IS YOUR CRITICAL INFRASTRUCTURE REALLY PROTECTED?

A CIP SECURITY ASSESSMENT WILL TELL YOU; KNOW NOW, BEFORE IT IS TOO LATE.

CAPCO

White Paper

Introduction

With cyberattacks rapidly rising in frequency and impact, the level of protection needed to secure your critical infrastructure continues to increase. In the past couple of years, utilities around the country rushed to implement NERC CIP (Critical Infrastructure Protection) before the mandatory implementation dates. Almost all claim compliance but are relying on internal audits – or none at all – to verify that they meet all the compliance criteria.

The standards around CIP require a comprehensive approach to security in many different areas, not just cybersecurity but at the physical layer, as well. All organizations, not only utilities, face challenges in fully implementing initiatives to meet certain security objectives or regulatory compliance without leaving any holes behind in the security layers. Some of these weak points can relate to process, documentation or maintenance issues left in the wake of the implementations. In order to achieve true security, organizations must go beyond mere compliance to stay ahead of intruders and saboteurs by deploying the latest tools.

Capco Energy Solutions was asked to manage the security program for a major electricity utility and successfully executed, and continues to execute, more than 20 individual projects related to NERC CIP compliance. Below, we outline some of our focus areas and lessons that any organization wanting to protect their infrastructure can use.

Asset, patch and configuration management

Recent cyberattacks show that if companies don't apply the latest software updates, their cyberassets become extremely vulnerable. Companies must have a thorough patch management process and system, along with upgrading all operating systems and software to the latest versions. Unsupported systems should not be in the critical infrastructure. There are software products that can continuously update company systems and report how secure they really are.

Transient devices

When needing to work on critical systems that require laptop computers or other devices to manage them, dedicated devices that are isolated from the internet need to be built. These devices are checked out and used only when directly needed and checked back in to a secure location. We found it is extremely difficult to build such devices with all the necessary security layers while remaining functional and with all the necessary software . In order to achieve this, companies should develop and use a strong testing methodology.

Network anomalous behavior monitoring

Numerous network security tools exist on the market that look for known vulnerabilities in the network or potential intrusions from outside, but they do not check for internally based attacks or yet unknown vulnerabilities. To do this, use available tools that develop a baseline model of normal behavior on your network and alert you to anything out of the ordinary, so it can be investigated. This adds another layer of security that may make the difference in preventing a major security breach. Capco performed a tools evaluation and helped our client choose the only product that met all of their requirements and negotiated a better price, as well.

Log consolidation

Your infrastructure has a lot to tell you, probably telling you so much and in so many ways that you can't possibly digest it all. However, this data contains critical clues that you need to find. The first step is to collect this data and manage it: That's where log collection tools can do powerful work. They pull logs from a vast array of servers, middlewares and applications. You can customize them to pull log data in from custom developed applications, too.

Security event alerting

Once you have collected your log data, there are tools that enable you to develop alerting rules which look for specific events. Best practices and some regulations mandate that companies collect an audit trail of security events, such as credentials issuance, logins, access denials and password changes. QRadar can filter out events and treat them with the proper priority and create the mandated audit trail.

Video monitoring

Video monitoring hardware and software are improving rapidly and provide capabilities such as classifying types of events and even facial recognition. Video is a security data stream that you should also keep as part of an audit trail. Software can classify events and send clips as alerts to the security personnel who need to see them. The video archives can be compressed and stored easily; data storage prices have come down considerably.

Secured enclosures

Physical security has gained even greater importance lately, with a greater number of more sophisticated access and control devices on the market. Various types of equipment require physical enclosures, and these need documented access control policies. Access needs to be electronically controlled, monitored and logged. Badges can be used to access these enclosures, just as they are used to access buildings. There are highly capable software solutions that can manage access and revoke access quickly when necessary.

Identity and access management

Managing user IDs and passwords across hundreds of systems is a monumental challenge that poses ever-increasing odds of compromises, requiring an identity and access management system to manage all these credentials. The system must be customized to implement specific policies for various systems or physical locations. When personnel leave or credentials become compromised, these systems and their customizations enable the instant revocation of access everywhere it has been granted to that person

Multifactor authentication

Standard practice is now to use multifactor authentication to access the most critical systems. This may be as simple as additional prompts to users or as complex as biometric authentication. Many of the top security agencies use biometric-plus-PIN access for many years, and this has just begun catching on in the commercial world. However, malicious actors are keeping up: Several publicized breaches have involved multifactor authentication, including Apple iCloud – and even almost President Trump's Twitter account – because the prompts became predictable. For the highest security access, consider the latest biometric multifactor authentication, such as iris scanning.

Backups, restoration, and disaster recovery

Of course, regular backups and the ability to restore and restore to an alternate location are standard critical capabilities. Most IT senior management will say their systems are covered in this area, but when a failure occurs, we see many situations where recovery was not possible because of deficiencies (one recent example, British Airways). It is important to determine if the backups are being done correctly and thoroughly and to undergo restoration and disaster recovery and continuity testing regularly. Testing these systems is the only way to gain confidence that your backup systems and plan work, and in our experience, systems almost always fail on the first test. Doing a deeper dive into your recovery capabilities is essential to gain peace of mind and maintain gainful employment.

Network security zones

Today's best practices in network design involve many more layers and isolation zones than the past, and many networks are not effectively protected against today's hackers. Intruders can penetrate individual firewalls, and once an intruder does, what defenses does your network infrastructure have? Multiple VPNs and port-level insulation need to be carefully architected to prevent intrusions and limit damage when intrusions do occur. Implementing these layers while preserving access between systems and users is a challenge that requires experience that is usually not available in-house.

Policies and procedures

Although every organization has them, policies and procedures are often outdated, hard to find and often not followed. Policies and procedures need to be threaded within the standard operating procedures, with established checks that verify adherence to policies. Automated systems that implement and audit these procedures are essential for easy and comprehensive compliance.

In conclusion

Hopefully by reviewing these focus areas for critical infrastructure protection, you have identified areas for improvement for your employer. After all, improvement is imperative: Hackers capabilities evolve rapidly with innovations every day. If they outpace your infrastructure's security improvements, then a breach can result. Hopefully your company will do more than detect a successful attack, using the latest tools and practices to prevent it from happening in the first place.

Capco, Energy Solutions has helped clients evaluate their security defenses with a specific utilities perspective, including SCADA systems. Learn more about how your infrastructure compares with others in the industry, especially those doing it well. We can show you how to be one of the best protected and not one of the low- hanging fruit for easy picking by the black hats.

MORE INFORMATION

Lee Van Doren:
lee.vandoren@capco.com

ABOUT CAPCO

Capco, an FIS™ company, is a global management consultancy with a focus in energy and financial services. Our Energy, Utilities, and Commodities Practice has been focused on Energy clients for over 19 years. We combine innovative thinking with unrivalled industry knowledge to deliver business consulting, digital, technology and transformational services. Our collaborative and efficient approach helps clients reduce costs, manage risk and regulatory change while increasing revenues.

WORLDWIDE OFFICES

Bangalore - Bratislava - Brussels - Chicago - Dallas - Dusseldorf - Edinburgh - Frankfurt - Geneva - Hong Kong - Houston - Kuala Lumpur - London - New York - Orlando - Paris - Singapore - São Paulo - Stockholm - Toronto - Vienna - Washington, DC - Zurich

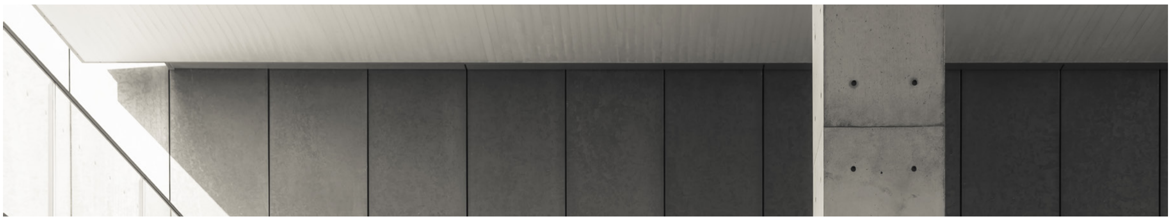
To learn more from our Energy practice, contact us in North America on +1 713-350-1000.

To learn more, visit our web site at www.capco.com or follow us on Twitter @Capco

CAPCO WORLDWIDE:

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
STOCKHOLM
SÃO PAULO
TORONTO
VIENNA
WASHINGTON D.C.
ZURICH

SHAPING THE EVOLUTION OF ENERGY AND FORMING THE FUTURE OF FINANCE



CAPCO.COM