MIT Technology Review
Insights

As the cybersecurity landscape becomes increasingly complex, organizations must establish business-wide cyber resilience to avoid costly unplanned downtime and data loss.

Adapting to new threats with proactive risk management

Produced in partnership with

Hitachi Vantara

In July 2024, a botched update to the software defenses managed by cybersecurity firm CrowdStrike caused more than 8 million Windows systems to fail. From hospitals to manufacturers, stock markets to retail stores, the outage caused parts of the global economy to grind to a halt. Payment systems were disrupted, broadcasters went off the air, and flights were canceled. In all, the outage is estimated to have caused **direct losses of more than $5 billion** to Fortune 500 companies. For **US air carrier Delta Air Lines**, the error exposed the brittleness of its systems. The airline suffered weeks of disruptions, leading to $500 million in losses and 7,000 canceled flights.

The magnitude of the CrowdStrike incident revealed just how interconnected digital systems are, and the extensive vulnerabilities in some companies when confronted with an unexpected occurrence. "On any given day, there could be a major weather event or some event like what happened...with CrowdStrike," said then-US secretary of transportation **Pete Buttigieg** on announcing an investigation into how Delta Air Lines handled the incident. "The question is, is your airline prepared to absorb something like that and get back on its feet and take care of customers?"

Unplanned downtime poses a major challenge for organizations, and is estimated to cost Global 2000 companies on average **$200 million per year**. Beyond the financial impact, it can also erode customer trust and loyalty, decrease productivity, and even result in legal or privacy issues. A **2024 ransomware attack on Change Healthcare**, the medical-billing subsidiary of industry giant UnitedHealth Group – the biggest health and medical data breach in US history – exposed the data of around 190 million people and led to weeks of outages for medical groups. Another ransomware attack in 2024, this time on CDK Global, a software firm that works with nearly 15,000 auto dealerships in North America, led to **around $1 billion worth of losses** for car dealers as a result of the three-week disruption.

Key takeaways

1. Businesses continue to face a rapidly changing threat landscape. Ransomware-as-a-service, software supply chain attacks, and a growing attack surface area are making companies more vulnerable to disrupted operations. The fast adoption of AI is creating new risk, and changing global regulations demand attention.

2. A focus on adaptive security and proactive cyber resilience starts with executives. Creating a resilient business requires a broad approach to security, risk management, and business operations, focused on improving security awareness, ingraining compliance requirements into operations, and recognizing the limitations and strengths of AI systems.

3. AI tools can enhance cyber resilience and support data protection. Companies can use AI to simplify the identification of important assets, make analyzing threat data easier, and move at the speed and scale required by the threat landscape.

"We've got to be more preventative and use intelligence to focus on making the systems and business more resilient."

Chris Millington, Global Cyber Resilience Technical Expert, Hitachi Vantara

"The more we do, the more we get plugged in digitally, the greater that attack surface is."

Justin Lam, Senior Research Analyst, 451 Research, part of S&P Global Market Intelligence

Managing risk and mitigating downtime is a growing challenge for businesses. As organizations become ever more interconnected, the expanding surface of networks and the rapid adoption of technologies like AI are exposing new vulnerabilities – and more opportunities for threat actors. Cyberattacks are also becoming increasingly sophisticated and damaging as AI-driven malware and malware-as-a-service platforms turbocharge attacks.

To prepare for these challenges head on, companies must take a more proactive approach to security and resilience. "We've had a traditional way of doing things that's actually worked pretty well for maybe 15 to 20 years, but it's been based on detecting an incident after the event," says Chris Millington, global cyber resilience technical expert at Hitachi Vantara. "Now, we've got to be more preventative and use intelligence to focus on making the systems and business more resilient."

Know your risks

The cybercrime ecosystem is becoming increasingly specialized. Initial access brokers are skilled hackers who are able to gain unauthorized access to corporate networks, which they sell to other cybercriminals. Ransomware-as-a-service (RaaS) groups sell ransomware code or malware to other hackers called "affiliates," who use it to launch attacks and conduct extortion campaigns. And a variety of money-laundering services use cryptocurrency and other schemes to clean the profits gained from cyberattacks. This is making bad actors more effective, dangerous, and lucrative than ever before.

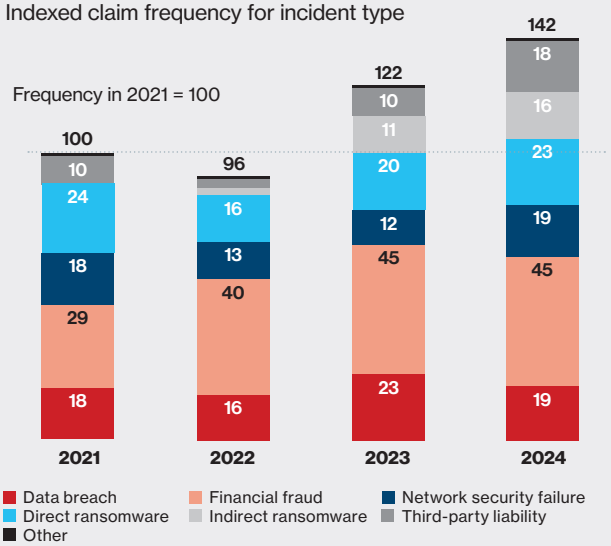
And enterprise networks are increasingly exposed to risk as they spread across different systems, clouds, and locations, and rely on a variety of third-party providers. "The more we do, the more we get plugged in digitally, the greater that attack surface is," says Justin Lam, senior research analyst at 451 Research, part of S&P Global Market Intelligence. "The underlying changes of technology in concert with making data more accessible, that makes us more data-driven, increasing the attack surface as well."

Indirect ransomware – attacks on third-party vendors, business partners, or other organizations that indirectly impact a target – is on the rise too. According to **research by security and insurance firm At-Bay**, indirect ransomware accounted for 11% of cybersecurity claims in 2024, a 43% increase on the year before, while direct ransomware accounted for 16%.[1] In fact, cyber incidents caused by a third party accounted for 31% of all claims filed in 2024, **according to a second cyber-insurer Resilience**. While many businesses may assume that third-party providers are taking the necessary steps to mitigate risk, further checks are often needed.

"Third-party oversight, or TPO, is not a technology – it's a business practice," says Lam. "Companies want their suppliers to certify to them in writing under contractual legal responsibility that they're in full compliance and have adopted a resilient and defensive cyber posture with good hygiene. The problem can be even worse,

Ransomware and third-party incidents continue to rise in 2024

Indexed claim frequency for incident type



Source: Compiled by MIT Technology Review Insights, based on data from At-Bay Insurance Services, 2025

[1] The At-Bay data uses 2021 as its baseline, meaning that a frequency of 16 for indirect ransomware in 2024 equates to a volume of claims equal to 16% of the 2021 total. The actual proportion of claims for 2024, however, is 16 divided by 142 = 11.3%.

because those suppliers have suppliers. It's essentially turtles all the way down," Lam adds, emphasizing the need for all organizations along the supply chain to have effective security measures in place.

Adding to the complexity, regulations are evolving and at varying rates across different jurisdictions. In the US, for example, a variety of regulations cover different aspects of data protection, cybersecurity, and now cyber resilience, from federal laws to state-level legislation and industry-specific standards. Globally, the European Union's Digital Operations Resilience Act (DORA), which came into effect in 2025, mandates that financial firms implement a comprehensive ICT risk management framework, which includes reporting, intelligence sharing, mitigating against third-party risks, and testing of digital operational resilience.

Establish a resilient culture

To address this shifting threat landscape, organizations need to create a resilient business. This requires a holistic approach to security, risk management, and business operations:

- **Executives must lead the charge** on developing an organizational culture of cyber resilience that includes workforce engagement, security awareness programs, and training sessions in areas like compliance and recognizing the limitations and biases of AI systems.

- **Create a system that applies to everyone and works for everyone** – from the C-suite to managers and employees – to avoid exposing vulnerabilities. Disruption often finds its way to a company through the weakest link.

- **Avoid a "set it and forget it" approach** and instead make cyber resilience a business priority, with investment into tools and resources to ensure there is a process of continuous improvement.

"The decision-makers at the top are probably not aware of the impact of a wrong decision," says Millington. "When we talk about education of our employees, this education has to be for everybody at every level. If we have an approach that fits everybody regardless of status, then it's very easy for us to be able to adopt that approach. And, more importantly, manage and secure that approach long term."

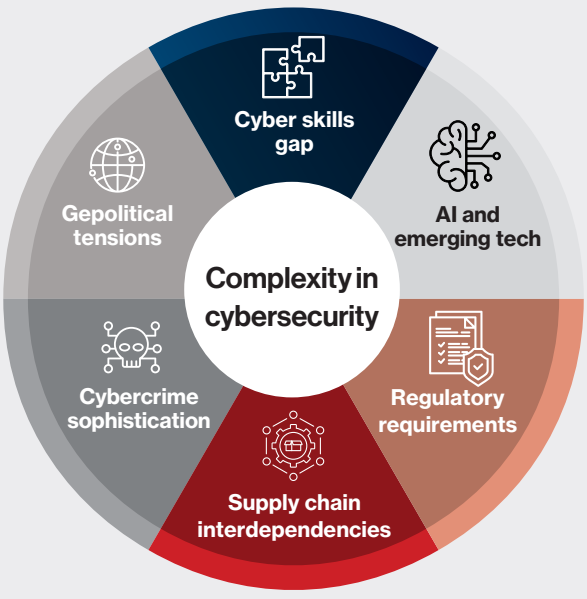
While technical systems can be used to protect the organization, cross-functional training should emphasize the potential security and compliance implications of technical and business decisions made across the company. "Cyber resilience is not just a fancier word for backup and recovery," says Mark Katz, CTO at Hitachi Vantara. "We're in a new realm of data protection and resilience because the nature of the threat has changed. The attack surface is huge; it's your entire company's data assets."

To develop best practices, leaders must turn to other executives in their industry to share insights and ideas, says Lam. "It's about having a real conversation about security, resilience, and risk management," Lam explains. "Being able to say, okay, we've got these other classes of risk out there that may be of existential importance for our business. Inventory, for example; what are all the parts that make up my goods and services and how do I make sure that my supply chain is resilient?" Lam adds.

Lean into AI

Threat actors are already using AI to make their attacks more effective and more disruptive. Nation state-affiliated groups, often linked to governments that engage in cybercrime for political or strategic

Factors compounding the complex cyber landscape



Source: Compiled by MIT Technology Review Insights, based on data from World Economic Forum, 2025

"One of the biggest changes is how serious these attacks are, how serious these adversaries are, and the amount of automation they're able to employ."

Justin Lam, Senior Research Analyst, 451 Research, part of S&P Global Market Intelligence

goals, are **known to have used OpenAI**, for example, to help code malware, gather intelligence, and create more convincing email lures for spear-phishing attacks. Researchers have also detected **early attempts by attackers to use AI agents** to automate initial reconnaissance and probe digital infrastructure.

Ever more sophisticated applications of AI and agentic AI for cyberattacks will certainly continue, says Lam. Organizations must exploit the same tools for defense. "One of the biggest changes that's occurring is how serious some of these attacks are, how serious some of these adversaries are, and the amount of automation that they're able to employ," he says. "In the same way, corporate enterprises and individuals have a lot of automation at their disposal to remediate things."

AI-powered cybersecurity tools can enhance threat detection, automate incident response, and even predict potential attacks and recommend remediation measures. Companies can also use AI to enhance data resiliency solutions. AI excels at simplifying complexity, says Katz. It can help identify important assets, analyze threat data, and codify best practices into daily operations. "It's almost impossible to understand how 1,500 apps relate with each other across tens of thousands of data sets, especially when it's not even clear where the data is," Katz says. "AI can be very good for teasing apart these sorts of intractable things where an administrator has no ability to look at your 50 million files and tell you where the important files are."

Overall, companies need to take advantage of AI's ability to find the mission-critical systems within operations infrastructure. Protecting the integrity and availability of data is crucial in a world where data is often stored in the cloud and regularly accessed by AI systems. Liability and compliance restrictions also mean that companies need to be aware of the status of their data-storage

How to take a layered approach to cybersecurity

There are a number of strategies to enable better data protection and cyber resiliency:

Protect your data

If data is well protected, then recovery is possible. Immutability ensures that snapshots, files, and other data cannot be corrupted or deleted. Role-based access controls, event logging, and data integrity checks ensure authenticity, enhance privacy and security, and provide full audit and search capabilities.

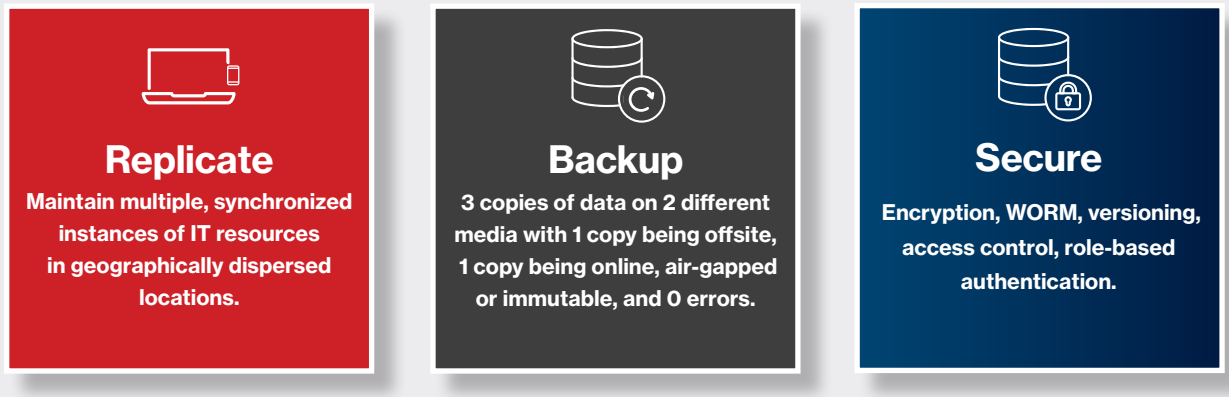
Detect intruders

Bring in technologies and services to help detect and intercept malware at the point of attack. The sooner you know an attack is happening, the sooner the affected systems can be isolated to prevent the spread, which reduces data loss.

Automate recovery

Adaptive production may not always show up in traditional productivity metrics, but its impact lies in sustaining high operational efficiency amid increasing demands for customization, resilience, and sustainability. By preventing potential productivity losses and enabling industries to adapt without sacrificing competitiveness, it represents a vital shift toward a more agile and future-ready manufacturing paradigm.

Protect your data with the right infrastructure and tools



Source: Compiled by MIT Technology Review Insights based on data from Hitachi Vantara, 2025

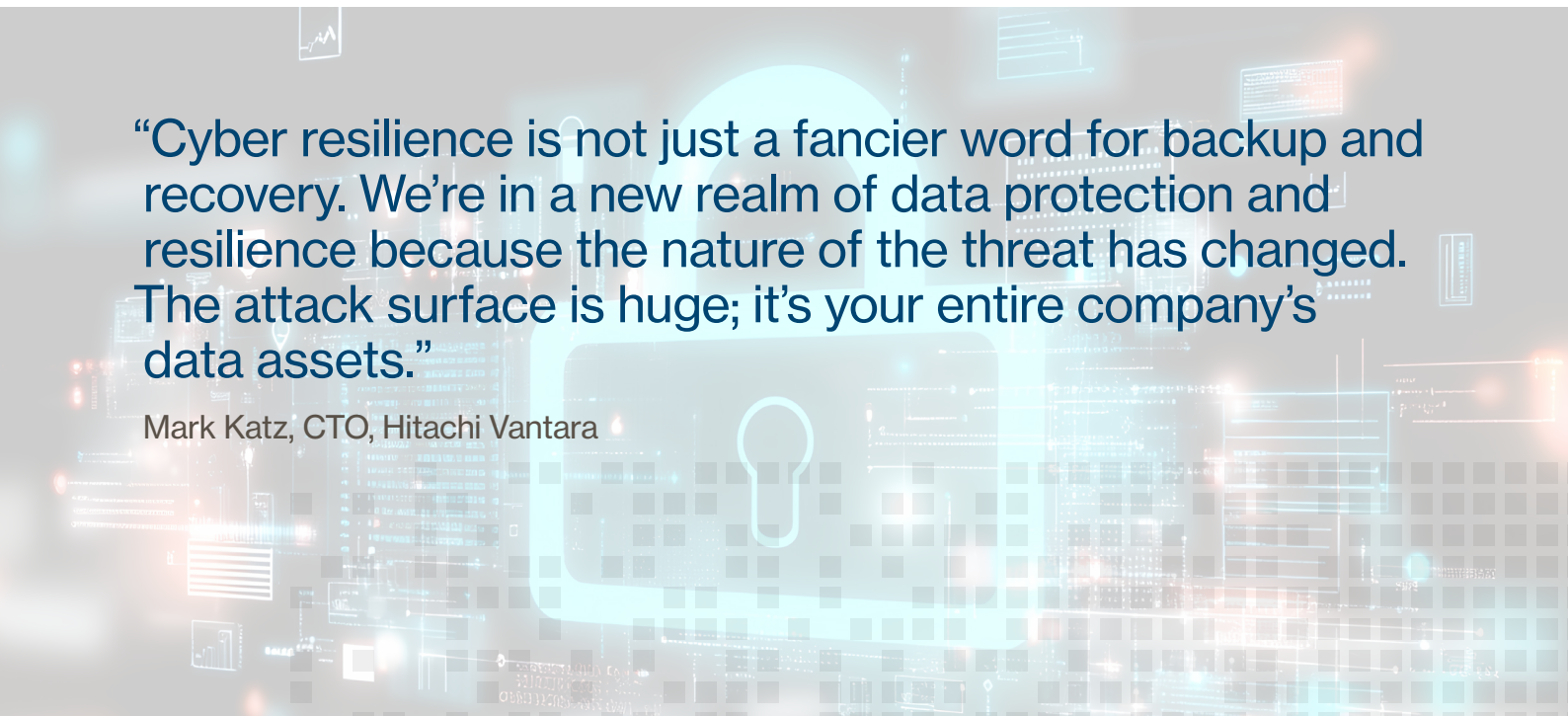
systems and protected data. By planning and practicing the detection of, response to, and recovery from cyberattacks, businesses can minimize disruption.

Proactive cyber resilience for an unpredictable future

A changing landscape of more sophisticated threats, the unknowable interactions between the variety of digital systems that make up a modern business, an ever-growing risk surface area, and the advent of innovative AI applications all make operational disruptions increasingly likely for the under-prepared company.

To adapt to these evolving risks, executives must focus on proactive cyber resilience, says Millington. "We can't know everything all the time, so we've got to keep testing and we've got to keep educating," he says. "You need to develop an openness so that you can evolve very quickly, make the right decisions, and be responsible for the decisions that you make."

The first step for business leaders is to accept that their organization has some work to do to enhance resilience. Then they must determine where their company is in terms of its security posture and identify where the vulnerabilities are. Creating an open culture focused on resilience is also a priority. Executives must empower their people to invest in continuous improvement and set an example by embedding proactive resilience measures into every aspect of the business.



"Adapting to new threats with proactive risk management" is an executive briefing paper by MIT Technology Review Insights. Virginia Wilson was the editor of this report, and Nicola Crepaldi was the publisher. MIT Technology Review Insights has independently collected and reported on all findings contained in this paper.

We would like to thank the sponsor, Hitachi Vantara, as well as the following experts for their time and insights:

Justin Lam, senior research analyst, 451 Research, part of S&P Global Market Intelligence

Mark Katz, chief technology officer, Hitachi Vantara

Chris Millington, global cyber resilience technical expert, Hitachi Vantara

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution — producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad, and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. This content was researched, designed, and written entirely by human writers, editors, analysts, and illustrators. This includes the writing of surveys and collection of data for surveys. AI tools that may have been used were limited to secondary production processes that passed thorough human review.

From the sponsor

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., Hitachi Vantara provides the data foundation the world's 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 **www.hitachivantara.com**.

Hitachi Vantara offers a comprehensive, one-stop cyber resilience solution that simplifies risk reduction and ensures regulatory compliance through tailored assessments and managed services. **Learn more**.

Hitachi Vantara

Illustrations

Cover art from Adobe Stock and spot illustrations created from Adobe Stock and The Noun Project.

MIT Technology Review Insights

www.technologyreview.com

insights@technologyreview.com