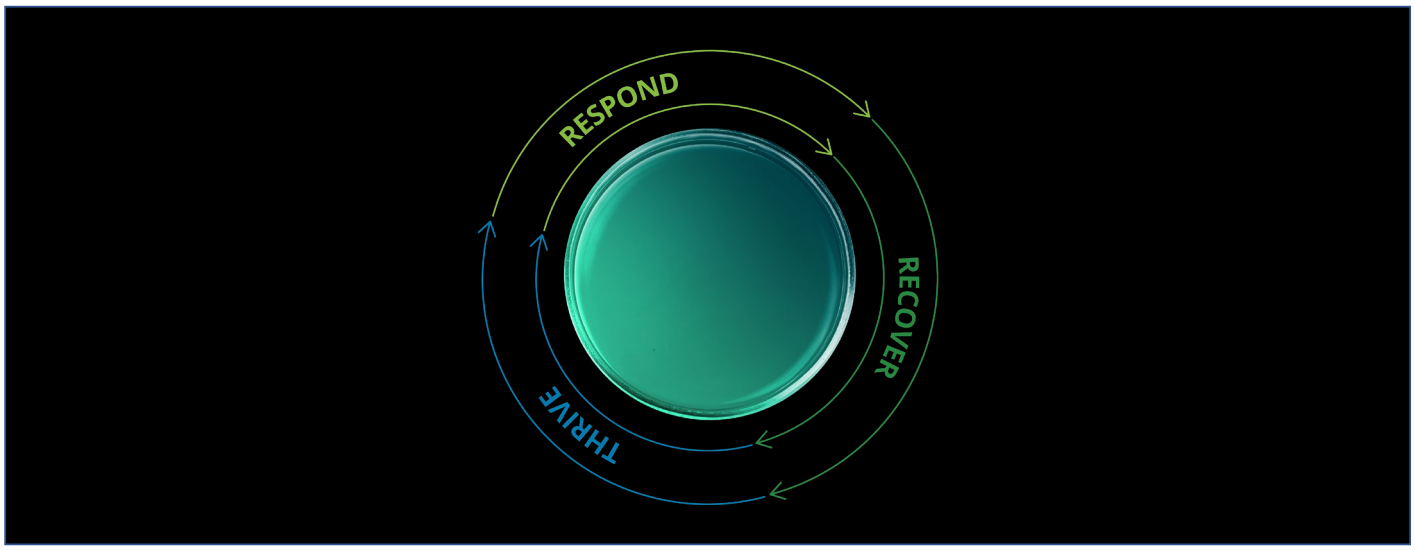
Deloitte.



The Impact of Cyber on "Critical Infrastructure" in the Next Normal

COVID-19 creates a new generation of critical infrastructure requiring new levels of security and oversight

As COVID-19 dramatically reshapes global society into the "next normal," many organizations that never considered themselves part of the critical infrastructure discussion are now classified as such. Perhaps the most vivid example of this is grocery stores. Before COVID-19, the critical infrastructure classification fell on the food production supply chain, but not on the retailers selling that food to consumers. Likewise, hospitals are understandably critical infrastructure, but medical research labs typically have not been – and in the case of COVID-19, research labs will be, arguably, critical for leading the world out of the pandemic. This fact is not lost on cyber threat actors, while most organizations impacted by a cyber-attack may risk losing data or financial information, a successful attack on critical infrastructure could potentially impact health, safety, or the environment. New exploits are targeting vaccine research labs, clinical trial administrators and other members of the healthcare ecosystem that suddenly find themselves to be "newly critical" organizations. As society moves to the next normal, these newly critical enterprises face expanded cybersecurity challenges and regulatory compliance mandates.

Same Old Threats, Brand New Implications

When companies suddenly become critical to national welfare, it changes the implications of cyberattacks. Threat actors are motivated by monetary, political, economic or another impetus to achieve a malicious goal. For example, a small metal fabricator in Minnesota, U.S., provides a small, precision component used in ventilator assemblies. In normal times, this 40-person company would be a small member of the manufacturing supply chain. But with the need for ventilators in hospitals in the US and around the world, the company, and many like it, are not only now part of the critical infrastructure of the U.S. but also are more likely targets for nefarious-minded cyber adversaries.

Before COVID-19, there was no requirement for this company, or others like it, to be able to run operations 24x7. And, should they be hit with a distributed denial of service (DDoS) or other cyberattack, shutting down for a period to remediate the attack would have been a typical response. Today, however, this manufacturer has zero tolerance for downtime, because it would delay the production of desperately needed ventilators. In the next normal, this company has transformed from a tiny supply chain partner, to a newly critical player in the race to ameliorate a public health emergency.

Industrial Control Systems (ICS) are the essential control systems and instrumentation necessary for daily necessities such as air and lights. They include supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLC), industrial automation and control systems (IACS), and remote terminal units (RTU). Threats to ICS are particularly dangerous types of cyber-attacks because of the blurred line between cyber and physical attacks of this nature. ICS remain pervasive across all industries and in countless organizations, demonstrating the large attack surface for threat actors to target.

Attacks against ICS could have rippling effects for a geographic area due to shutdowns and damaged equipment causing a loss of service as well as pose health and safety risks to individuals. For example, an adversary could turn off the heat for areas with extremely cold temperatures or create false readings in food processing plants. ICS face varying risks depending on the organization; however, several remain common among them and should be considered even more as organizations adjust to life during and post COVID-19. These include the increasingly close connection between information technology (IT) and operational technology (OT), remote workforce models, use of third parties to manage and maintain systems, and increase in mobile devices. These issues introduce the possibility for threats to be introduced to the IT network, which can then propagate to the OT network.

In another example, the growing pressure on health care providers from the COVID-19 pandemic may also make them more desirable targets for ransomware attacks or other types of extortion. The time-sensitivity of many health care operations and their lower tolerance for downtime are part of why they have become such attractive targets for many ransomware operators in the first place. The perception that health care providers now have even less tolerance for downtime due to COVID-19 exacerbates this risk factor.

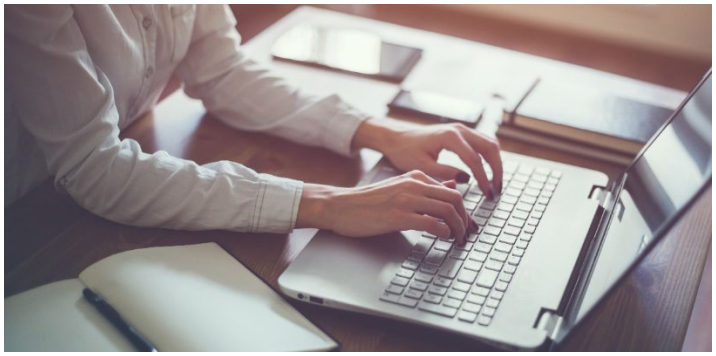
Deloitte Cyber Threat Intelligence predicts that state-sponsored threat actors will seek to collect data pertaining to COVID-19, if they have not already done so. Possible collection requirements would include: IP, particularly biomedical and pharmaceutical research for treatments, cures, and vaccines for COVID-19; infection and other health statistics; and inside information on measures that foreign governments take to contain the pandemic as countries return "back to life" after the initial outbreak.

The Compliance Conundrum

Beyond cyberthreats, critical and essential organizations are subject to regulatory compliance that may require the adoption of new technologies and processes for many of the newly classified organizations. For example, a plastic sheet manufacturer – which historically had only minimal compliance requirements – has been reclassified as "critical" because it now produces the medical-grade protective masks needed for healthcare workers). Now part of the country's critical infrastructure, the manufacturer will be required to meet a variety of cybersecurity and privacy regulations, some of which took effect and were adopted over time, but in this "next normal", organizations are finding themselves with limited time to comply. Such efforts may require extensive rearchitecting of security infrastructure, and various governance and reporting processes.

In the U.K., for instance, grocery stores are handling personally identifiable information (PII) on 1.5 million high-risk citizens, so they can prioritize these citizens for the assembly and delivery of grocery orders. While this provides a critical service to citizens in need, it also places unprecedented privacy requirements on grocery stores that they must manage properly to comply with the European General Data Protection Regulation (GDPR). The expense to retrofit or newly invest in cyber programs to provide the necessary levels of data protection could be quite costly to organizations that might not have considered such measures before.

While many regulatory bodies around the world are relaxing enforcement during the crisis, newly critical organizations need to plan for longer-term regulatory compliance, because stronger enforcement will return once we go back to life the way it was. Data security and data management will both be challenges after the crisis – in some cases, newly critical organizations will need to dispose of data that they no longer need (the grocery stores in the U.K. being a good example of this). In other cases, organizations will need to implement security controls on new processes that emerge from the COVID-19 pandemic, which will include everything from working from home to telehealth.



The first step for all critical infrastructure companies – both new and traditional – is to reassess their cyber risk. Processes will change (the work at home model being an excellent example), and habits developed during the pandemic (such as ordering groceries online) are likely to become permanent for many people. These changes will have a corresponding impact on each organization's risk footprint, requiring an evolution of both security and compliance technologies and processes. It's important to recognize that depending on the goal and planned actions, a threat actor is likely to study, as well, to understand how to modify systems in an impactful way. Or, an adversary could potentially leverage points of access and connection to prepare for a destructive attack augmented by the access and information gained during initial reconnaissance they did months ago. Threat actors are likely to continue targeting critical infrastructure and related sectors to further their own strategic geopolitical and economic goals.

That is why it's important for organizations now recognized as critical or essential, to adopt an established security framework, such as NIST or ISO, as the core of security strategy, rather than tactically trying to address new security and compliance issues on a piecemeal basis. Using a framework will enable a holistic approach to cybersecurity, based on leading practices, that reduce inefficiencies in addressing issues as they arise, leading to a potential reduction in time and money spent.

Cyber considerations for newly categorized critical and essential organizations:

Don't confuse compliance with security

Regulations are not, and never have been, security frameworks. When reassessing cyber risk, it is critical to evaluate enterprise risk through a data security lens that adapts to an evolving threat landscape, not a compliance lens that seeks only to meet regulatory requirements.

Understand third party risk

Third parties (or their fourth party subcontractors) with access to an organization's systems are a potential threat. Organizations must understand the potential risk from these business partners and implement technical and contractual controls to ensure they comply with cybersecurity policies.

Strengthen Incident Response

Newly critical organizations need to review and evolve their cyber incident monitoring, response and reporting capabilities. Doing this effectively will enable them to limit the impact of cyber-attacks, and to remain both secure and compliant.

Best Practices to Protect Against Cyber Threats

- **Layered Defense:** Adopt a layered defense approach, making your organization's security stack robust and protection techniques deployed from the perimeter and inwards. This includes protections for the cloud, protections for devices, firewalls, email security, and other layered security protections.
- **Network Segmentation:** Segment networks, particularly IT and OT to avoid compromise from IT spreading to OT. Deploy network sensors within internal networks to detect lateral movement and other suspicious activity.
- **Endpoint Security:** Deploy an endpoint agent with Endpoint Detection and Response (EDR) capabilities capable of providing visibility into malicious activity. Ensure that behavior-based rules are enforces, such as automatic execution of Macros from emails.
- **Access Controls:** Implement role-based access control, limiting access to least privileges required to perform daily activities. Secure remote access channels with two-factor authentication (2FA) in the form of a push notification. Implement robust and efficient system logging and increase the likelihood of detection.
- **Prevention and Detection:** Implement counter-measures to mitigate attacks at the perimeter of the network such as firewall rules to block unused ports and deny HTTP requests to non-standard ports, intrusion prevention systems to detect and block malicious traffic from entering an environment, content filtering to allow users to only access trusted sites, and restrictions on browsing with local admin privileges on their machines.
- **Privileged Access Management:** Monitor for anomalous behavior such as indications of privilege escalation or lateral movement.
- **Data Backup:** Rely on frequent, segmented, and redundant backups to restore encrypted files in the event of ransomware.

Newly critical organizations are under tremendous stress right now, because they are not accustomed to operating in a world where failure is not an option. By taking steps to implement proven security frameworks and adopting best practices, they can not only reduce the risk of business interruptions during the pandemic; they can also support potentially greater business agility and resilience in the next normal.

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber

Contact us

Andrew Jefferies
Canada
Phone: +15064604666
Email: ajefferies@deloitte.ca

Raj Mehta
US
Phone: +17139822955
Email: rmehta@deloitte.com

Puneet Kukreja
China
Phone: +862133138338
Email: puneetkukreja@deloitte.com.cn

Mark Carter
London
Phone: +442070075018
Email: markcarter@deloitte.co.uk