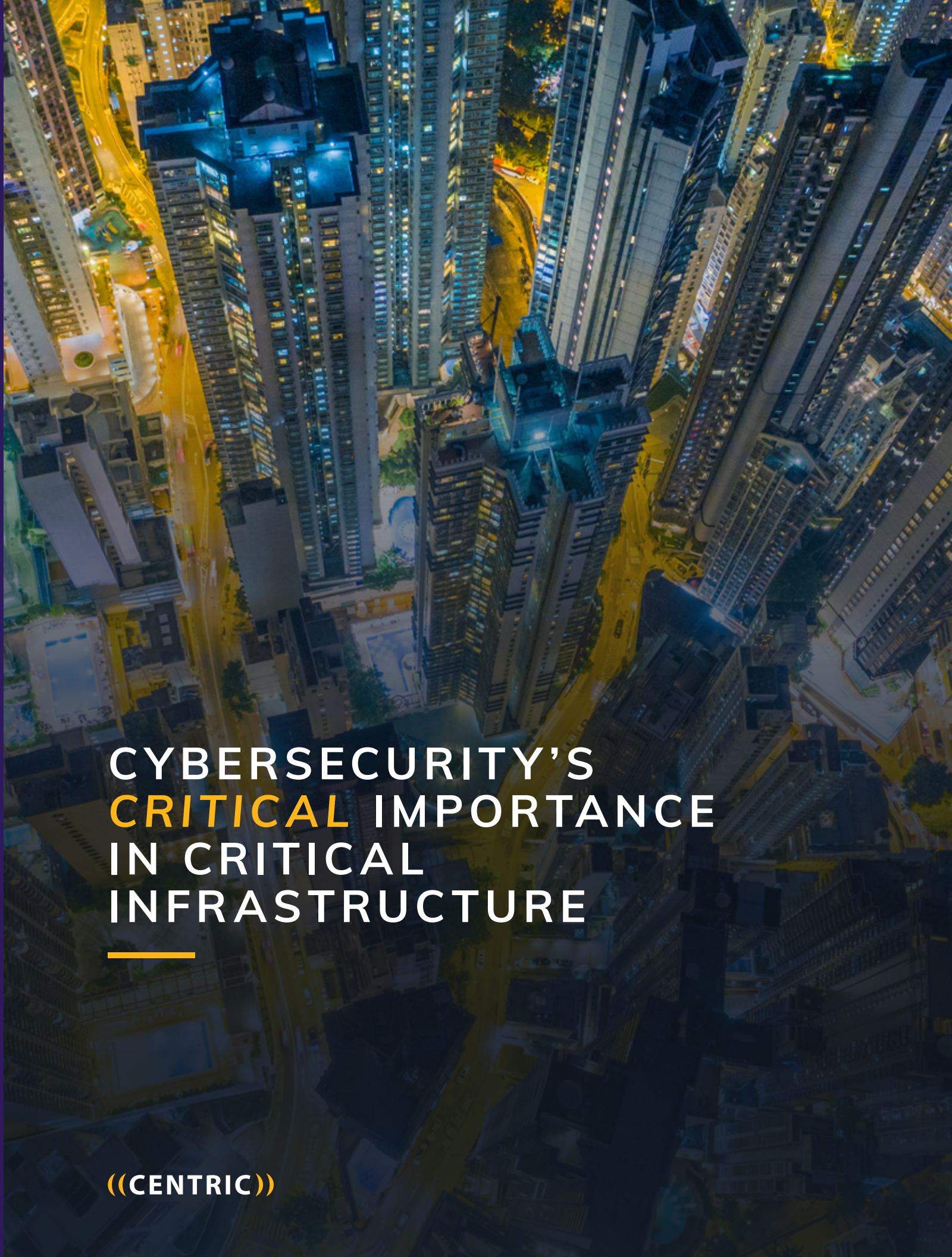


CYBERSECURITY'S *CRITICAL* IMPORTANCE IN CRITICAL INFRASTRUCTURE

((CENTRIC))

In July 2024, CrowdStrike, a leading cybersecurity company, caused a major outage that took out several critical industries due to a software update gone wrong.

Because the update addressed Windows systems, several users and industries that primarily use Microsoft products experienced outages that took from several hours to several days to resolve. If you were traveling at this time, you might have seen its impact on airlines.

However, the outage affected more than our ability to travel. It also impacted critical infrastructure, including banks, hospitals, 911 lines, and even the London Stock Exchange.

We define critical infrastructure as systems crucial for daily life — whether personal, business or health-related. The failure of these mission-critical systems can affect quality of life and, in some cases, life itself.

While the CrowdStrike incident wasn't a hack, it demonstrates our dependence on seamlessly operating systems. Hackers know this, and they are increasingly targeting our critical infrastructure for cyberattacks. For example, the SolarWinds attack in 2020 allowed hackers to break into organizations worldwide that used SolarWinds' Orion platform for network monitoring. The attack gave bad actors access to sensitive personal information, remote access to customer networks, and more.

Unfortunately, many critical infrastructure systems are inherently vulnerable, outdated, and lack necessary patches, making them susceptible to basic attacks. Various actors, including state-sponsored hackers, company insiders, and even amateur hackers, can exploit these vulnerabilities.

The FBI's 2023 Internet Crime Report found that over 40 percent of ransomware attacks reported to the Bureau targeted critical infrastructure. It's also being targeted more within warfare, such as in the Russia-Ukraine conflict, where systems, hospitals, manufacturing facilities, and energy infrastructure are prime targets.

With a strong security posture, organizations can take vital steps toward protecting their businesses and the people they support every day. We'll explore seven of those steps here after considering the unique security threats faced by four of the Cybersecurity and Infrastructure Security Agency's (CISA) defined sectors:

- Utilities: Energy, Water and Wastewater Services
- Healthcare and Public Health
- Financial Services
- Critical Manufacturing

UTILITIES: ENERGY, WATER AND WASTEWATER SERVICES

Energy, water and wastewater services, also known as utilities, are cornerstones of critical infrastructure due to their essential role in everyday life. Without access to heating, cooling or clean water, people are at risk of heatstroke, severe dehydration, illness, and even death.

According to the Environmental Protection Agency (EPA), cyberattacks against water utilities are becoming more frequent and more severe. In 2023, Sandworm, a Russian military unit, attacked utilities serving small towns in Texas. While the impact was low, the same group had caused blackouts in Ukraine.

What leaves utilities open to such attacks? To start, many utility systems were not designed with modern security in mind.

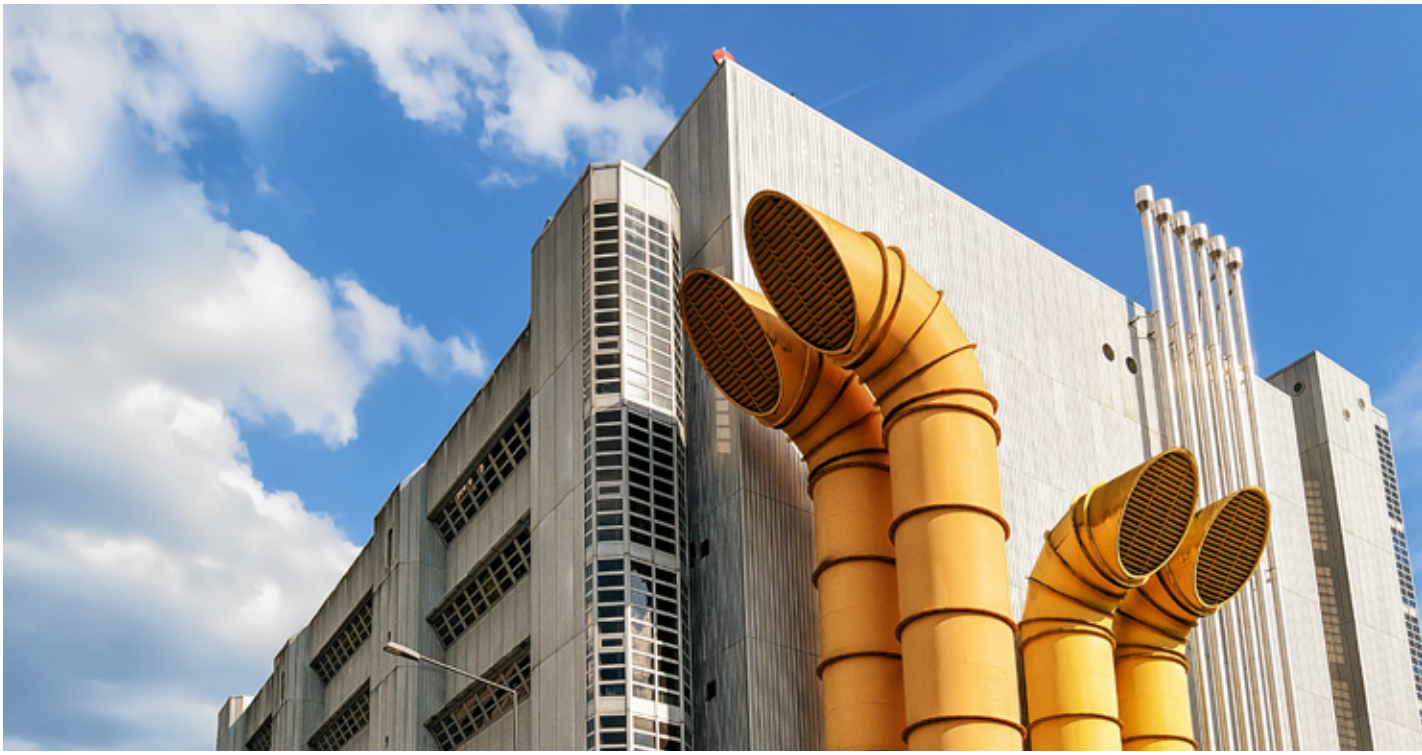
Penetration tests often reveal unpatched vulnerabilities that are costly to fix – when they can be fixed – and even costlier to replace when a fix is unavailable. This has also led to industry pushback when it comes to cybersecurity mandates. The EPA even pulled back from requiring cyber risk assessments for water utilities due to such resistance.

Plus, using both old and new technologies together creates problems. For example, automatic meters are less secure than their manual predecessors but more secure when securities invest in smart grid cybersecurity.

Utility cyber maintenance is limited because utilities need high uptimes. For example, electric utilities have thousands of miles of exposed physical remote assets, such as power lines, substations and more. An attack on any one of these assets could have cascading effects for thousands of utility customers.

Lastly, lack of talent, silos between IT and operational teams, and a reliance on third-party software vendors all leave utilities open to everything from deliberate attacks to badly timed firmware updates.

While attacks on utilities can impact everyone, there are even more personal sectors to consider: our healthcare system.



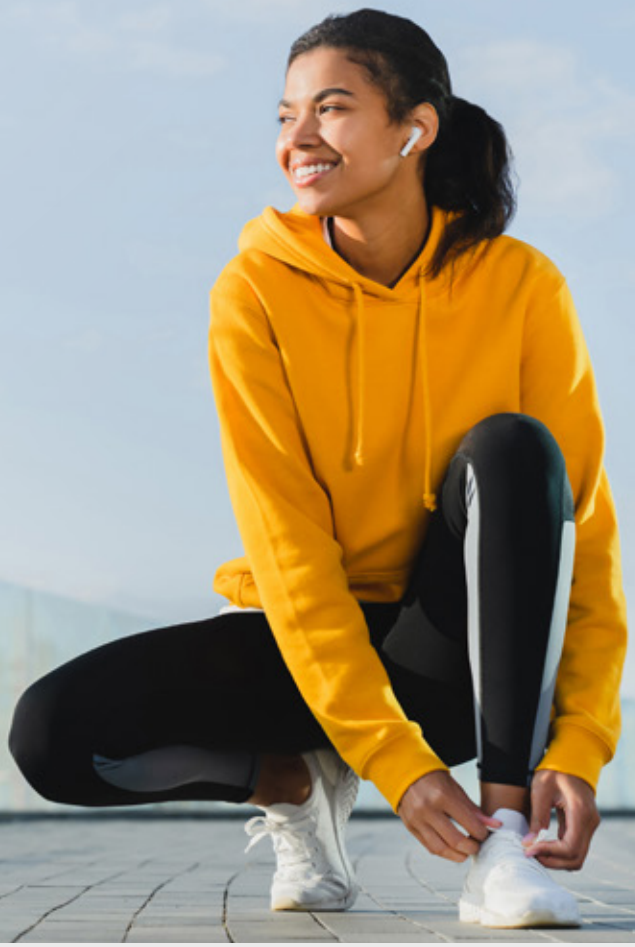
HEALTHCARE AND PUBLIC HEALTH

Healthcare and public health directly affect human lives every day. Cyberattacks on healthcare systems can have severe consequences, including increased mortality rates and compromised patient privacy.

In fact, a recent ransomware attack on Ascension, a major U.S. hospital network, may have done both. While the attack allowed cybercriminals to steal patient files, it also left nurses without access to patient records. Given the sheer amount of data that healthcare organizations process each day and their need to stay current with Health Insurance Portability and Accountability Act (HIPAA) regulations, the attack put a massive strain on hospital operations.

Cyberattacks like this one can actually lead to an increase in patient mortality. While 3 in 100 hospitalized Medicare patients will die at the hospital in normal circumstances, the number becomes 4 in 100 during a cyberattack.

The healthcare industry is also increasingly reliant on interconnected systems. That was another reason the hospitals were so overloaded during the Ascension attack – hospitals and pharmacists were no longer interconnected, so it took longer both to process prescriptions and to maintain the proper checks and balances between hospitals and pharmacies. This interconnectivity also means that if one part of a system is hacked, it's that much easier to get into another.



HEALTHCARE AND PUBLIC HEALTH

Hackers can find interconnectivity vulnerabilities in portable devices that hospitals and other healthcare organizations ask their patients to wear, such as wristbands for tracking patients, insulin pumps, and even pacemakers. Like utilities, the IT infrastructure can't always keep up with all these devices, leaving them vulnerable to attack, even in their own buildings.

One unique factor hospitals share is that anyone can typically access their buildings 24/7. As a result, the public can walk into their facility and even plug into its local area network (LAN) connection in a patient's room, leaving the network vulnerable to both accidental and malicious attacks.

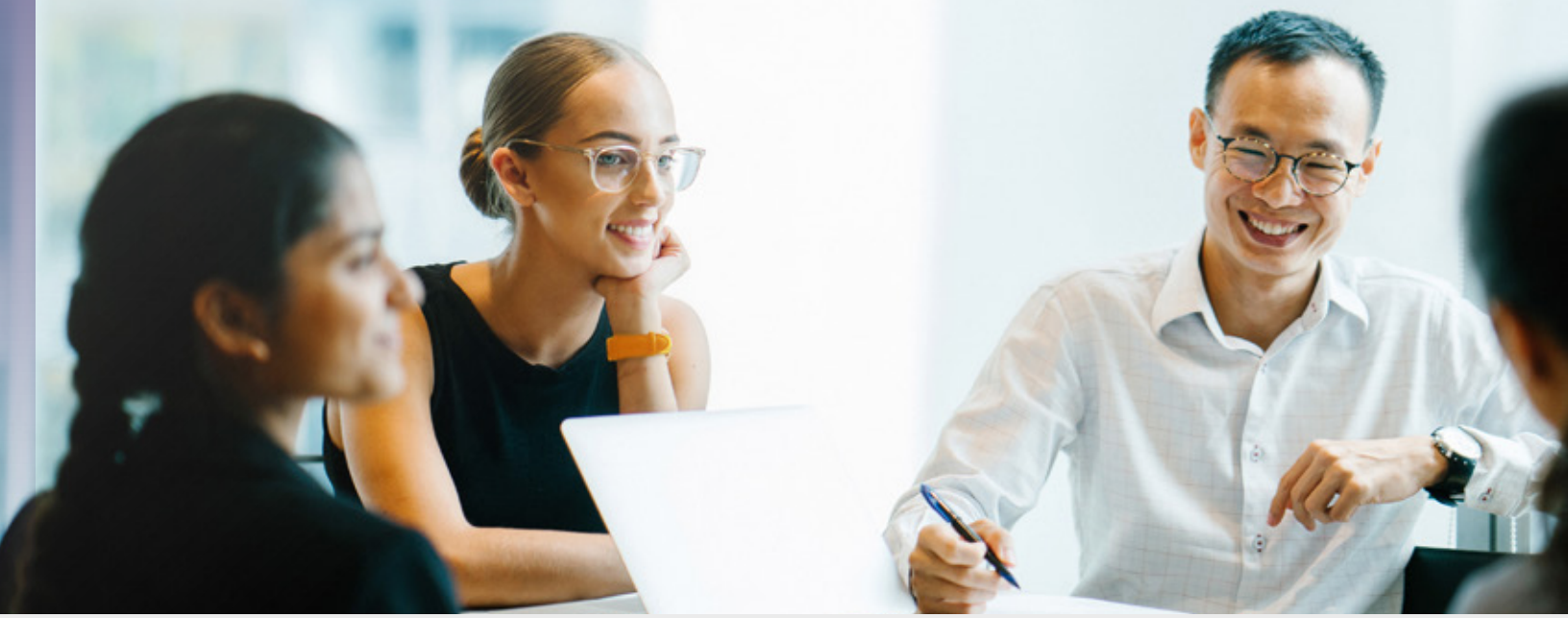
Network vulnerability also opens the healthcare industry to social engineering attacks, which can exploit the emotional stress of patients, their families, and healthcare staff. If a malicious actor emails a distraught parent while they are in the hospital, for example, and the parent then plugs directly into the LAN port to reply, they could inadvertently infect the hospital's network with malware.

Such emotional manipulation can also bring down several critical infrastructure sectors, including financial services, that directly impact individuals and societies.

FINANCIAL SERVICES

According to the International Monetary Fund (IMF), cyberattacks committed against financial services organizations are a "serious threat to global financial stability." They've cost financial firms $12 billion in the past 12 years alone. A recent attack on the U.S. division of the largest bank in the world, ICBC, even disrupted U.S. Treasury trades. The financial services' inclusion in CISA's list of critical infrastructure sectors is clear: bad actors could exploit their role in maintaining the economy and access to consumers' sensitive personal information and trust to the detriment of entire countries.

Worse still, almost anyone can manipulate financial services, leading to huge losses or gains. A few individuals on social media manipulated GameStop stocks, causing a short squeeze and hedge funds to lose out financially. After a bank run, where several companies needed to withdraw cash all at once, Silicon Valley Bank became one of the largest bank failures in the U.S. since 2008. Both examples also highlight the real-time nature of the finance business, which leaves very little room for downtime to install updates or security patches.



There are also often different types of attacks with different purposes behind them:

- **Some groups infiltrate markets to steal money or personal information.**
- **Some are there to disrupt the system.**
- **Others work toward a larger goal of bringing the entire financial system down.**

Attacking financial services organizations becomes easier when they still rely on legacy technology. While the technology is good for high-volume transactions, it can also cause issues because many data centers are still on-premises. This becomes a problem because of the expense involved in maintaining the physical services, the length of time it can take to back up servers, and the number of people trained to maintain them.

Payment processors and some aspects of banking services also tend to be more modern than investment services. Interconnecting newer systems with legacy systems leaves both open to attack as bad actors seek out vulnerabilities in older or undermaintained software.

Because the financial services industry has access to sensitive personal information, including everything from customers' biographic data to PINs and card validation codes, these organizations are also heavily regulated. As with healthcare and utilities, processing and protecting the data financial services collects, as well as ever-changing regulations, makes compliance difficult.

When companies involve third-party vendors in data processing, such as credit card processors, compliance becomes more complicated as organizations must review their own policies along with their vendors. If companies miss something during that review, vendors could not only cause the financial organization to face large fines but also cause a rift in trust with the organization's customers.

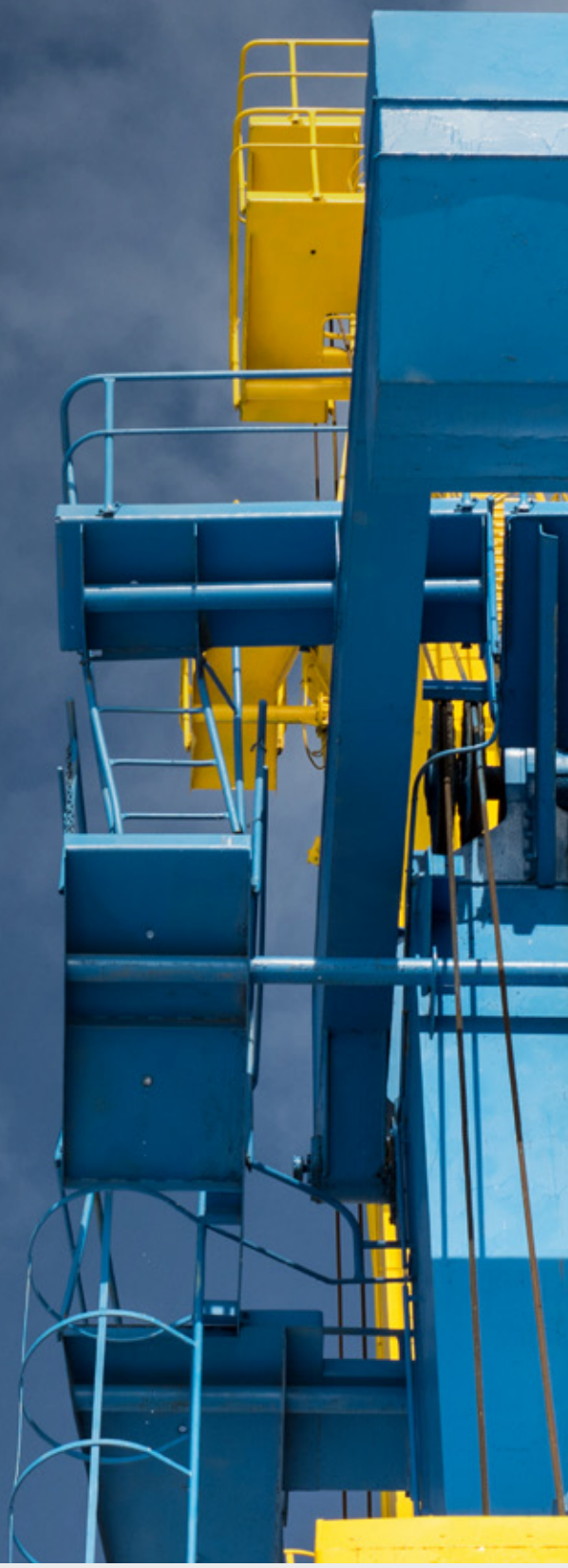
Reputation in finance can make or break an organization. It's also vital to critical manufacturing or supply chain.

CRITICAL MANUFACTURING

Critical manufacturing or supply chain underpins global commerce and plays a vital role in a country's economic stability and ongoing operations. An attack on or disruption to key components of this industry could significantly affect essential national functions and multiple other critical infrastructure sectors like those mentioned previously.

According to CISA, four primary industries serve as the hub of this sector:

- **Electrical Equipment, Appliance, and Component Manufacturing**
- **Machinery Manufacturing**
- **Primary Metals Manufacturing**
- **Transportation Equipment Manufacturing**



The best illustration of how disruption to the global supply chain can affect us is the COVID-19 pandemic. As safety restrictions limited the number of people allowed to work in one location, manufacturers couldn't produce goods quickly enough for consumers. The result: shortages and shutdowns as ports became congested and costs skyrocketed.

As we saw with utilities, geopolitical tensions can also exacerbate cybersecurity threats to supply chains, which we've seen during the Russia-Ukraine war. Manufacturing sectors become prime targets of cyberattacks due to their involvement in manufacturing weapons or providing aid. The goal could be to break down the supply chain altogether or to steal proprietary information such as trade secrets.

Cyber attackers may also infiltrate manufacturing networks to extract valuable data, which they can then use to replicate products, undercut prices, or gain a competitive edge. State-sponsored espionage poses an even greater threat, as it can be part of broader strategic objectives to weaken economic competitors.

The supply chain's integrated nature means that attacks can have cascading effects across multiple stages of production. Cyber attackers can target suppliers to introduce vulnerabilities that spread throughout the supply chain. This can compromise quality control processes, leading to the production of defective or unsafe products.

Additionally, hackers can disrupt distribution stages, delaying the delivery of essential goods. As a result, a single cyber incident can affect not only one company but an entire network of businesses, emphasizing the need for comprehensive cybersecurity measures at every supply chain stage.

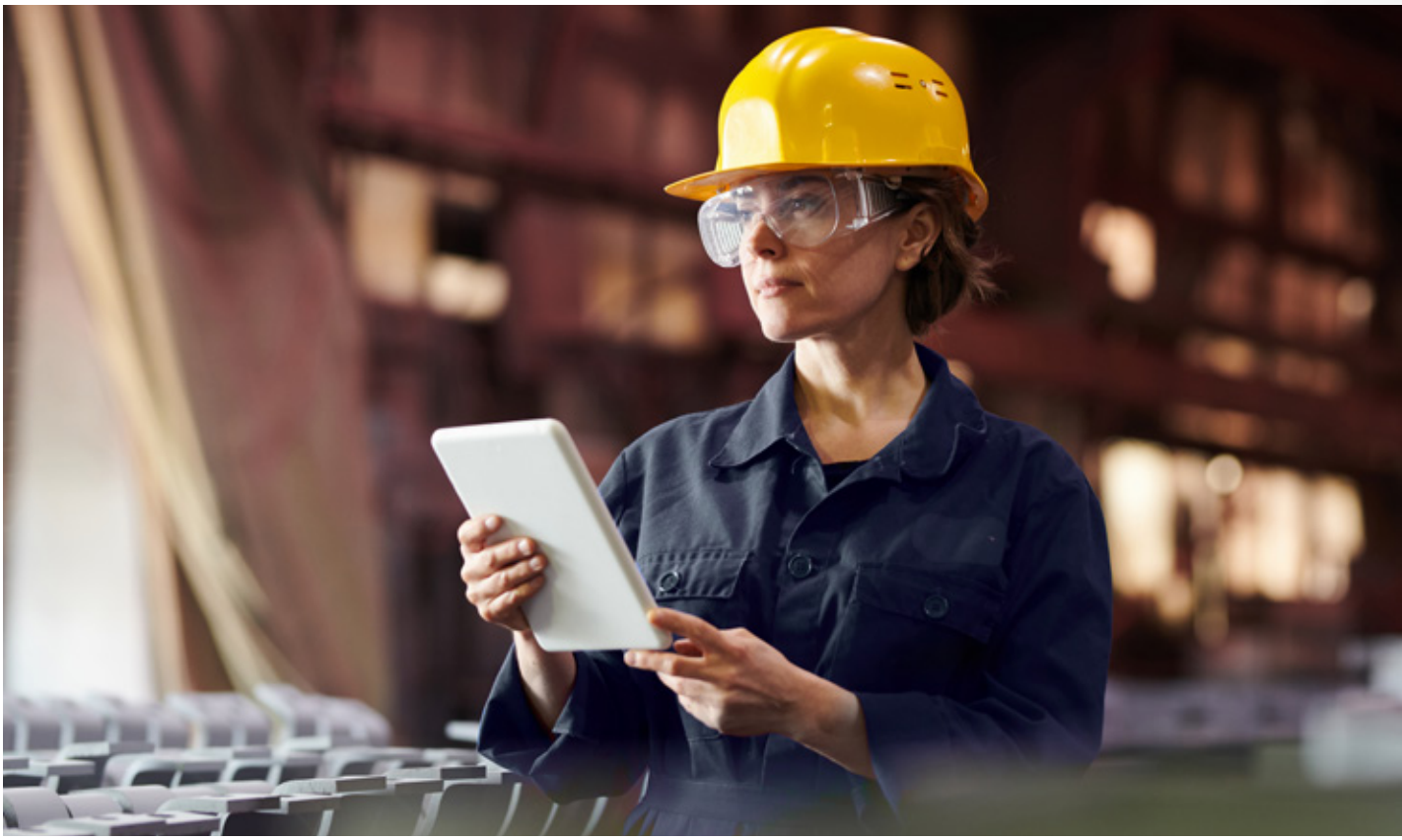
One reason the supply chain is integrated is due in part to its reliance on automation. Automated systems streamline production, reduce labor costs, and improve efficiency, but they also create vulnerabilities. Automated manufacturing processes often rely on interconnected networks of machines, sensors and control systems. A single compromised component can disrupt entire production lines, leading to substantial financial losses and operational downtime.

An example of this automation is programmable logic controllers (PLCs), which automate and control manufacturing. With the advent of web-based PLCs, users can now access and manage these systems remotely. While this enhances operational flexibility, it also introduces significant vulnerabilities.

Remote access opens the door to cyberattacks that can manipulate or disable critical manufacturing processes.

Hackers can exploit weak points in PLC security to gain unauthorized access, potentially disrupting production, damaging equipment, and creating safety hazards.

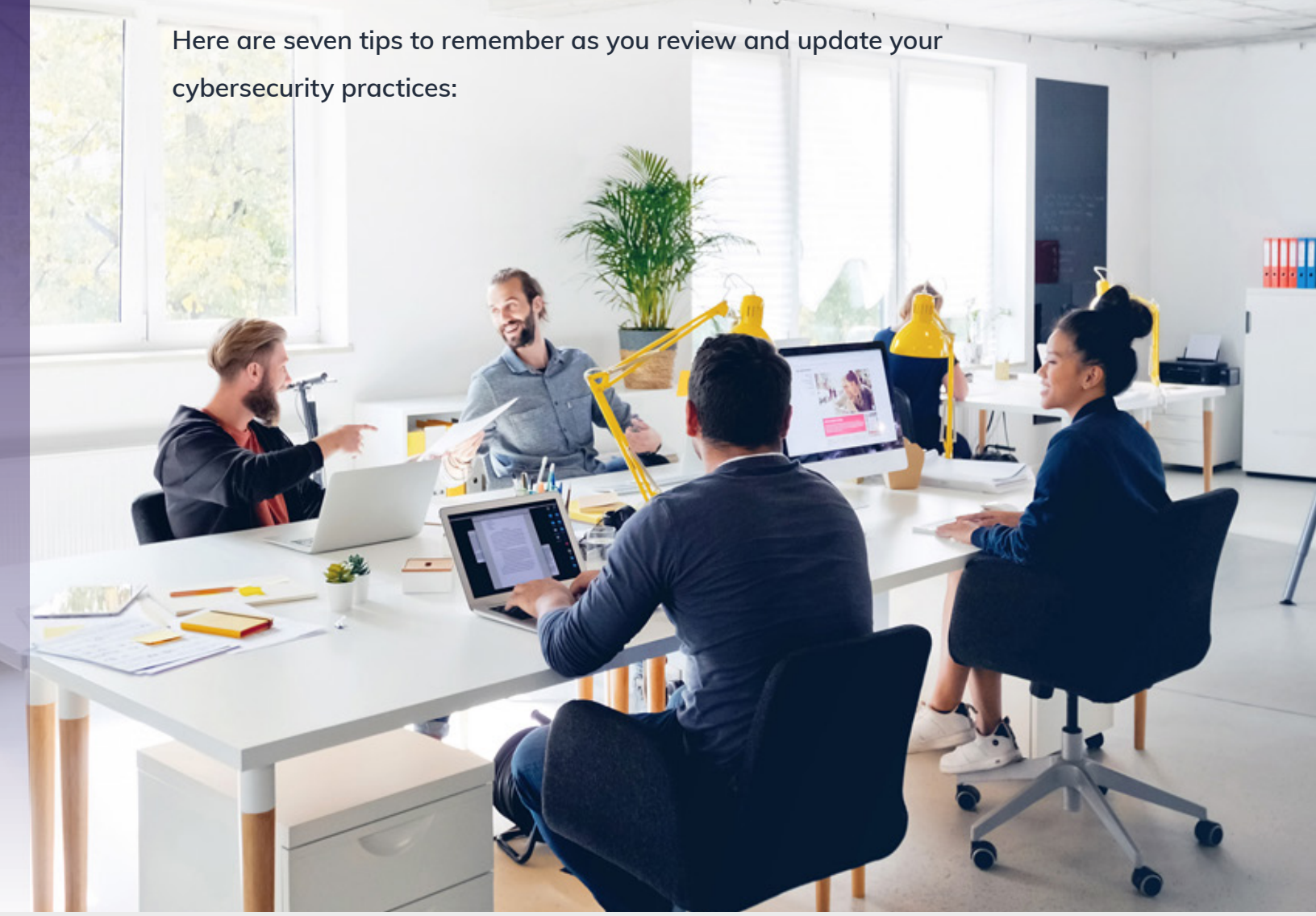
Cybersecurity is a vital part of your operations whether you're dealing with the supply chain, utilities, financial services, healthcare, or one of the other twelve critical infrastructure sectors. So, what are a few things you can do to protect your organization?



7 RECOMMENDATIONS FOR SECURING YOUR CRITICAL INFRASTRUCTURE ORGANIZATION

Maintaining your critical infrastructure organization's cybersecurity is paramount to ensuring the stability and continuity of the essential services it provides. With cyber threats becoming increasingly sophisticated, your organization must adopt comprehensive security measures tailored to its unique needs, each falling under one of these three pillars: people, process, and technology.

Here are seven tips to remember as you review and update your cybersecurity practices:



01. TECHNOLOGY: FOLLOW BASIC CYBERSECURITY PRINCIPLES

Start by adhering to basic cybersecurity principles, such as the principle of least privilege. It is crucial to ensure that only individuals who need access to specific systems or data have that access and regularly review their rights. Periodic access reviews help identify and remove unnecessary permissions, reducing the attack surface. Similarly, segment and segregate your systems to prevent the spread of malicious traffic within networks.

These principles are most effective as part of a comprehensive identity access management (IAM) program. IAM is not simply about implementing tools like two-factor identification. It also includes quantifying risks and creating mitigation and improvement roadmaps that address key functions such as user provisioning, de-provisioning, and access privileges.

02. TECHNOLOGY: USE A SECURITY FRAMEWORK

Adopting a trusted security framework such as the NIST Cybersecurity Framework, CIS18, or ISO 27001 can help you make decisions and implement security measures. These frameworks have proven effective over time and offer structured approaches to achieving cybersecurity maturity, starting with basic cyber hygiene and moving on to more advanced security measures.

By gradually implementing these guidelines, organizations can enhance their security posture over time, ensuring continuous improvement so you don't have to purchase a tool and cross your fingers.

Whichever security framework you choose, you'll also need to assess and document existing tools, identify outdated or unused systems, develop a plan to update or eliminate unnecessary tools, and integrate new technologies seamlessly.

03. PEOPLE: IMPLEMENT REGULAR CYBERSECURITY TRAINING FOR STAFF

Your team members can either be the weakest link or the strongest defense in cybersecurity, depending on their training. Regular training sessions on identifying phishing and social engineering attacks can empower employees to act as the first line of defense for preventing potential breaches. Continuous education and awareness programs guarantee that everyone remains vigilant and informed about the latest threats.

04. PEOPLE: BREAK DOWN SILOS BETWEEN IT AND OT

In terms of people, make sure to break down silos between your IT and operational technology (OT) teams if applicable to your business. Doing so can enhance security by combining expertise and resources, eliminating redundant efforts, and fostering a holistic approach to security. Breaking down silos also enables better communication and idea sharing, leading to a more resilient security posture.

One approach to breaking down silos is integrated governance, risk and compliance (GRC) programming. In some companies, different departments largely enforce different aspects of GRC, leading to an “us vs. them” mentality in the business. Integrated GRC distributes responsibility for GRC policies to every department in the company, combining them in the shared mission of protecting the company’s assets, compliance strategies and brand.

05. PROCESS: VET YOUR VENDORS

Every critical infrastructure sector uses vendors that can lead to vulnerabilities, illustrated by several of the examples mentioned above. Regularly vetting your suppliers, understanding their security measures, and updating your vendor agreements are important aspects of securing your organization.

This process doesn't require complex tools but demands diligence. You can start by reviewing their SOC 2 report and any other data privacy and security policies that they may follow, which can also clarify what your vendor is responsible for protecting.

06. PROCESS: PERFORM REGULAR RISK ASSESSMENTS

Perform regular risk assessments and evaluate how risks are measured in terms of likelihood and impact. Companies that rated CrowdStrike as a medium risk prior to its outage likely prevented companies from having procedures in place in the event of an attack.

Reassessing and potentially updating risk definitions and impacts ensures that high-risk elements are addressed appropriately. Regularly updating these assessments helps you stay ahead of evolving threats. One thing to keep in mind: While the cloud offers many security benefits, even all-cloud organizations must regularly assess their risks.

07. PROCESS: ESTABLISH DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

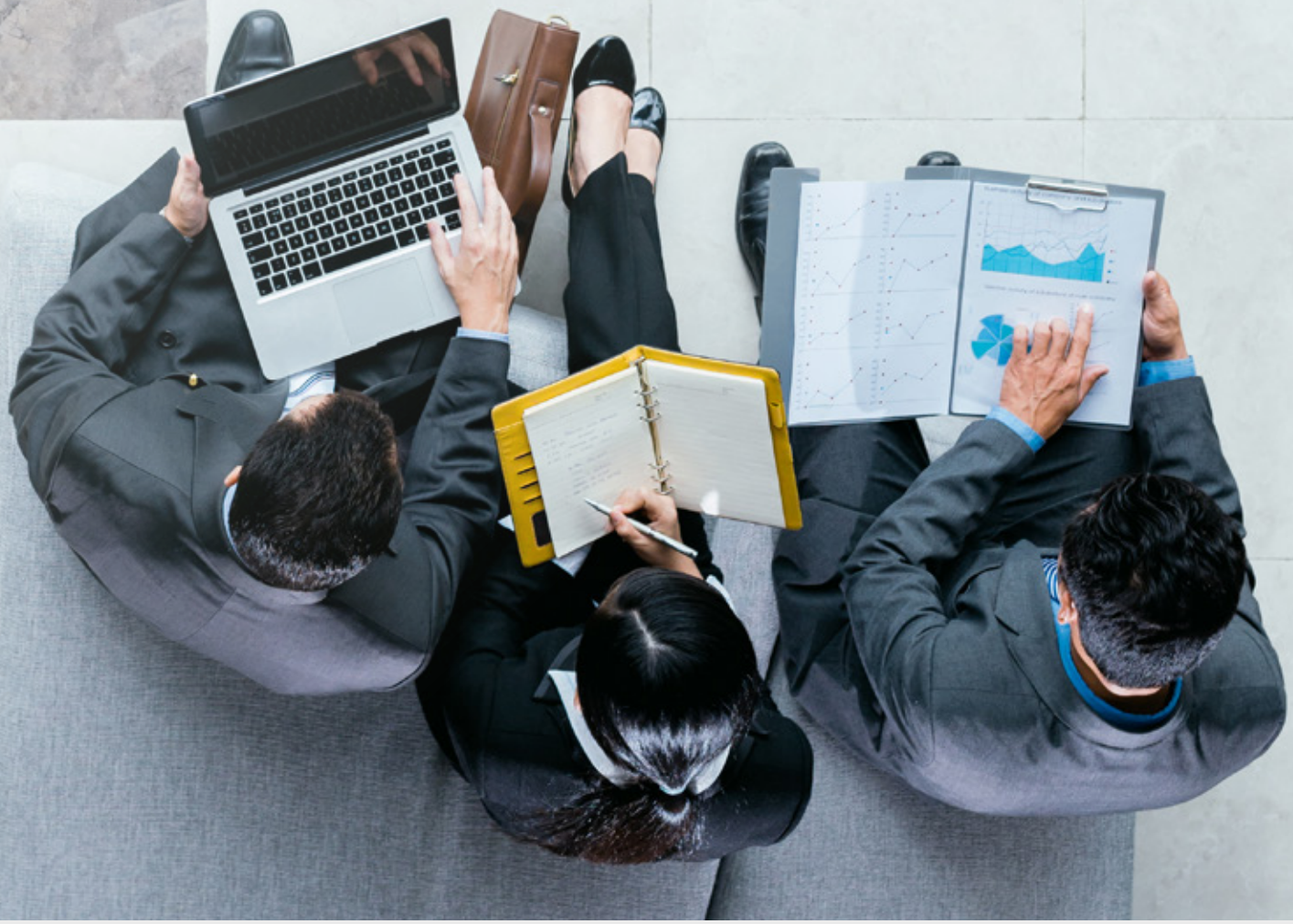
Effective response plans and conducting regular exercises to test them are critical for maintaining operations during cyberattacks. Tabletop exercises and simulations can help you prepare for scenarios where your primary security tools may fail, and developing and practicing fallback strategies prepares your organization to continue operating even during major outages or other adverse conditions. You should regularly update these plans to reflect new threats and changes in the operational environment.

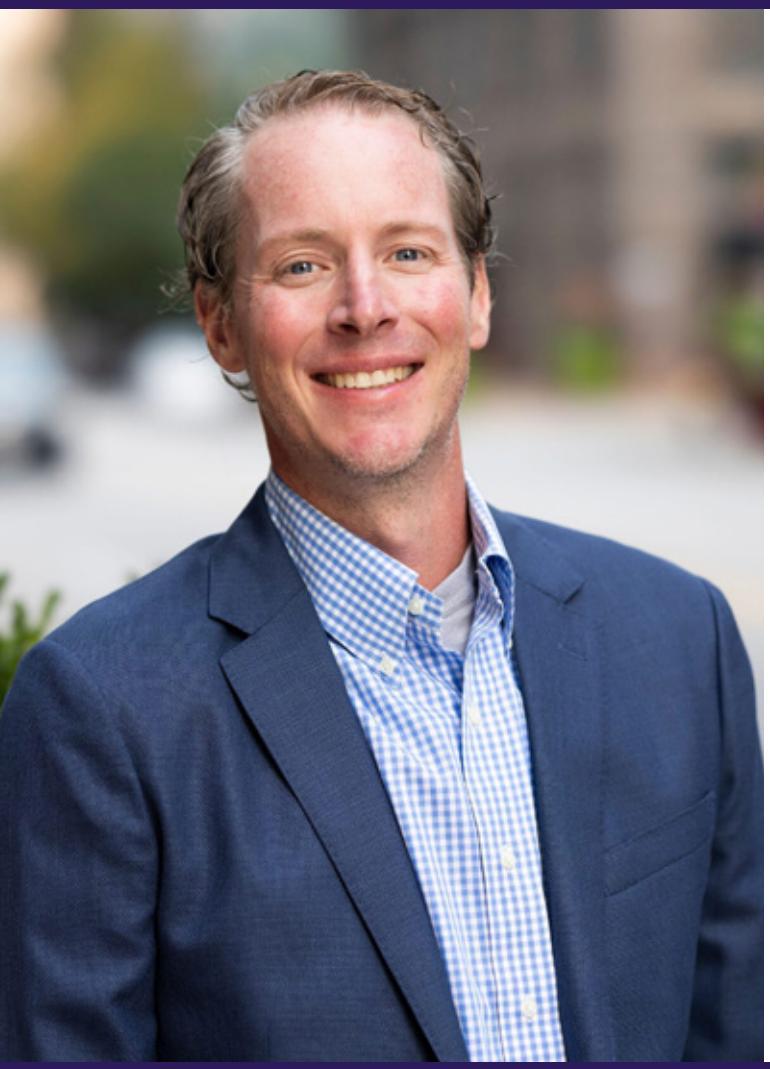
Each of these seven steps is a cost-effective and efficient strategy that will help protect and strengthen vulnerable systems within your critical infrastructure environment. As you work through them, consider what you aim to achieve with your security measures and how you plan to implement them so your organization can prepare for the worst while maintaining operations.

PROTECTING PEOPLE BY PROTECTING CRITICAL INFRASTRUCTURE

Though we often don't realize it, critical infrastructure affects our daily lives. Securing these sectors is part of what keeps many people safe and healthy. However, their security is not a one-time project but an ongoing commitment that requires continuous review and adaptation.

By focusing on people, processes and technology, your critical infrastructure organization can build a resilient security posture that protects people, keeping everybody safe and providing a quality of life worth living.





ABOUT THE AUTHOR

David Lefever
Vice President | Cybersecurity

David has expertise in cyber strategy, enterprise risk management, and framework selection and adoption. David has worked in IT and cyber risk management for 20 years and is located in Carmel, IN.

David loves fly fishing, live music, time with family, and a healthy work environment.

Our experts can help you achieve the needed security posture that addresses today's vast array of security threats.

Contact us.

((CENTRIC))

ABOUT US

For 25 years, Centric Consulting has created unmatched experiences for employees, clients and communities. An international management consulting firm, we bring expertise in AI strategy, cyber risk management, cloud solutions and more. The firm combines the benefits of experience, flexibility and cost efficiency to create tailored solutions centered on what's best for your business. Founded in 1999 with a remote workforce, Centric has grown to 1,500 employees and 14 locations across the country and India.

Visit www.centricconsulting.com to learn more.