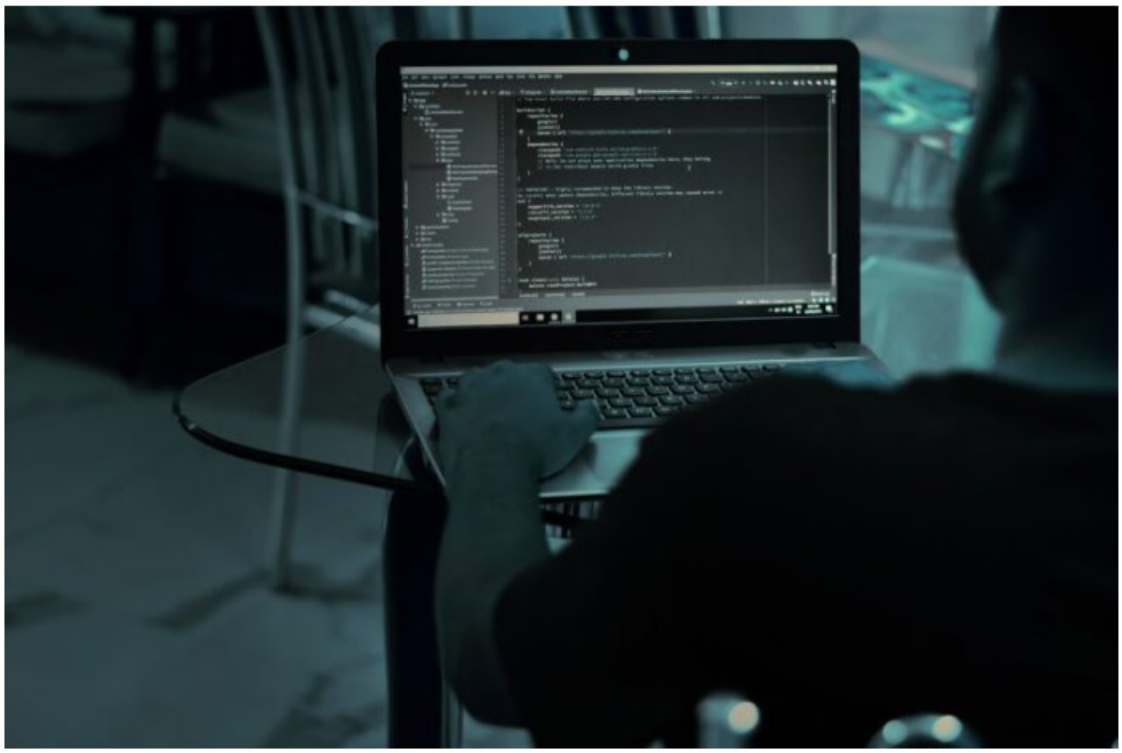
SUBJECT MATTER AREAS CYBERSECURITY INFORMATION TECHNOLOGY

10 Essential Steps to Cyber Resilience as Hackers Target Critical Infrastructure

By Michael Sanchez May 18, 2021



A motivated hacker will break into a system they target. No doubt, no question. Perhaps you have heard that stated less assertively, but the sentiment is the same. Hackers come in all experience levels and sizes, from individual actors to full nation-state forces. Some cybercriminals depend on teams, bots, harvested intelligence, brute force, and relentless targeting. Sometimes, an attacker is fortunate to encounter just dumb luck. Regardless of the skill level or support, a motivated hacker will ultimately succeed in compromising a set of their targets.

Our job as cybersecurity professionals is to prevent these attacks, and, absent that, to at least minimize their frequency and severity of any successful intrusions. The relentless efforts of a determined attacker call for more than a simple "ounce of prevention" and companies with gaps in their security practices have learned hard lessons about why more is required. There are countless security breach examples but the recent Colonial Pipeline example reveals the sophistication and reprehensible nature of cyber criminals in their use of ransomware for profit. While all industries can all benefit from 13-plus years of lessons learned in NERC CIP, the mandatory cybersecurity requirements for power companies that operate critical infrastructure, the oil and gas sector will likely be best aided based on their similar technologies and risks.

While every incident is unique, the data from thousands of breaches has taught us how this usually happens. This information is freely shared amongst the cyber community, so why does this keep happening? Recent high-profile examples all demonstrate that, as cyber teams improve, the bad guys advance their tactics. Unfortunately, in many cases, cybersecurity only improves as a result of advances in criminals' maneuvers.

Brian Harrell, former Assistant Secretary for Infrastructure Protection at DHS, recently said, "Our critical infrastructure sectors are the modern-day battlefield and cyber space is the great equalizer. Hacker groups can essentially attack with little individual attribution and virtually no consequence. With over 85 percent of all infrastructure owned and operated by the private sector, significant investment and attention must be placed on hardening key critical systems. I anticipate more attacks like this happening in the future. A key lesson here is that while technology and automation is good, we must also have the ability to efficiently operate manually as well. Attacks will happen, but how quick can you recover and restore critical services?"

The goal is to "respond" to an incident and not just "react." What happens when intruders are in your environment? Do you have an incident response plan, and a team, and does that team have the necessary tools and intel to respond and recover from the incident? Perhaps your organization uses external incident response specialists who can help, but is this enough? Experience has taught me that it is not. While these teams may be good at what they do, they cannot address the need for business continuity – how the business continues to operate until systems are restored, crisis communications, and information protection if these programs were not already in place.

The business need is to provide reliability of the IT systems essential for continued operation. If your organization was compromised by a cybersecurity event, how would the business continue to operate until systems are restored? What information was taken, and was it in a usable state? What information is helpful to share with your employees, customers, and community? All of these questions support the need for cyber-resilient programs that strengthen incident response,

redundancy, and disaster recovery by including business continuity, information protection, and crisis communications.

How can you make your organization more resilient? Here is a checklist to achieve these goals.

10 Essential Steps You Can Take Today

1. Create a "culture of security" in your company. Your employees, contractors, and vendors can be your greatest asset or weakest links. Support your joint success through continued training and awareness and make sure they understand that your security depends on their security practices. And demand a sound organizational change management plan when changes impact your team.
2. Know your assets. Creating an accurate asset inventory is the first step. Include hardware and software, and keep updated through change and configuration management. Periodic walkdowns are helpful to validate electronic to physical lists.
3. Minimize your attack surface. Remove unnecessary and unsupported systems and applications, and deactivate services and ports that are not needed.
4. Identify your business-critical systems and sensitive data. Place additional security measures over these systems and data, and make them more difficult to access through network segregation and encryption. Unstructured data is a real problem, so for Pete's sake discover and move sensitive data to common repositories.
5. Limit and manage cyber and physical boundaries, log and monitor activity. Both the logical and physical entry points into your environment need to be discovered and protected.
6. Be prepared for real-time events. Are your incident response plans clearly defined, and rehearsed? And are they supported by business continuity, information protection, and crisis communications?
7. Audit accounts and permissions, adopt the principle of least privilege. It is surprising how often accounts or access are never terminated.
8. Manage your vulnerabilities. This can be accomplished through a thorough risk assessment. Similarly, while everyone knows how important it is to patch systems we see companies often getting caught short by inconsistent or poor patching programs.
9. Measure and document your baselines. Knowing what your environment should look like when it is running optimally is the best barometer to indicate when something is amiss.
10. Review your internal controls to make sure you have a good balance of preventive and detective controls. Remember that untested controls will atrophy so develop an audit plan to test the effectiveness of these controls based on criticality, testing issues or current threat. If you are not sure which common controls are most impactful, take a look at cybersecurity hygiene controls. Assessments are available online but be familiar and trust the portal where you share this information.

These recommendations are straightforward but elements in these programs are inter-connected and there is a logical order for development and implementation. Don't try to boil the ocean; instead, take a measured and methodical approach and continue to evaluate your program maturity. And as beneficial, work with an experienced and trusted cybersecurity partner to assist you through this process. With the correct approach and commitment, you can achieve cyber resilience.

Michael Sanchez, CEO (CISA, CCSFP) is involved in the scoping and planning of every project, and then serves in an advisory capacity until all deliverables are completed. He has over 33 years of experience in information technology, cybersecurity, physical security, compliance, and audit. Michael has held senior leadership positions in the energy, oil & gas, healthcare, and transportation industries. He is a former VP and General Manager for ICF International, a large global management consulting firm, where he served as head of Commercial Cybersecurity and Compliance. In other past roles, he managed IT and OT for a $12-billion energy corporation, assisted in the IT rebuild and redesign for a large power generation company, and served for 12 years as a board member for FBI InfraGard Houston, helping to facilitate the sharing of information related to domestic physical and cyber threats.