Guidehouse

outwit complexity™

Securing Critical Infrastructure in an Age of Cyber Warfare

As cyber threats grow in complexity and frequency, critical infrastructure organizations must develop proactive cyber protection and prevention strategies to secure essential operations.

Increasingly sophisticated cyber threats pose potentially severe consequences for critical infrastructure organizations. As the cyber risks facing critical infrastructure continue to grow, building a strong cyber protection and prevention program is essential to mitigating risk.

In an age where crime and warfare take place in a digital context, organizations in critical infrastructure sectors face very real threats and must prepare for the likelihood that they could be targets for cyberattacks from foreign nations or cyber criminals. Successful disruptions from cyberattacks have the potential to be catastrophic for critical infrastructure organizations and the citizens they serve.

The Potential Impact of Modern Cyberattacks

According to the World Economic Forum's Global Risks Report 2023, as cybercrime rises, "attempts to disrupt critical technology-enabled resources and services will become more common, with attacks anticipated against agriculture and water; financial systems; public security; transport; energy; and domestic, space-based, and undersea communication infrastructure."[1]

In its *Digital Defense Report 2022*, Microsoft said that the proportion of nation-state attacks—i.e., those with technological, financial, or other support from a sovereign state—against critical infrastructure doubled from 20% to 40% between July 2021 and June 2022. The most common targets were government agencies, non-governmental organizations, and intergovernmental organizations (29%), followed by infotech (22%), education (9%), finance (5%), media (4%), transportation (2%), communications (2%), and healthcare (2%).[2]

In 2021, the US experienced high-profile cybersecurity breaches at water treatment facilities. Hackers breached systems in water treatment facilities in the San Francisco Bay Area and in Oldsmar, Florida, as part of attempts to poison those water supplies. Later in the year, water treatment plants in Nevada, Maine, and California were hit by ransomware attacks on the supervisory control and data acquisition systems that control OT operations. These incidents demonstrated that limiting access to potable water is now one of many strategies in the arsenal of cyber criminals or terrorists focused on damaging critical infrastructure.

Modern Warfare

In March 2022, the Cybersecurity and Infrastructure Security Agency (CISA), in conjunction with the FBI and NSA, issued a cybersecurity advisory encouraging US critical infrastructure organizations and state and local government agencies to prepare for the threat of Russian state-sponsored cyberattacks. In line with that advisory, we're now witnessing the increasing use of cyberattacks in modern warfare. Since Russia began waging war against Ukraine in February 2022, there have been numerous cyberattacks impacting the distribution of medicine, food, and relief supplies in targeted areas. In 2022, Russian government-backed attackers targeted users in Ukraine more than any other country, according to Google's 2023 Fog of War report. Russian government-backed attacks on users in Ukraine were up 250% in 2022 compared to the 2020 baseline, according to the report.[3]

[1] Global Risks Report 2023 | World Economic Forum | World Economic Forum (weforum.org)

[2] Microsoft Digital Defense Report 2022

[3] Fog of war: how the Ukraine conflict transformed the cyber threat landscape (blog.google)

Protecting Critical Sectors

CISA recognizes 16 sectors in which cyberattacks could have a "debilitating effect on national security, national economic security, national public safety, or a combination thereof."

Those sectors are:

- Chemical
- Communications
- Commercial facilities
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

How to Build Cyber Resilience in Critical Infrastructure

The tempo, frequency, and sophistication of attacks will only continue to intensify. Organizations must take urgent, proactive steps, such as creating a companywide strategy to continuously build and review resilience against cyber threats, rather than waiting to react after an attack has occurred.

Based on Guidehouse's decades of experience helping critical infrastructure and government organizations build cybersecurity strategies, our team recommends the following steps:

1. Fortify the security of perimeter defenses. Assess key assets (staff, applications, data, vendors), along with critical points of failure, and review maximum allowable downtime estimates to manage risk exposure.
2. Review whether the current level of downtime is still acceptable. Frequently, organizations find that what was acceptable three to five years ago is no longer tolerable. Segregate OT and mission-critical IT resources from the rest of the organization to minimize the impact of an attack on those systems.
3. Run scenario-based simulations to prepare for an attack and identify gaps in security and resiliency plans. Develop a plan for dealing with security gaps that includes obtaining sufficient funding and resources. Demonstrate the severity of risks and threats to stakeholders.
4. Review and enhance incident response and crisis management capabilities, recovery and communications plans, and contact lists. Open clear escalation channels to high-risk areas of the organization to establish rapid response capabilities.
5. Review and confirm agreements for third-party incident-response support by asking questions such as, Is my organization guaranteed priority support, even in the event of widespread problems? Is this adequately documented in service-level agreements? Is there a back-up or alternate provider?
6. Implement security best practices and guidance provided by security frameworks, such as NIST 800-53 and 800-171.

Critical infrastructure organizations must also commit resources to proactively and regularly look at guidance offered by the FBI and other agencies. This guidance provides information on the latest concerns and the ever-changing cybersecurity landscape.

The Complex Relationship Between IT and OT—An Energy Example

The intrinsic connection between IT and OT systems means that a robust, holistic strategy is needed to secure both simultaneously. An energy organization's typical threat landscape, for example, is made up of IT and OT architectures, including both legacy and modern systems. It may also include disparate systems acquired via mergers or acquisitions that struggle with interoperability and lack a coherent, consistent governance structure.

Integrating the right tools into control, transmission, generation, distribution, and field networks while remaining compliant requires custom solutions with open standards and APIs to assist with streamlining. The mix of legacy and new equipment means that some infrastructure can't be patched or hardened, and instead requires a risk management approach that includes network segmentation, intrusion detection, and endpoint detection and response.

Successfully meeting this asymmetrical IT challenge requires a multifaceted approach. The risks involved cannot be averted by the purchase of a "point product" or an additional audit. Energy companies need holistic assessments and strategies that integrate cyber hygiene and compliance to better protect distributed systems and build organizational resilience.

Benefits of a Cyber Resilience Strategy

Ensuring you have a strategy in place to defend your critical infrastructure organization—and the people you serve—against sophisticated cyber threats will allow you to:

- Build greater cyber and organizational resilience
- Protect your sensitive data (and that of your customers)
- Minimize downtime to operations and IT services
- Maintain business continuity
- Protect your organization's reputation
- Combat cyberattacks before they have an impact

Completing a comprehensive risk assessment and resiliency program can also unearth opportunities to cut costs, reallocate resources to higher-value areas of the organization, and streamline operations.

An Ongoing Effort against Cyber Threats

Nation-state threats, particularly if government-led or government-funded, will be highly resourced, highly skilled, and highly intelligent, with a specific goal in mind. They should not be underestimated, especially in industries related to critical infrastructure.

Organized crime has also been involved in ransomware attacks in a variety of critical infrastructure sectors and can be expected to increase the breadth and complexity of its attacks as well. Phishing-as-a-Service (PhaaS) attacks, especially in healthcare and finance, are expected to rise as criminals attempt to gain identity information and sensitive data.

Critical infrastructure sectors can't simply hope they'll survive a cyberattack. If an IT network is down or under attack, the organization's entire operations can suffer, as can service to customers and public perception of the organization. These are risks you simply cannot afford to take.

Cybersecurity and resilience preparations require an experienced partner who understands technology, security, governance, and risk and can provide a comprehensive and robust strategy for addressing today's growing challenges.

Guidehouse's credentialed subject matter experts in cybersecurity, enterprise risk management, IT strategy, enterprise data management, IT modernization, and program management can address these challenges at all levels of an organization. We have supported clients with worldwide presence and mission requirements, as well as specific missions within an organization, to build a strong track record of success in protecting critical infrastructure.

Contacts

Nong Nai
Director, Cyber
nnai@guidehouse.com

Glenn Nick
Associate Director, Cyber
gnick@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit www.guidehouse.com.

guidehouse.com/cybersecurity @GHTechSolutions linkedin.com/guidehouse-technology-solutions/