Paul Polsinelli

IFT 302 – 43489 Sum20

**Bridging OT and IT Security**

Operational and information security is a complex methodology that must be considered, designed, and implemented with discipline. Its facets are outlined in the NIST Preliminary Cybersecurity Framework which breaks down the practice into the categories of Identify, Protect, Detect, Respond, and Recover. We will take a brief look at these aspects and some of what is entailed with a substation case study.

1. Substation layout 

2. The facility is an electrical substation that provides electrical switching for the surrounding community. It is not manned full time but may be operated by a skeleton crew of at least two engineers during ‘operational hours’ and perhaps a dozen during maintenance operations. It contains four 345kv Shunt Reactors and two345/115kv Transformers outdoors. There is a relatively small control building which will contain monitoring equipment such as computers and proprietary software. The monetary value is in the tens of millions of dollars range with transformers of that size costing appx $5mil apiece (1). The informational assets it contains could be invaluable for hostile intelligence and sovereign actors. There are four designated physical access points to the facility including two gates in a chain-link fence and two doors, one opening to the outdoor space within the facility and one on the exterior wall to the facility. The exterior wall is 40’ high and the chain-link fence 14’ high with a perimeter roughly 1000’ combined of roughly equal length.

3. Risk Assessment

A. Identify:

Physical devices and systems within the organization are as follows in order of criticality are as follows: (2)\*

1. Proprietary Software
2. 2ea 345/115kv Transformers - Anchored
3. 4ea 345kv Shunt Reactors - Anchored
4. Live Tank Circuit Breaker – Standard
5. Dead Tank Circuit Breaker – Standard
6. Disconnect Switch – Rigid Bus
7. Lightning Arrestor
8. CCVT – Cantilevered
9. Wave Trap – Cantilevered
10. Bus Structure – Rigid
11. Computer and Network Equipment

The transformers are the heart of the purpose of the substation. All other assets, with the partial exception of the software, supports the function of the transformers to step down current to forward downstream to smaller substations and local power distribution sites. All dependencies are downstream in the distribution process. However, aside from functionality, security and safety dependencies are system-wide as a power surge at a substation could cause surges both up and down and across the distribution system and cause system-wide failure.

The security of the controlling and monitoring software is particularly critical to preventing such a scenario as attacks on the substation can be carried out invisibly through it. Such attacks could include not just purposefully aggressive causal methods such as the type used in the STUXNET attack but passive methods that may simply cause the system to not be alerted or act when a naturally occurring disruption in the system occurs.

The software is vulnerable by its connective nature and so must be monitored continuously for infiltration and be protected by the most up to date firewall and antivirus technology available. Intelligence on hostile activity both in motion and in planning for both cyber and traditionally physical must be accounted for in security activity. Half of the perimeter of the facility is chain-link fence, allowing visibility and easier infiltration capability to any actor with a pair of bolt cutters.

B. Protect

The outer perimeter should have complete coverage by overlapping IR capable IP cameras. The cameras can be monitored 24/7 from either within the control building or remotely. Cameras should be tilt, pan, and varifocal capable to better investigate any actual or suspected intrusions. Cameras should be mounted either on the perimeter fencing and walls or on purpose designed poles.

The facility should be manned around the clock by an armed security guard team of two with at least one guard always within the control room at all times for monitoring and emergency response. They should be equipped with military grade assault rifles in the event of a terrorist attack or coordinated attack on our infrastructure with both satellite and landline communications for redundancy.

All entry to the inner perimeter should be multi-step with multiple authentication methods. A cipher lock will be inadequate alone. A biometric keylock and security card combination is preferable along with visual confirmation by security guards. Since the chain link fence is the weak link (no pun intended) in the physical barrier, it should be electrified.

To support compliance with policy a comprehensive training program should be implemented consisting of:

* **Classroom training**
* **Online training**
* **Visual aids**

(3)

Covered subjects may include:

* Phishing
* Physical security
* Desktop security
* Wireless networks
* Password security

(3)

Additional training for Privileged users will consist of:

“

* What makes a privileged user?
* How the actions and inactions of privileged users can constitute insider threats.
* What should and should not be done with privileged user credentials
* Specific privileged User responsibilities for Information Assurance (IA) and Public Key Infrastructure (PKI)

” (4)

C. Detect

Detection of unwanted access can come in many forms. Physical detection can come in the form of cameras, IR detectors, open/close switches, and accelerometers among others. Cyber intrusions can be more difficult to detect and so constant monitoring by an IT professional, email monitoring, unusual password activity, having firewalls in place, passwords that expire quarterly, and a good up to date antivirus and software in general. If your network crashes. is running slow, doing abnormal things, or is missing data, it is a good sign you may have been infiltrated.

The best way to detect physical breaches is with a security team. Security officers can patrol the premises inside and out to look for signs of infiltration and monitor cameras while also authenticating who enters and leaves the premises and their activities while there. Monitoring equipment and software will also detect any abnormal activity of the equipment which could indicate a breach.

D. Respond

Physical breaches would be responded to by armed deterrence if detected in progress and law enforcement notified immediately. If an intruder is caught in the act they should be detained until law enforcement arrives. Breaches detected after the fact would be subject to investigation internally and by law enforcement. Both physical and cyber breaches would be assessed for damages and/or stolen property or information through forensics. Findings internally would be shared with law enforcement and all stakeholders both during and after with a full report.

All data contained in the server room will be encrypted in preparation of the event that it is physically breached, and hard drives are stolen. A beacon program, that can contact the owners and send local router information when it is reconnected outside the network as part of its boot process, should be developed and implemented. National government authorities should be alerted immediately and provided a detailed description of what was stolen and a backup copy.

E. Recover

If the beacon program has been developed and implemented, the ip address should be traced to its physical location. The stolen device should also be equipped to delete it’s data by either an external or internal trigger such as a command issued over the internet when it comes online or automatically when it doesn’t receive a pre-decided timed security confirmation.

Recovery plans must be documented beforehand and executed in situ. Any sort of physical attack on our infrastructure is going to cause a major public outcry. The method of breach must be immediately identified, further damage mitigated if not eliminated, and area secured. After this is done, the public must be made immediately aware of these measures. Services must be restored as the highest priority while assuring citizens that the wheels of justice have begun turning, other infrastructure is secure, and the situation will not be repeated. Following these steps and letting people know what measures, changes, and lessons learned have made the organization better will help restore the reputation of and confidence in the organization.

A cyber breach will not cause as much panic if it is just theft of software, though this could enable a far worse attack in the future. The network will have to be taken off the internet at least temporarily until the method of breach can be determined and a patch or operational procedure can be developed and implemented. Cyber forensics in cooperation with law enforcement should begin immediately to try to find the perpetrators and prevent them from attacking again. Informing the public of the steps taken should help mitigate any loss of reputation and confidence that might occur.

4. Conclusion

A thoroughly thought out and well implemented security using the NIST Preliminary Cybersecurity Framework created in 2013 by Executive Order 13636, “Improving Critical Infrastructure Cybersecurity” (5), is necessary to maintain American infrastructure security. Plans are multi-stepped and require cooperation with outside agencies, vigilance, discipline, and awareness, continuously. A well-conceived and implemented plan will not guarantee that a breach will not occur, but it will eliminate the possibility to the degree that it can be and mitigate damages incurred by one.

References

1. Aleen Mohammed, Power Transformer: Learn the Purpose, Cost, and Lead Time to Procure, <https://peguru.com/2019/08/power-transformer/> , Sept 15, 2019
2. Steelman, Joshua & Song, Junho & Hajjar, Jerome. Integrated Data Flow and Risk Aggregation for Consequence-Based Risk Management of Seismic Regional Loss, <https://www.researchgate.net/figure/113-4-Default-Mapping-for-VHV-Substation-Components_tbl1_32965427>, 2020 \*not all information obtained from reference
3. Rapid Awareness Training, Rapid7, <https://www.rapid7.com/fundamentals/security-awareness-training/>
4. Security Awareness for Privileged Users, MediaPro, <https://www.mediapro.com/mediapro-trainingpack-courses/security-awareness-privileged-users/>
5. Brooks, Grow, Craig, & Short, 2018, *Cybersecurity Essentials*, John Wiley and Sons Inc.