21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2018 Grid of the Future Symposium

A Survey of Cybersecurity Frameworks

T. LAUGHNER, S. MORRIS
Alchemy Global Networks
USA

SUMMARY

The need for situational awareness in unmanned substations has increased. As a result, many types of sensors are being deployed within the substation LAN. However, as utilities begin to rely on cyber connected assets, they should simultaneously consider cybersecurity. When developing a cybersecurity program, there are several frameworks available which represent best practices. This paper describes the various frameworks and makes high level comparisons between them.

KEYWORDS

NIST, FISMA, CIS, Cybersecurity, Framework,

smorris@alchemy-global.net

Introduction

In order to become more efficient, many utilities have replaced personnel with electronic means to remotely control substations. Historically, these devices were based on serial protocols and concentrated into a SCADA system at the central office. Because of the low speed of these serial connections, few data points were returned: bus voltage, feeder current, and switch position.

In the last few years, utilities have switched to network-based protocols. In combination with high-speed fiber-optic connections, these protocols enable many data points to be returned to the SCADA system at the central office. Simultaneously, vendors and research organizations alike have envionsed a variety of sensors to help system operators have situational awareness not only of the operating status of the device, but also the health of the asset.

These new sensors enable more complete situational awareness about the condition of the substation assets. This, in turn, enables system operators to make better decisions about whether to put an asset in service or to take one out of service for maintenance. However, the quality of the decisions is predicated upon the veracity of the sensor data.

Along with all the good, comes the potential for bad. Whether a malicious actor deliberately trying to gain access or control of a system from the outside, or an employee who is disgruntled trying to "get back" at the system in general, or more common unintentional infections from bringing in computer systems or test systems that had attached to other networks and bring an infection with them. No matter how isolated, or air-gapped a network may look on paper, where is the weakest link?

Importance of Cybersecurity

Dictionary.com defines cyber security as "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." Utility networks are often targets of these types of attacks. Clearly, more reliance on network-based sensors, provides a larger footprint on which to attack the utility.

Fortunately, there are several frameworks that promote good cybersecurity practices. It is important to note that good cybersecurity practices will not remove the threats. However, good practices reduce the threat surface which malevolent individuals can use to compromise the integrity of critical data.

Everyone has heard of some of the larger attacks throughout the world. The Ukraine Power Grid attack in 2016 (and subsequent attacks through 2017 and 2018), the release of the WannaCry ransomware attacks that targeted hospitals and Critical Infrastructure entities. Hacking tools such as Crash Override (aka Industroyer) or malware such as Triton that have both theoretically demonstrated and empirically demonstrated the vulnerabilities of systems and the capabilities of attackers.

Ask yourself, can you truly say that you understand all of the attack vectors to your network? Have you protected adequately against them? Would you actually even know if an attack occurred?

Cybersecurity Regulations

There are indeed some regulations that will affect the Critical Infrastructure sector and their use of technology. In 2014, President Obama issued Executive Order 13636 [1] which mandates improvements in the CyberSecurity architectures of the Critical Infrastructure programs.

The Department of Homeland Security released guidelines in 2018 that while merely guidelines right now, are being viewed as the precursor to more stringent rules regarding CIP.

Cybersecurity Frameworks

The cybersecurity frameworks all provide guidance on managing risk to threats from cyber attacks. They collectively represent standards, guidelines, and best practices when developing elements of a cybersecurity program. A variety of different frameworks exist, but they all have many themes and elements in common.

The most popular cybersecurity frameworks are PCI DSS, ISO 27001/27002, CIS Critical Security Controls, and NIST Framework [2]. The primary decision in which framework to implement is generally determined by industry type or regulation. PCI DSS is one of the most widely deployed frameworks in the industry. Unsurprisingly, this is the security standards council for the payment card industry. The risk of PCI data exposure is high and therefore attention to cybersecurity practices is of paramount concern. Meanwhile, NERC Critical Infrastructure Protection (CIP) is a regulatory requirement for transmission utilities in North America. However, utilities seem slow to adopt cybersecurity practices as best practices for business reasons.

The cost of compliance is an important piece in overall business. However, the cost of non-compliance, or worse, the cost of an actual breach are much more significant. Simple steps can be taken to reduce the threat vectors that are present in any integrated network.

The NIST Framework provides a comparison of a variety of the cybersecurity frameworks [3]. The major functions of the NIST Framework include Identify, Protect, Detect, Respond, and Recover. Each of these functions have subcategories. These subcategories will be explored in the following sections.

The first and most critical step in developing a cybersecurity program is to Identify the current state or baseline. The NIST Framework breaks down Identification into several categories: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy. From a business perspective, you cannot change what you do not measure, nor can you mitigate that which you do not see. Therefore, taking note of the current conditions provides guidance what current assets need to be protected and what the potential risks are. Table 1 [5], below, shows an excerpt of the table Asset Management category from the NIST Framework for Identification. It is important to note that many of the categories have elements in several different frameworks.

Table 1 – Excerpt of the NIST Identity/Asset Management Framework [5]

Category	Subcategory	Informative References
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

As Table 1 shows, there are numerous references for each category and sub category. Many of these are cybersecurity frameworks or cybersecurity regulations themselves. Each category in the NIST framework is sub-divided into subcategories. These subcategories identify very specific elements of a

cybersecurity program. For example, within Asset Management, physical devices, software, and personal are specifically named. These individual components are all of the actors within the system that could be the source of a malicious attack.

Once the assets, risks, and threats are identified, it is important to protect the assets. The NIST Framework breaks down Protection into several categories: Training, Data Security, Procedures, Maintenance, Protective Technology. Notably, much of protection deals with human factors. An often-used term in cybersecurity is insider threat. An insider threat is threat that comes from people who have inside information concerning the organizations security practices [4].

Once a baseline is obtained and the system is protected, change detection becomes an important element of cybersecurity. To that end, the NIST Framework suggests that Detection systems be put in place. Detection involves Anomalies and Event detection, Security Continuous Monitoring, and Detection Process development. The adage "a good offense starts with a good defence" is apropos here. Unplanned and unexpected changes may be the result of suspicious or malevolent activity.

Even with the best cybersecurity measures in place, it is possible for an unplanned event to occur. Therefore, NIST recommends that Response protocols and procedures be put in place. These procedures include Planning, Communications, Analysis, Mitigation, and Improvements.

Finally, when an unplanned event occurs the NIST framework suggests, putting recovery programs in place. These include Recovery Planning, Improvements, and Communications.

NIST and NERC CIP

While organized differently from the NIST Framework, the NERC CIP regulation follows the NIST framework very closely. For example, in CIP there are requirements around defining assets, training (CIP-4), configuration and change management (CIP-10), incident response (CIP-8), and recovery (CIP-9).

Conclusions

New sensors have created a need for better communications. However, more ubiquitous communication pathways have created the potential for cyber-attacks. Utilizing good cyber security program not only reduces threat exposure but is best practice for utility systems that rely heavily on remote sensors. Fortunately, there are a variety of cybersecurity frameworks that can be used to design a cybersecurity program.

While utility companies know their product and their engineering capabilities very well, as they move into an increasingly networked and automated set of systems and devices in order to improve efficiencies and capabilities, they are finding that the capabilities of yesterday are not sufficient for the protocols and networks of tomorrow. Putting a framework in place and investing properly in a CyberSecurity program is a critical necessity within the critical infrastructure.

BIBLIOGRAPHY

[1] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks/

[3] https://www.nist.gov/cyberframework

[4] https://en.wikipedia.org/wiki/Insider_threat

[5] https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx