of cybersecurity. Increasingly, MSSPs are supplementing these human resources with AI-powered tools that can process huge amounts of data and identify threats in real time.
- **Cost efficiency:** Your organization pays a set monthly fee to the MSSP for the security service. While the monthly fee may be substantial, paying an MSSP is generally far less expensive than recruiting, training, and equipping an in-house team that can deliver the same caliber of service.
- **Swift scalability:** As your organization grows (or shrinks) or its security needs change, the MSSP can scale its services up

or down accordingly. For your organization, this is far easier than hiring (or firing) security staff.

- **Improved compliance and reporting:** Part of MSSPs' business is keeping their clients compliant with applicable regulatory frameworks, such as the Digital Operational Resilience Act (DORA) or the 1996 Health Insurance Portability and Accountability Act (HIPAA). MSSPs' services include in-depth reports and audit trails that lighten the burden of compliance audits on organizations.

Implementing Best Practices for Applying Patches and Upgrades

To keep your organization's systems secure, you normally want to apply patches and upgrades as soon as they become available so you can benefit from the fixes and any new features they include. To ensure cyber resilience, never install patches and upgrades on a live system without testing them comprehensively first. Instead, apply the patches and updates in a secure but non-live environment where you can test them and their effect on the system fully before deploying them.

CROWDSTRIKE'S 8 MILLION BLUE SCREENS

For an example of the havoc that faulty updates can cause, cast your mind back to July 2024. On July 19, CrowdStrike Holdings, Inc., a high-profile Austin, TX–based cybersecurity company based in Austin, TX, released a disastrous update to its Falcon Sensor security software.

The update, which CrowdStrike had apparently not tested enough, caused blue screen of death (BSOD) crashes on more than 8 million computers running Microsoft Windows. These crashes led to global computer outages in key services including banking, healthcare, and air travel.

REMEMBER

The best tool for testing patches and upgrades is typically a digital twin (see Chapter 4), a virtualized representation of the corresponding physical system. By using a digital twin, you can test the effect of the patches or upgrades on your system thoroughly in a safe environment, applying the updates to your live systems only when you are sure they are effective and beneficial.

When using a digital twin, you would normally proceed as follows:

1. **Create the digital twin environment.**
2. **Save one or more snapshots of the digital twin's pre-patch state.**
3. **Benchmark the speed of the digital twin before the update so that you can compare the speed after the update.**
4. **Run attack simulations before the update to determine the security status. Again, you do this so that you can compare the security status after the update.**
5. **Install the patches in the digital twin. Make sure they install cleanly. Verify that all the system's services still run and that dependencies are intact.**
6. **Test the digital twin for stability and compatibility. Run normal operations and benchmark performance. Watch for abnormal behavior, incompatibilities, and performance degradation. Run attack simulations and compare their results with the pre-patch results to gauge the effect of the patch.**
7. **Roll back the digital twin to its pre-patch state for any further testing needed.**

After you confirm the patches are safe and effective, prioritize the patches and create a plan for which patches to install on which systems and the order in which to install them. You can then deploy the patches to the live system in controlled stages, monitoring the live systems using the metrics you found useful on the digital twin.

Driving Continuous Improvement

With the cyberthreat landscape continuing to evolve rapidly — if not actually speeding up — cyber resilience is more a process than a destination. To keep your organization secure, embed the principle of continuous improvement into its security operations.

Moving beyond compliance to handle evolving threats

Meeting the requirements of the applicable compliance frameworks can be a great way to start implementing cyber resilience, but you need to go further to handle evolving threats.


TIP

Look at each new threat, each attack, and each vulnerability as a stimulus for growth and reinforcement, and learn from them. After each incident, conduct an in-depth analysis to determine its root cause, identify which vulnerabilities the attack exploited, and highlight any gaps in the detection and response capabilities of your current controls. Use this information to improve your organization's defenses.

To improve them further, adopt a proactive stance to threat intelligence, monitoring how the threat landscape is evolving and staying aware of the latest attack vectors, vulnerabilities, and adversary tactics. Make any needed changes to your systems' defenses, apply patches and updates to your systems (after thorough testing), and organize security training on new threats for your colleagues.

Leveraging metrics and testing

To determine whether your organization's performance is improving, you need to measure performance and test it. To measure performance, first establish key performance indicators (KPIs) for cyber resilience using metrics such as mean time to detect (MTTD) incidents, mean time to respond (MTTR) to incidents, successful containment rates for breaches, or how often security control failures occur. Gather data for these KPIs and analyze the results to see which areas are improving and which need improvement.

To test cyber resilience, perform the annual penetration tests required by regulatory frameworks such as DORA and HIPAA as an absolute minimum. You should also regularly scan for vulnerabilities and run red team exercises and simulated attacks to stress-test your organization's defenses and assess how well it responds to threats. When a test exposes failures, use this information to remedy weaknesses, improve your playbooks for responding to attacks, patch vulnerable systems, and train staff in cybersecurity.

IN THIS CHAPTER

- Understanding regulations and compliance needs
- Prioritizing and protecting critical data
- Identifying and closing security gaps
- Testing and boosting recovery processes
- Embedding security into culture and development
- Monitoring systems and driving continuous improvement

Chapter 7
Ten Steps to Cyber Resilience

Cyber resilience is the ability to withstand cyber incidents and quickly recover from them to keep your organization's business running. To implement cyber resilience in your organization, follow these ten steps:

1. **Grasp regulations and compliance requirements.**

   Understand this action for your organization's business sector and its geographical locations and reach. Build suitable policies for your organization based on this step. See Chapter 1 for more info.

2. **Prioritize business-critical data.**

   Classify the data based on sensitivity and operational impact. Make sure you understand the life cycle and the value of the data (Chapter 5 discusses this in more detail). Protect sensitive and valuable data by using secure and immutable storage.

3. **Identify risks and gaps.**

   Conduct regular cyber assessments to complete this step in your organization's defenses. Evaluate your infrastructure,

review IT policies, and audit layered defenses to find both technical and procedural weaknesses. Prioritize the risks and their remediation. See Chapter 4.

4. **Create a backup plan.**

   Develop and implement a comprehensive backup plan, focusing on a robust strategy and clear processes. For quick recovery, take snapshots instead of regular backups. Document your recovery workflows, assign ownership for operations, and schedule regular testing. For more info, see Chapter 5.

5. **Protect your backup environment.**

   Secure your backup environment using immutability and isolation — for example, use a cyber vault (check out Chapter 5 for more).

6. **Test and refine your recovery process.**

   Identify and implement any improvements needed. Use virtualization such as digital twin environments for realistic simulations; see Chapter 4.

7. **Embed security and compliance into development.**

   Embrace the DevSecOps model in this step instead of bolting on security and compliance after development. Head back to Chapter 4 for more details.

8. **Make your employees a security asset.**

   Train employees in security awareness during onboarding and regular follow-up sessions. Foster a culture of clear communication so any employee can confidently respond to a threat. See Chapter 4.

9. **Monitor your systems and data.**

   Complete this action to detect threats early and reduce damage and downtime. Use AI-powered threat detection tools. Monitoring also provides an audit trail for compliance with regulations. Flip to Chapter 6 for more information.

10. **Drive continuous improvement.**

    Recognize that cyber resilience is an ongoing journey instead of a destination. Don't assume you've reached resilience; instead view each new threat, each attack, and each vulnerability as a stimulus for driving continuous improvement. See Chapter 6.

Resilience *Simplified.*

Your One-Stop Trusted Partner.

Struggling with rising threats, regulatory demands, and limited resources?

Hitachi Vantara provides complete cyber resilience through a single, trusted partner. We're the choice of 86% of the Global Fortune 100 for a reason. From identifying risk to accelerating remediation and achieving audit-ready compliance, we simplify resilience with integrated protection, detection, and recovery—built into your hybrid cloud.

Ensure predictable business continuity with 100% data availability and the world's fastest ransomware recovery, empowering you with unwavering confidence.

Scan to learn more

Subject to Hitachi Vantara's terms and conditions; please contact your Hitachi Vantara Representative for details.

Hitachi Vantara

Transform cyber risk into resilience

This book contains everything you need to start engineering cyber resilience into your organization's infrastructure. You learn how to design a strategy that spans hybrid environments, unifies security and data governance, and accounts for AI-driven threats. You also gain clarity around automating threat detection, response, and recovery. The result is a scalable, resilient architecture built to support uptime, compliance, and long-term business continuity.

Inside...

- Assessing the evolving threat landscape
- Meeting regulatory requirements
- Securing workloads across hybrid environments
- Aligning security with data governance
- Evolving to a proactive defense model
- Automating workflows
- Embedding a culture of resilience

Hitachi Vantara

Guy Hart-Davis is the author of several computer books, including *Killer ChatGPT Prompts: Harness the Power of AI for Success and Profit; iPhone For Dummies, 2025 Edition; macOS Sequoia For Dummies;* and *Teach Yourself VISUALLY iPhone 16.*

ISBN: 978-1-394-30196-6
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.