IRON MOUNTAIN®

White paper

Protecting data where cybersecurity and global realities converge

Contents

Introduction

Cybersecurity has risen to the top of what executives around the world consider their greatest risk. As discovered during research conducted by Economist Impact in 2023, sponsored by Iron Mountain, global organisations have begun to increase their investments in the ongoing monitoring of cyber risk and in acquiring cybersecurity talent.

To explore the specific challenges of cyber threats and how businesses and governments must address them through targeted investment, collaboration, and partnerships, Iron Mountain hosted a panel at the 2024 World Economic Forum in Davos, Switzerland, featuring world-renowned experts from business, academia, and two of the world's foremost intelligence agencies, moderated by a Pulitzer Prize-winning journalist and author.

This paper includes six themes they consider to be essential for consideration in building resilience in an ever-evolving cyber threat landscape.

Navigating the intersection of geopolitics and cybersecurity

We live in a world where geopolitics and cybersecurity shape a complex and ever-changing landscape. Over the past few years, regional wars and continued rising tensions have upset the global order, challenging trust and security among nations.

Geopolitically, there are shifts in power, emerging alliances, and disruptions to international agreements. China's ascent as a global power along with on-going tension with Taiwan, Russia's expansionist campaigns, and divisive actions by North Korea and Iran—as well as the rise of nationalism in Western democracies—are redrawing geopolitical lines. These shifts and fractures can lead to organizations across the globe being impacted by state-sponsored cyberattacks, either by design or simply as collateral damage.

All too often we become acutely aware of how vulnerable our infrastructure is through highly publicized ransomware attacks such as the SolarWinds, WannaCry, and NotPetya incidents that encrypted victims' data, as well as the Colonial Pipeline attack in 2021 that disrupted fuel supplies along the US East Coast, leading to a ransom payment of millions of dollars to the attackers.

Meanwhile, artificial intelligence (AI) presents both opportunities and risks for cybersecurity. While AI can boost security measures, it also opens doors to more sophisticated cyberattacks. Authoritarian regimes deploying AI surveillance raise privacy concerns, while autonomous weapons fueled by AI raise ethical questions.

When even the most sophisticated systems experience a cyberattack by a state-sponsored organization, it is very difficult—if not impossible—to assemble perfect defenses. An organization's data protection must go beyond keeping cybercriminals out to include a robust recovery strategy and operational steps.

So what do leading organizations do to strengthen their defenses? Chief Information Security Officers (CISOs) and C-level executives must collaborate across industries and borders, leverage emerging technologies responsibly, and prioritize the protection of their organizations and stakeholders in this dynamic and complex landscape. More and more, they are looking to build robust isolated recovery—or air-gapped restoration capabilities—to guarantee a timely recovery of critical information and operations in the event of a cyberattack or data breach.

Achieving heightened fairness, transparency, and trust in AI

When it comes to integrating AI capabilities into an organization's tools and processes, multiple challenges exist, such as biases, lack of transparency, and trust in AI-based models. A significant concern is the built-in bias that exists in the data used to train AI models. These models can inherit biases in the data they are trained on, leading to unfair or discriminatory outcomes. In 2019, for instance, a study by the National Institute of Standards and Technology (NIST) found that many commercial facial recognition systems had higher error rates when identifying individuals with darker skin, leading to concerns about racial bias in these technologies.

These models, primarily based on deep learning models, can be highly complex and opaque. More transparency is essential to understand how an AI model makes decisions to better trust the outputs, especially when critical security decisions are involved. Some AI models are open-source, allowing anyone to inspect the code to understand how they work and get access to private data used in the modeling. As such, they are susceptible to adversarial attacks, where malicious actors manipulate input data to deceive the model into making incorrect predictions or classifications. Another factor requiring further attention is the reliability and completeness of the AI models in real-life scenarios.

CISOs must ensure that AI models used in security applications are free from biases that could result in unfair treatment or discrimination against specific individuals or groups, while at the same time complying with relevant laws and regulations and adhering to ethical principles. It's important to use AI cautiously and carefully evaluate the risks and benefits of adoption. Heightened trust can be achieved through transparency, fairness, rigorous testing and validation, as well as ongoing monitoring and evaluation of their performance in real-world settings.

Staying vigilant in the evolution of cyberattacks

Bad actors in cybersecurity, such as cybercriminals, nation-state actors, unethical hackers, hacktivists, or thrillers, are motivated by various incentives to carry out their activities. Financial gain is a primary motivation for cybercriminals who steal sensitive information, extort money from victims, commit fraud and ransomware attacks, or sell stolen data on the dark web.

Another incentive for bad actors is espionage and intelligence gathering, particularly by nation-state actors or state-sponsored hackers. These adversaries seek to gather sensitive information, intellectual property, or strategic intelligence to gain a competitive advantage or further political agendas.

Some cybercriminals are motivated by ideology or politics, engaging in hacktivism to promote their beliefs or protest against perceived injustices. Hacktivist groups like Anonymous have targeted government agencies, corporations, and organizations to expose corruption, advocate for human rights, or raise awareness about social issues. For example, Anonymous launched distributed denial-of-service (DDoS) attacks against government websites during the Arab Spring protests in 2011 to support pro-democracy movements in the Middle East.

> Understanding these incentives is crucial for CISOs to develop effective cybersecurity strategies to detect, prevent, and mitigate cyber threats posed by various malicious actors. It's important to remember that these examples are just the tip of the iceberg. The motivations behind attacks can be complex and intertwined, and new threats emerge constantly. Organizations must remain vigilant, implement robust cybersecurity measures, and invest in a security culture to protect themselves from the evolving landscape of cyberattacks.

Building boardroom awareness and engagement around cybersecurity

Boards of directors require comprehensive awareness of the risks posed by emerging cybersecurity threats, whether driven by advancements in AI or intersecting geopolitical causes. Despite the potential challenge of boards' limited awareness of cybersecurity risks, there is an opportunity for positive change through enhancing alignment between CISOs and C-level executives.

Here are three changes organizations can make to improve board-level engagement:

Shift the conversation from absolute protection to risk management and resilience

Establish clear lines of communication with business units

Incorporate board members with diverse cybersecurity backgrounds

Shifting the conversation between CISO and the board from protection to resilience despite an anticipated increase in cybersecurity budgets has resulted in advancements. It should be understood that complete protection is unattainable, therefore discussion between CISO and the board should focus on efforts to minimize the risk and facilitate swift recovery.

The second change is to establish clear lines of communication between CISO and C-level executives and business unit (BU) heads to facilitate regular updates on cybersecurity risks and incidents. The CISO can facilitate cross-functional collaboration between cybersecurity teams and other BUs to ensure that cybersecurity considerations are integrated into their strategic decision-making processes. This collaborative approach enhances an organization's resilience to emerging threats and promotes a culture of cybersecurity awareness and accountability at all levels.

Additionally, with regulatory bodies such as the SEC in the United States emphasizing the importance of cybersecurity risk management, boards must adapt by incorporating members with diverse backgrounds and expertise.

> Creating a culture where cybersecurity is consistently prioritized and discussed at every board meeting reinforces its significance as an ongoing commitment rather than a mere annual update. By proactively enhancing cybersecurity awareness and engagement at the board level, organizations can better protect themselves against cyber threats and demonstrate a solid commitment to resilience and security.

Prioritizing education for the next generation

Prioritizing global education on cyber risk awareness and prevention is a matter of societal responsibility and a strategic imperative for long-term cybersecurity resilience. As technology continues to advance rapidly, today's younger generations are growing up in a world where online interactions are ubiquitous.

Investing in educational programs about online risks and safe digital practices can help cultivate future generations that are better equipped to protect themselves, their communities, and their employers from cyber threats.

A significant benefit of cyber awareness education is the potential to mitigate future threats and vulnerabilities. Providing information on good digital hygiene practices early on, such as creating strong passwords, recognizing phishing attempts, and safeguarding personal information, can help prevent common cyber incidents that often stem from human error. This is an opportunity for organizations to conduct regular training sessions to build cybersecurity awareness among employees.

Looking ahead, the importance of cyber education becomes even more critical as emerging technologies like AI and quantum computing reshape the digital landscape. As AI becomes increasingly integrated into daily life, particularly through the use of large language models, the next generation must understand the ethical implications of AI algorithms and the potential risks associated with decision-making. Similarly, as more devices connect through the internet of things (IoT), learning the importance of securing smart devices and the potential consequences of IoT-related vulnerabilities is crucial.

Cyber education also plays a key role in addressing broader societal challenges such as cyberbullying, online harassment, and misinformation. By equipping young people with the skills to critically evaluate online content, identify misinformation, and engage in respectful digital discourse, they are empowered to contribute positively to online communities and combat the spread of harmful content.

Organizations should carry out annual online training sessions, featuring up-to-date content, for all employees who have access to any system. Additionally, tabletop simulations of cyber events involving management should be conducted annually under external facilitation.

> Ultimately, as organizations invest in cyber education they invest in building a safer, more secure, and more responsible digital future for generations to come. CISOs should help lead initiatives to ensure that the next generation of employees will be cyber-savvy leaders who protect their organizations from cybersecurity risks, by design.

Advancing public-private partnerships

Collaboration between public and private organizations is essential for addressing the complex and evolving global risks stemming from geopolitical tensions, cybersecurity threats, and the rapid advancement of AI.

Advancing the public-private relationship can address these challenges through the sharing of threat intelligence and best practices. Public agencies often have access to valuable intelligence about geopolitical risks and cyber threats, while private companies possess unique insights into emerging cybersecurity trends and AI developments. By sharing information and collaborating, public and private entities can enhance their collective ability to detect, prevent, and respond to cyber threats that may arise from geopolitical tensions or malicious actors.

Public-private partnerships may also drive innovation and the development of advanced technologies that counter emerging threats. Collaborative projects between government research agencies, academic institutions, and private companies can focus on developing AI-powered cybersecurity solutions that detect and mitigate cyber threats in real time. By pooling resources and expertise, stakeholders can accelerate developing and deploying innovative technologies.

In addition to technological innovation, partnerships between public and private organizations can also drive policy development and regulatory frameworks that promote cybersecurity resilience and responsible AI governance. Policy-makers and industry stakeholders can develop policies that balance security, privacy, and innovation by engaging in constructive dialogue and sharing insights.

> Public-private partnerships can work together to establish standards and guidelines for AI ethics, data protection, and cybersecurity resilience, ensuring that regulations are informed by industry expertise. Collaboration between public entities such as CISA, FFIEC, FH-ISAC, IANNA, Carnegie Mellon, EU's ENISA, UK's NCSC, and private companies like Crowdstrike and Recorded Future is essential to address the global risks posed by geopolitical tensions, cybersecurity threats, and AI advancements.

Conclusion

It is evident that cyber risk is not transient. It is here to stay at all levels of public and private institutions and daily life. The confluence of significant global happenings such as geopolitical conflicts and the exponential rise in the use of AI, not to mention lingering disruptions in ways of working caused by a global pandemic, demands significant attention and resources toward cybersecurity. To ensure maximum control over the protection of data, and ultimately an organization's reputation, there must not only be collaboration among internal departments but also with partners, vendors, government regulators, academics, and other subject matter experts or associations. CISOs and their teams need to harness the power of the friction caused by the intersection of all these factors to create ever-new opportunities for protecting what matters most to them.

Why partner with Iron Mountain?

For more than 70 years, Iron Mountain has empowered customers around the world to mitigate risks to their brand, reputation, financial status, and ability to serve their customers, patients, or citizens effectively. We help protect against loss of data, vital information, and historical archives in any format; provide secure destruction of physical and IT assets; recommend policies to ensure compliance with regulators; and offer secure facilities to store inventory and precious artifacts—all within a trusted chain of custody framework.

Our Iron Cloud Cyber Recovery Service is designed around a holistic view of security, disaster recovery, and business continuity to support your organization through any of the adverse conditions, stresses, or inevitable compromises of cyber-enabled business.

This fully managed data protection service helps your organization achieve business resilience against cyberattacks and quickly restores data when infrastructure is attacked. We achieve this by simplifying recovery with immutable backups, mitigating risks with AI-enabled anomaly and threat detection, providing thorough ransomware investigation services, and leveraging our advanced Iron Cloud tiered-storage platform.

To mitigate the risk of data loss or exposure on your IT assets and workplace devices, it's also imperative to protect your hardware through effective asset lifecycle management (ALM). When you partner with Iron Mountain ALM, we work with you to develop a program that cares for your assets from deployment and active use to retirement and disposition, supported by our industry-leading data security and sustainability measures.

IRON MOUNTAIN®

800.899.IRON | ironmountain.com

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

USBR-WP-030524A