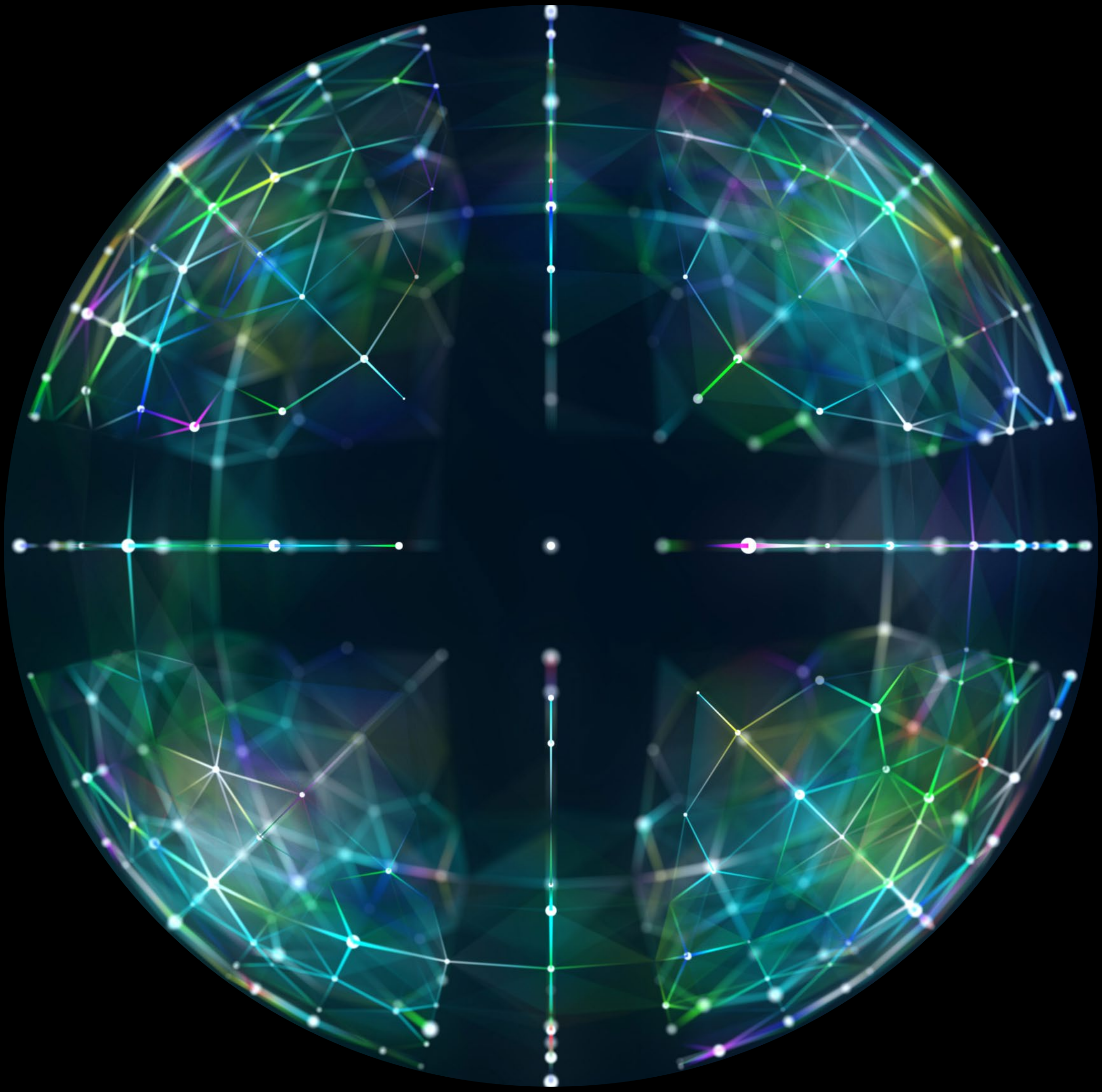
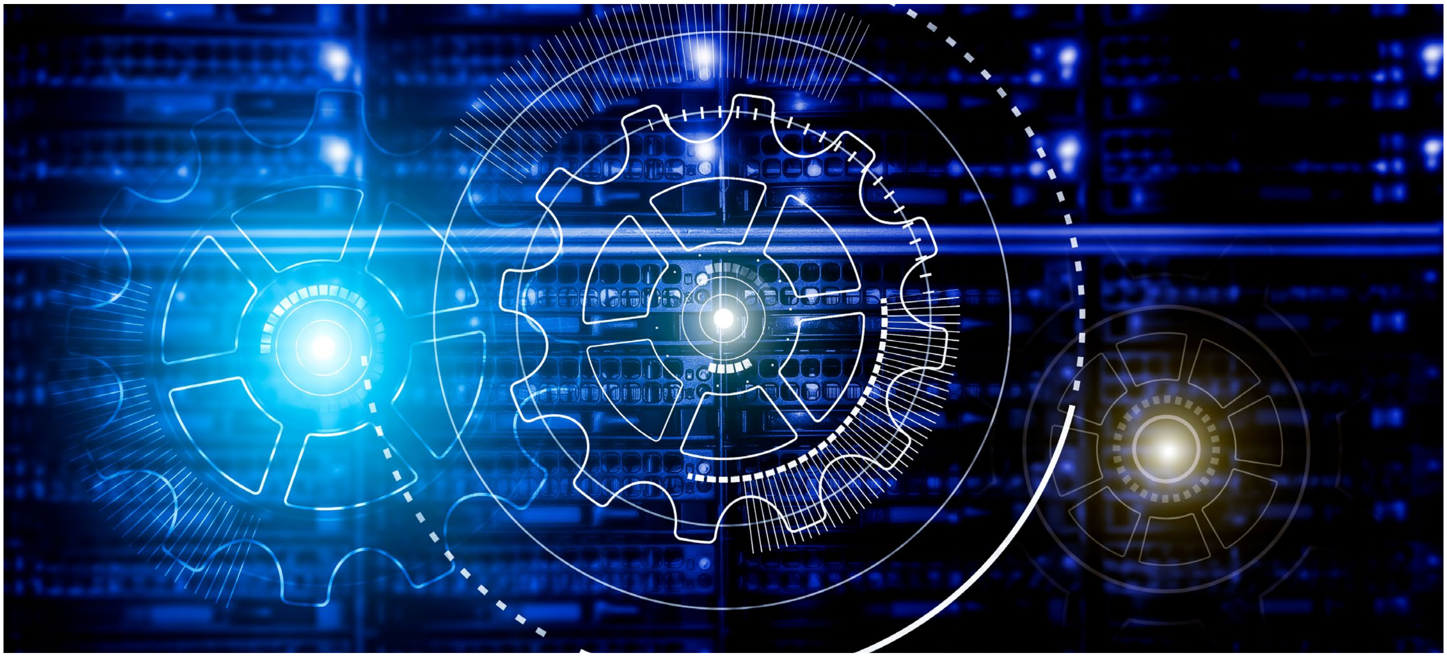
Deloitte.



Building cyber resilience through adoption of emergency management frameworks and principles

February 2025



Introduction

Technological innovation and the growing interconnectedness it enables are reshaping our world through greater efficiencies and higher productivity. But the downside has been greater exposure to cyber risk. From home devices to self-driving cars to the operational technology that runs our critical infrastructure, IP-based technologies now connect nearly every aspect of our lives. This increasing integration of digital and physical systems is expanding the "attack surface" that can be exploited by threat actors, and managing cyber risk and being prepared to respond to a potential cyber disaster is something governments across the world are now grappling with, including the United States and Australia.

Global spending on cybersecurity is projected to reach $300 billion in 2026[1]—a big number, no doubt, but far less than the estimated economic impact of cybercrime globally. In the next four years, the cost of cybercrime is expected to surge from $9 trillion in 2024 to $13 trillion in 2028.[2] While profit motive has been and will continue to be a primary driver of cybercrime, it is but one piece of a larger cyber problem we must contend with. Nation-state and non-state actors may also seek to exploit cyber vulnerabilities to gain geopolitical leverage. Further, they can use cyber vulnerabilities to impose real kinetic effects on whole populations, not just the organizations or devices being targeted. The Colonial Pipeline attack is a case in point: In 2021, a ransomware attack led to the shutdown of one of the largest and most vital oil pipelines in the eastern United States. The consequence was skyrocketing gas prices and gas shortages across large parts of the country. Unfortunately, the Colonial Pipeline attack was not a one-off but a harbinger of a steady rise in cyberattacks since then against critical infrastructure. In 2022 alone, there was a 140 percent increase.[3]

Traditional cybersecurity measures—such as firewalls, identity and access management, endpoint detection and response, penetration testing—will increasingly become an imperative, but they are not a sufficient solution on their own to manage the collective risk we face. Government, industry, and communities need to embrace cyber *resilience* as an approach to planning for what happens when deterrence and security fails. In addition to plugging holes in the dam through strong cybersecurity controls, it is also important to prepare for when the dam breaks. Here, emergency management frameworks, principles, and processes can help us prepare for, respond to, and recover from that "worst-day" scenario—a cyber disaster.

New frontier: Grappling with the nefarious costs of innovation

With the rapid pace of technological advancement, perhaps the most reliable prediction we can make about the future is that change will be constant. Alongside these changes, cyber threat actors will continually evolve their tactics, techniques, and procedures to overcome common security measures. For example, following launch of a publicly available generative AI tool, hackers began harnessing the technology to accelerate, scale, and create ever more authentic phishing attacks. By duping the GenAI tool, they have also been able to write malicious code despite guardrails put in place that it can only "assist with useful and ethical tasks while adhering to ethical guidelines and policies."[4]

We live in an environment where a cyberattack occurs approximately every 39 seconds—and some of these attacks, if successful, pose a real danger to the health and safety of populations the world over.[5] We don't just rely on critical infrastructure for the convenience of reliably getting from one place to another; we need it to keep the lights on, process banking transactions, keep hospitals operational, access clean drinking water, and sustain communications in times of crisis. As defined in the Australian Security of Critical Infrastructure Act of 2018, critical infrastructure includes "physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation."[6] Critical infrastructure is similarly defined in the United States, per the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), as infrastructure that "comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health and safety."[7]

In 2020, a woman in Germany died after a hospital was forced to shut down its emergency department due to a ransomware attack.[8] In May 2022, Costa Rica declared a state of emergency after a devastating ransomware attack crippled government departments' ability to operate.[9] In August 2023, hackers infiltrated Poland's national railway frequency to trigger an emergency stoppage of 20 trains near the city of Szczecin in protest of Poland's support for Ukraine.[10] And, in April 2024, suspected Russian hackers flooded the Texan city of Muleshoe and disrupted its drinking water system by remotely accessing the town's water tower.[11] Yet, despite these glaring headlines, cyber is still often managed as an IT problem with an IT solution.

The consequences of cyber's legacy as an 'IT problem'

Despite the kinetic risk of cyberattacks today, the legacy of cyber as an "IT problem" is still pervasive among leading nations like the United States and Australia. Frameworks such as NIST, MITRE ATT&CK, and Essential 8, although necessary for an effective risk management strategy, mainly offer controls-based technical solutions to reduce vulnerabilities and ensure cybersecurity compliance. The Australian Signals Directorate (ASD) has admitted that "security frameworks only raise the baseline of security" and will not by themselves adequately manage the unique cyber risks facing organizations.[12]

To effectively manage cyber risks, we must extend our thinking beyond control-centric cybersecurity frameworks. Cyber must be viewed holistically, recognizing that cyber incidents are complex, dynamic, and influenced by various factors, including human error, and can have consequences that extend far beyond the boundaries of a security operations center. Relying solely on these frameworks might lead organizations to mistakenly equate framework-led compliance with the capability to effectively respond to and withstand a cyber incident. Managing the consequences of today's cyber threats requires more holistic incident management approaches and broader stakeholder collaboration than cybersecurity frameworks tend to consider.

Government policy is one piece of the cyber resilience puzzle

In recognition of the growing threat from cyberattacks, governments across the world have passed, or updated, policy directives designed to protect critical infrastructure from them. In Australia, the Security of Critical Infrastructure (SOCI) Act identified 11 critical industries for which cybersecurity must be a priority. The United States identified 16 such industries, or sectors, in Presidential Policy Directive 21 (PPD-21), which NSM-22 reaffirmed in 2024. Shown at center in Figure 1, the eight overlapping critical sectors between the two countries accounted for around 45% of the cyberattacks across global industries in 2022.[13]

Australia took an unprecedented step forward in bolstering national cyber resilience with the introduction of the SOCI Act in 2018. The SOCI Act requires regulated entities to embed leading emergency management practices within their security operations centers, including the sharing of near real-time incident information and adopting an all-hazards approach to safeguarding these vital assets. However, SOCI is widely seen in Australia as too narrow in its scope to provide a complete tool for enhancing national cyber resilience, and it ostensibly deflects responsibility for cyber resilience to private entities, many of which still treat cyber as an IT problem alone.

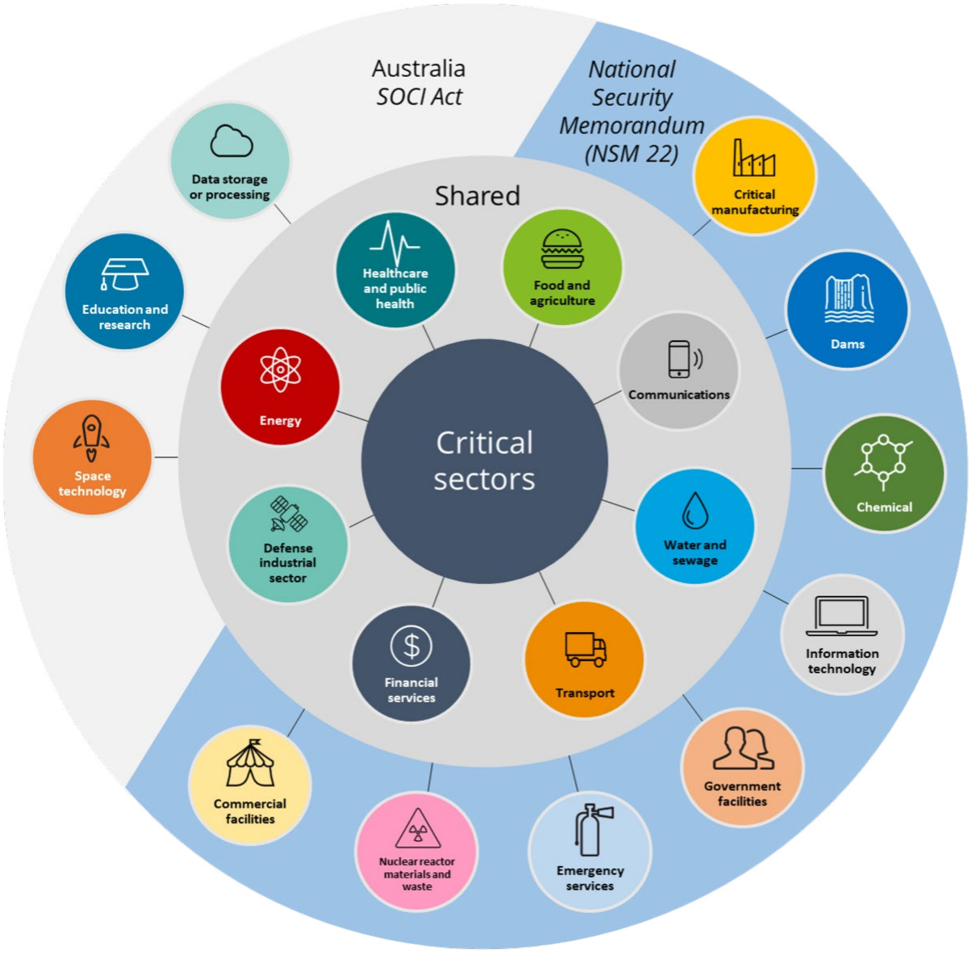


Figure 1: Australia/United States critical sectors overlap

In Australia, the recently released 2023–2030 Cyber Security Strategy reinforces the government's recognition of the need for innovation in the way it addresses cyberthreats; however, that is undermined by a noticeable lack of detail as to how these big ideas will be realized.

In the United States, protecting against cyberattacks on critical infrastructure has been a national imperative since 1998 when the Clinton administration issued Presidential Decision Directive No. 63 (PDD-63), which identified as a national goal the protection of the nation's critical infrastructure from both physical and cyberattacks.[14] In 2003, the Bush administration released Homeland Security Presidential Directive 7 (HSPD-7), which established a national policy requiring federal agencies to prioritize protection of critical infrastructure from terrorist attacks.[15] And, in 2013, HSPD-7 was superseded by the Obama administration's Presidential Policy Directive 21 (PPD-21), which placed emphasis on resilience and an all-hazards approach to critical infrastructure protection.[16] While HSPD-7 departed somewhat from PDD-63 in its emphasis on physical security, PPD-21 refocused on the importance of cybersecurity associated with critical infrastructure protection. It made clear that physical *and cyber* threats were on the same level of priority for the nation.[17] In April 2024, the Biden administration released NSM-22, which replaces PPD-21 and empowers the Department of Homeland Security through the Cybersecurity and

Infrastructure Security Agency (CISA) to lead a whole-of-government effort to secure US critical infrastructure. It reaffirms designation of 16 critical infrastructure sectors and directs federal agencies and departments with regulatory authority "to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure."[18] Further, it adopts a recommendation of the Cyberspace Solarium Commission directing CISA to identify a non-public list of "systemically important entities" (SIEs)—organizations that own, operate, or otherwise control critical infrastructure that if disrupted could cause "nationally significant and cascading negative impacts to national security … national economic security, or national public health or safety."[19] This list will help inform federal, state, and local operational priorities and resource allocation.

In sum, government policy in both the United States and Australia recognizes the vulnerable nexus between cybersecurity and critical infrastructure: A targeted attack on the nation's critical infrastructure could lead to serious consequences beyond the digital realm, including the loss of life, catastrophic damage to property, and the destabilization of systems and networks that underpin a country's national and economic security. However, neither the Australian SOCI Act nor US NSM-22 on their own are sufficient to address the "resilience gap" across critical infrastructure sectors. Closing this gap will require action by stakeholders on several fronts: 1) the willingness of the private sector to collaborate with government, 2) the ability of government to functionally integrate emergency management and cyber incident response capabilities, and 3) a commitment by government to operationally transition away from a reactive posture toward cyber incidents to a preventive one.

Emergency management for cyber incidents

Seeing cyberattacks as more than just an IT problem can expand our way of thinking to include mitigations that may be overlooked by a more traditional understanding of cyber risk management. Because the effects of a cyberattack are no longer confined to IT "dark rooms," neither should our thinking be on how to manage them. This is where the principles of emergency management can help us shift from an exclusively *compliance-based approach* to one of true cyber *resilience*.[20] A focus on resilience, or the capacity of a *whole system* to "anticipate, absorb, adapt to and recover from"[21] a range of disruptive challenges, combines the technical acumen of cyber professionals with the intuition and experience of emergency managers to create the ultimate *cyber emergency response team*.

At a strategic level, governments can incentivize and encourage preparedness activities to span not only chief information security officers (CISOs) and their staff, but the whole community, to include the private sector and emergency management offices.

Bringing emergency management into the cyber domain may take time and require patience by stakeholders on both sides. But, ultimately, strong integration between the two *before a cyber attack* may make the difference between a cyber incident that can be managed and a cyber disaster with long-term, real-world consequences.

When it comes to frameworks and procedures, cyber and emergency management professionals can benefit from mutually integrating their respective approaches. For example, to prepare for an emergency with a cyber component, incident command centers should include a cyber response "section," or emergency support function, to coordinate cyber incident management and share information. For its part, NIST should include procedures for involving—not just notifying—emergency managers when a cyber incident crosses into a life-safety event.

The success of cyber emergency management will depend, in part, on people's ability to think outside the narrow confines of personal experience where cyberattacks and real-world emergencies are distinct phenomena. Without seeing them as potential cause and effect, we may continue to assume they are usually unrelated, and that, in turn, could cause us to continue to prepare for—and respond to—cyberattacks and real-world emergencies in separate spheres. This is a failure of imagination, but the good news is we can break free from that legacy mindset with some simple steps.

What to do next (or first): Rethink how to prepare

The strategic goal of cyber resilience is to create a well-rehearsed ecosystem of responders who can help communities prepare for and bounce back quickly after a cyber disaster. The good news is that individual segments of responders are already rehearsing their individual roles quite well. Traditional cyber wargames and emergency management exercises happen every day and are effective in optimizing isolated segments of a broader response. However, less often do these activities involve all stakeholders who have a critical role to play in preparedness, response, and recovery from *cyber emergencies*. To prepare an organization for a real-world cyber emergency, in which cyber *causes* and kinetic *effects* may not be immediately obvious, what is required is an evolution in how wargames are designed and delivered.

The next generation of cyber wargaming will be more multidimensional, with a focus on the executive's role in managing not just the cyber but the physical fallout of a cyber disaster, as well. Furthermore, these kinds of wargames will represent a new paradigm where cyber defenders and emergency managers sit side by side. In these wargames, the security operations center (SOC) and emergency operations center (EOC) must act as one. This will be a big change for many organizations, and it will require a new approach to wargame design, development, and delivery. But wargaming is one investment organizations can make on the front end to help them shift "left of boom" and build a preventive operational posture, a critical step toward building greater cyber resilience.

Deloitte is uniquely equipped to help public and private organizations prepare for cyber threats by taking a multidisciplinary, integrated approach to wargame design and delivery. We help public and private sector clients derive insights from the wargame experience through data analytics and a focus on programmatic transformation. While there is inherent benefit in the wargame experience—building relationships, strengthening muscle memory, and working through communication and coordination challenges—they can also drive organizational change if developed and implemented as a mechanism for continuous improvement. Our data-enabled insights into which vulnerabilities are mission critical, paired with a persistent focus on closing gaps through repeated exercises, will help ensure that what is learned is not forgotten. Our experience delivering these next-generation cyber wargames can be a transformative first step for organizations grappling with the problems described in this paper. In Table 1, we provide a summary of the challenges described and the ways Deloitte can help.

Table 1: How Deloitte can help

Issue	Need	Solution
1) Cyber may be seen as an IT responsibility and treated as a cost center, rather than a mission enabler and critical investment toward building a viable, resilient enterprise. With the changing threat landscape and potential kinetic impacts from cyber incidents, this "traditional" approach can leave an organization highly vulnerable to operational disruption, reputational damage, and, potentially, impacts on client/constituent safety and security.	• Effective governance structures • Leadership training	• Conduct a "Greenhouse Lab": a one- or two-day facilitated workshop for executives to develop a governance framework in which roles and responsibilities are defined and potentially reimagined through "design thinking" approaches • Conduct executive training for leadership on risk management and building organizational cyber resilience • Develop and adopt a strategic plan for organizational transformation
2) Organizations may not have in-house talent experienced in emergency management or implementation of relevant frameworks, such as the Incident Command System, National Incident Management System, or NSM-22. Or, if they do, they are siloed within the organization and not well integrated with information security functions.	• Common understanding of relevant threats and hazards • Reduction of barriers between siloed parts of the organization to enable an effective "whole-of-enterprise" approach to cyber resilience; similarly, need to break down barriers between government and private industry • Integrate NIST and other IT risk management frameworks alongside emergency management frameworks	• Incorporate cyber into existing all-hazards emergency management frameworks at the state and federal levels • Conduct an enterprise-wide cyber hazard and risk identification program • Develop a risk register to document potential risks, their likelihood, potential consequences, planned mitigation measures, and who's responsible for them • Adopt and integrate relevant frameworks across the enterprise, including educating stakeholders on how to implement them • Conduct cross-sector stakeholder engagement and outreach • Establish cyber hazards leadership role within state emergency management frameworks to support a coordinated approach to managing cyber hazards (address gaps in legislative framework) and support knowledge sharing
3) Stakeholders are ill-prepared to respond to cyber disasters due to inadequate hazard awareness and training. Many organizations conduct cyber wargames and emergency management exercises separately, if at all, and they do so the same old (boring) way.	• Greater public awareness of cyber hazards and participation in simulation exercise to increase preparedness • Effective and realistic plans, policies, and playbooks	• Utilize cyber crisis simulation exercises and cyber wargaming to explore the full range of potential kinetic effects and to increase cross-sector interoperability • Utilize Deloitte WATCH, which brings order to the process and ensures a persistent throughline from objectives to outcomes; using real data, modeling and simulation (M&S)—Deloitte FutureScape, CentralSight—can enable an exercise/wargame that "deals in facts" right away and reduces scenario speculation by participants, which allows participants to spend every minute on solutioning • Prepare, train on, and exercise playbooks and crisis communications plan
4) Lack of resources to implement necessary remediation measures	• Mapping of available resources and guidance on how to strategically deploy them	• Utilize our grants management team, which can provide strategic guidance on federal and other funding sources available to clients

Authors

Jeff McLeod
Specialist Leader
Deloitte & Touche LLP
jemcleod@deloitte.com

Shannon Heathcote
AUS Director—CIR3
Deloitte Services Pty Ltd
sheathcote@deloitte.com.au

Georgia Ryan

Endnotes

1. See International Data Corporation (IDC), "New IDC spending guide forecasts worldwide security investments will grow 12.1% in 2023 to $219 billion," press release, March 16, 2023.
2. Anna Fleck, "Cybercrime expected to skyrocket in coming years," Statista, February 22, 2024.
3. Jonathan Reed, "High-impact attacks on critical infrastructure climb 140%," *Security Intelligence*, June 26, 2023.
4. Jim Chilton, "The new risks ChatGPT poses to cybersecurity," *Harvard Business Review*, April 21, 2023.
5. Gene Yoo, "The importance of time and speed in cybersecurity," *Forbes*, January 22, 2021.
6. Australian Department of Home Affairs, Cyber and Infrastructure Security Centre, Security of Critical Infrastructure Act 2018 (SOCI), accessed October 2024.
7. The White House, National Security Memorandum on Critical Infrastructure Security and Resilience, NSM-22, April 30, 2024.
8. Associated Press, "German hospital hacked, patient taken to another city dies," September 17, 2020.
9. Matt Burgess, "Conti's attack against Costa Rica sparks a new ransomware era," *Wired*, June 12, 2022.
10. BBC, "Poland investigates cyber-attack on rail network," August 26, 2023.
11. Sean Lyngaas, "Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says," CNN, April 17, 2024.
12. Edward Kost, "13 biggest data breaches in Australia," UpGuard, updated September 16, 2024.
13. Ani Petrosyan, "Distribution of cyberattacks across worldwide industries in 2023," Statista, March 22, 2024.
14. John D. Moteff, *Critical infrastructures: Background, policy, and implementation, Congressional Research Service*, updated June 10, 2015.
15. Cybersecurity & Infrastructure Security Agency (CISA), Homeland Security Presidential Directive 7, December 17, 2003.
16. Moteff, *Critical infrastructures: Background, policy, and implementation*,
17. Ibid, p. 14.
18. The White House, National Security Memorandum on Critical Infrastructure Security and Resilience.
19. Ibid.
20. Paul E. Roege et al., "Bridging the Gap from Cyber Security to Resilience," in Igor Linkov and José Manuel Palma-Oliveira (eds) *Resilience and Risk* (Springer, 2017), p. 386.
21. Ibid.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Created by CoRe Creative Services. RITM1999845

MAKING AN IMPACT THAT MATTERS since 1845