How to Target Critical Infrastructure: The Adversary Return on Investment from an Industrial Control System

GIAC (GCCC) Gold Certification

Author: Matthew Hosburgh, matt.hosburgh@gmail.com
Advisor: Adam Kliarsky

Accepted: June 11th 2016

Abstract

Imagine a device that could decrypt all encryption—within seconds. A box with this capability could be one of the most valuable pieces of equipment for an organization, but even more valuable to an adversary. What if that box only worked against American encryption? If true, a particular market would be ripe for the harvest. A device that powerful could be used to decrypt secrets and data in transit, making encrypted data an adversary might have access to, extremely valuable. Similarly, Critical Infrastructure is a target for some because of the yield that a successful attack could result in. Death, disruption or damage is a real possibility. The Return on Investment (ROI) and Return on Security Investment (ROSI) fall short in actually determining the level of protection required for an organization striving to protect the most sensitive data or system. The Adversary Return on Investment (AROI) is the missing piece to the equation. From the adversary's vantage point, data, infrastructure or systems have value. By understanding this value an organization can more appropriately align its security strategy; especially, for the most critical infrastructure.

1. Introduction

> “He said our codes were based on an entirely different system than the Russian codes, so this box really wouldn't work on them. The only thing it would be good for is spying on Americans. Sure, with a box like that they could read the FBI's mail. - Or the CIA's. - Or the White House's. No wonder they don't want to share with the other children” (Robinson, Lasker, Parkes, 1992).

Imagine a device that could decrypt all encryption—within seconds. A box with this capability could be one of the most valuable pieces of equipment for an organization, but even more valuable to an adversary. What if that box only worked against American encryption? If true, a particular market would be ripe for the harvest. A device that powerful could be used to decrypt secrets and data in transit, making encrypted data an adversary might have access to, extremely valuable. Similarly, Industrial Control Systems (ICS) are a target for some because of the rich yield that a successful attack could result in. Death, disruption or damage is a real possibility.

Every organization that operates an ICS has an adversary. It should not be a surprise that ICS, and especially Critical Infrastructure (CI), is a target of opportunity. In 2015, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 295 of reported intrusions, all targeting a form of CI ("NCCIC/ICS-CERT Year in Review", 2016). Out of those reported, it was discovered that 22 of those intrusions reached a depth of level 6, or the critical system level (“NCCIC/ICS-CERT Year in Review”, 2016). The Return on Investment (ROI) and Return on Security Investment (ROSI) fall short in actually determining the level of protection required for an organization striving to protect the most sensitive data or system. If an organization considers a threat from a defensive perspective, the organization will fail to fully understand the true value of what they are striving to protect. The Adversary Return on Investment (AROI) is the missing piece to the equation. From the adversary’s vantage point, data, infrastructure or systems have value. By understanding the value of the AROI, an organization can more appropriately align its security strategy for the most critical infrastructure.

2. Current Threats Against ICS

Before an organization can fully understand the adversaries it faces, it is important to recognize the current threats faced by Industrial Control Systems (ICS). Although Stuxnet is one of the most recognizable attacks on ICS', the start of reported or documented attacks go back much further. In 1982, alleged attacks by the CIA on a pipeline's ICS led to its eventual explosion (Carr, 2012). Although the perpetrator of the attack is still debated, it is worth noting that kinetic results could be a possibility as early as 1982. Over the past 35 years, it is also worth noting the increase in targeted cyber-attacks on ICS. Figure 1 illustrates a timeline of some of the major reported attacks on ICS' (physical and cyber) and figure 2 outlines the specific incident, industry, adversary and initial attack vector.

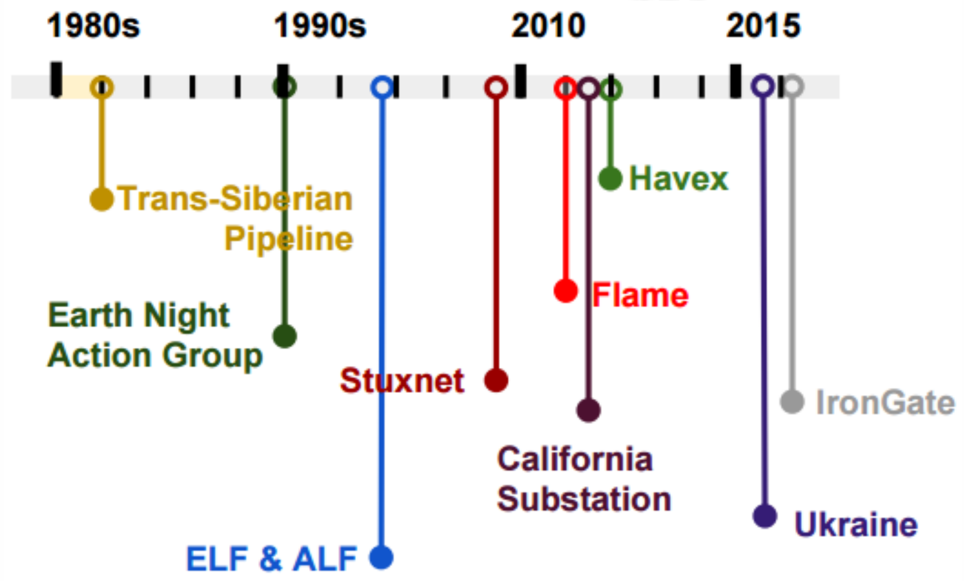
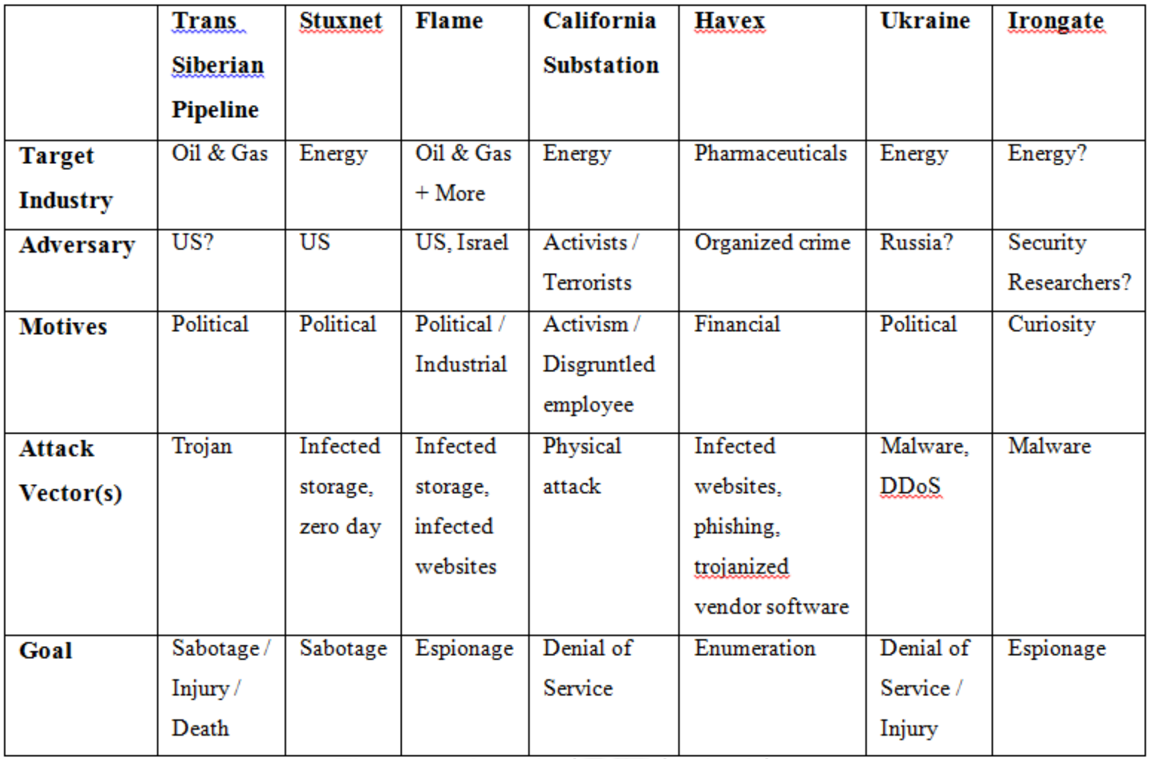


Figure 1. Overall timeline of various CI incidents.



	Trans Siberian Pipeline	Stuxnet	Flame	California Substation	Havex	Ukraine	Irongate
Target Industry	Oil & Gas	Energy	Oil & Gas + More	Energy	Pharmaceuticals	Energy	Energy?
Adversary	US?	US	US, Israel	Activists / Terrorists	Organized crime	Russia?	Security Researchers?
Motives	Political	Political	Political / Industrial	Activism / Disgruntled employee	Financial	Political	Curiosity
Attack Vector(s)	Trojan	Infected storage, zero day	Infected storage, infected websites	Physical attack	Infected websites, phishing, trojanized vendor software	Malware, DDoS	Malware
Goal	Sabotage / Injury / Death	Sabotage	Espionage	Denial of Service	Enumeration	Denial of Service / Injury	Espionage

Figure 2. Attack details by incident.

The bottom line is that targeting ICS is not new, but with more connected and exposed systems the attack surface is greater than it has ever been. Adversaries are well aware of this reality.

3. The Adversary Return on Investment (AROI)

The AROI is the missing link when determining what an adversary will target. For example, as a prudent homeowner, one might purchase a lock for a front door. When selecting this lock, one might determine what the budget is based on the level of protection that is being advertised by the model of lock. The more money spent, would gain more features or added protection. After the lock is installed the owner realized that their new car was stolen from the garage. It was wrongly assumed that a thief might be interested in the new TV inside the house; however, the attacker realized that there was a side door that provided direct access to the new car. The owner, in this case, failed to understand what the adversary was interested in from a targeting perspective. The items inside the house were of little value to the thief compared to the new car in the garage. Similarly, the AROI is used to help determine what and how an attacker might value an organization’s data, infrastructure or systems and how they might consider obtaining that objective.

3.1. The AROI Formula

The AROI is the missing link in determining the amount of protection an organization requires from a security perspective. To better understand the attacker’s view on the target, it is fundamental to understand what the attacker is targeting. In some cases, data, bandwidth, and process control all have a value. That value is better illustrated in figure 3, via the AROI.

$$\boldsymbol{Adversary\ ROI} =$$

$$\left(\frac{Attack\ Value\ (Value\ of\ Assets\ Compromised + Adversary\ Value\ of\ Operational\ Impact) - Cost\ of\ the\ Attack}{Cost\ of\ the\ Attack}\right)$$

$$x\ Probability\ of\ Success$$

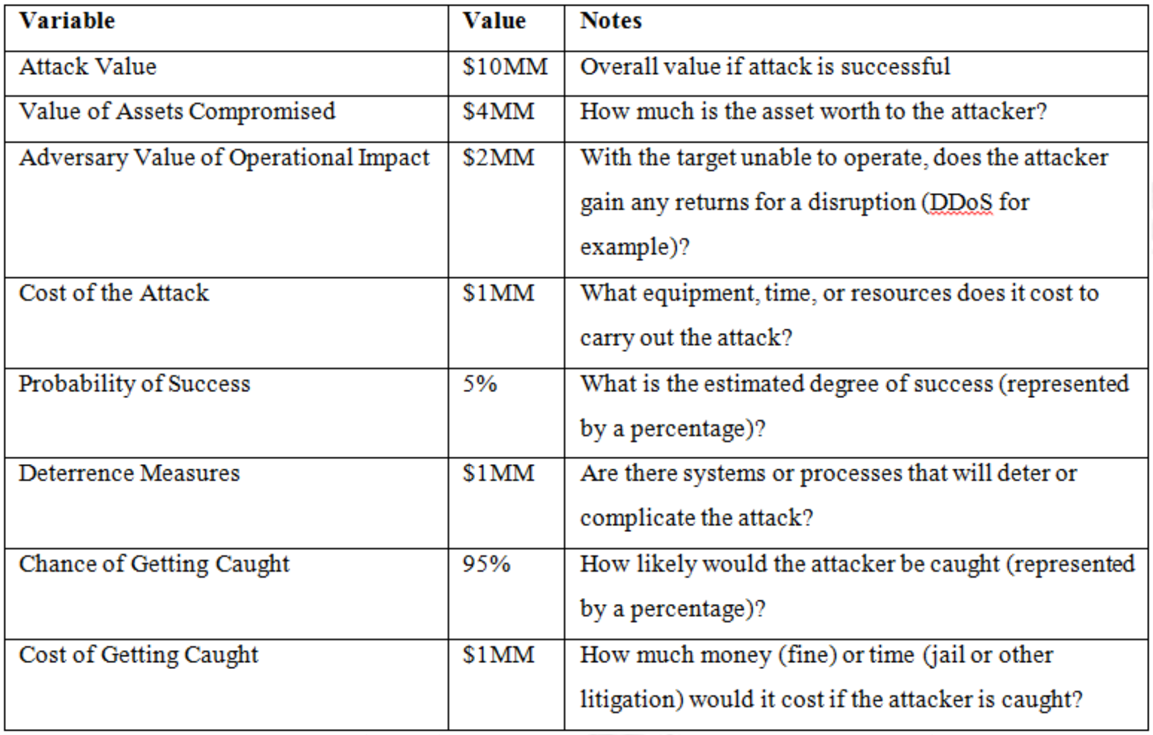
$$-\ Deterrence\ Measures\ (\%\ Chance\ of\ Getting\ Caught\ x\ Cost\ of\ Getting\ Caught)$$

Figure 3. The AROI formula (Corman, Etue, 2012).

It should be underscored that an adversary, more than likely, does not calculate this formula; however, it is more of a mental or unofficial check. The question that this formula answers from an attacker’s perspective is: “Will I (we) come out on top if I (we) achieve my (our) objective?” If yes (or if the number is positive), it is likely that an attacker would target the organization. The AROI can utilize any units of measure, which allow it to be implemented in existing risk assessments or business processes.

3.2. The AROI on an ICS

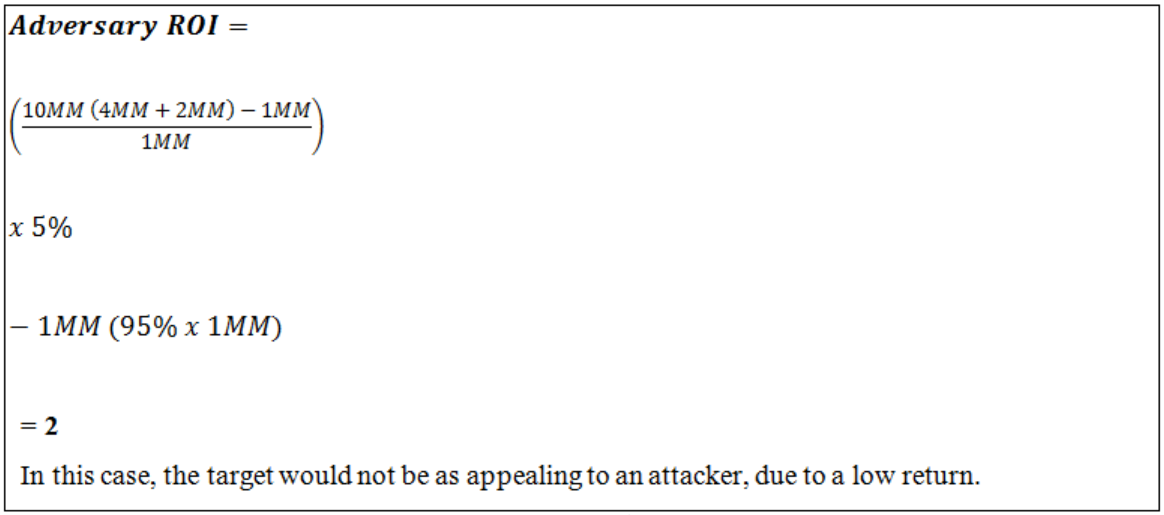
When the AROI is applied to an ICS, the target value to an attacker becomes more apparent. The following example will utilize the AROI to calculate the return, from an adversary’s perspective, on an ICS. The values for the variables in figure 3 will be assumed, but can be replaced with values that represent an actual ICS. Because the multitude of variables, this should be calculated on the ICS relevant to the organization’s environment. As an example, figure 4 has listed values for an organization that has been prudent in protecting their ICS.



Variable	Value	Notes
Attack Value	$10MM	Overall value if attack is successful
Value of Assets Compromised	$4MM	How much is the asset worth to the attacker?
Adversary Value of Operational Impact	$2MM	With the target unable to operate, does the attacker gain any returns for a disruption (DDoS for example)?
Cost of the Attack	$1MM	What equipment, time, or resources does it cost to carry out the attack?
Probability of Success	5%	What is the estimated degree of success (represented by a percentage)?
Deterrence Measures	$1MM	Are there systems or processes that will deter or complicate the attack?
Chance of Getting Caught	95%	How likely would the attacker be caught (represented by a percentage)?
Cost of Getting Caught	$1MM	How much money (fine) or time (jail or other litigation) would it cost if the attacker is caught?

Figure 4. The values for a fictitious organization with a level of protection.

These values, after being calculated in figure 5, can show that this organization's ICS is not necessarily an easy or cheap target.



$\boldsymbol{Adversary\ ROI} =$

$$\left(\frac{10MM\ (4MM + 2MM) - 1MM}{1MM}\right)$$

$x\ 5\%$

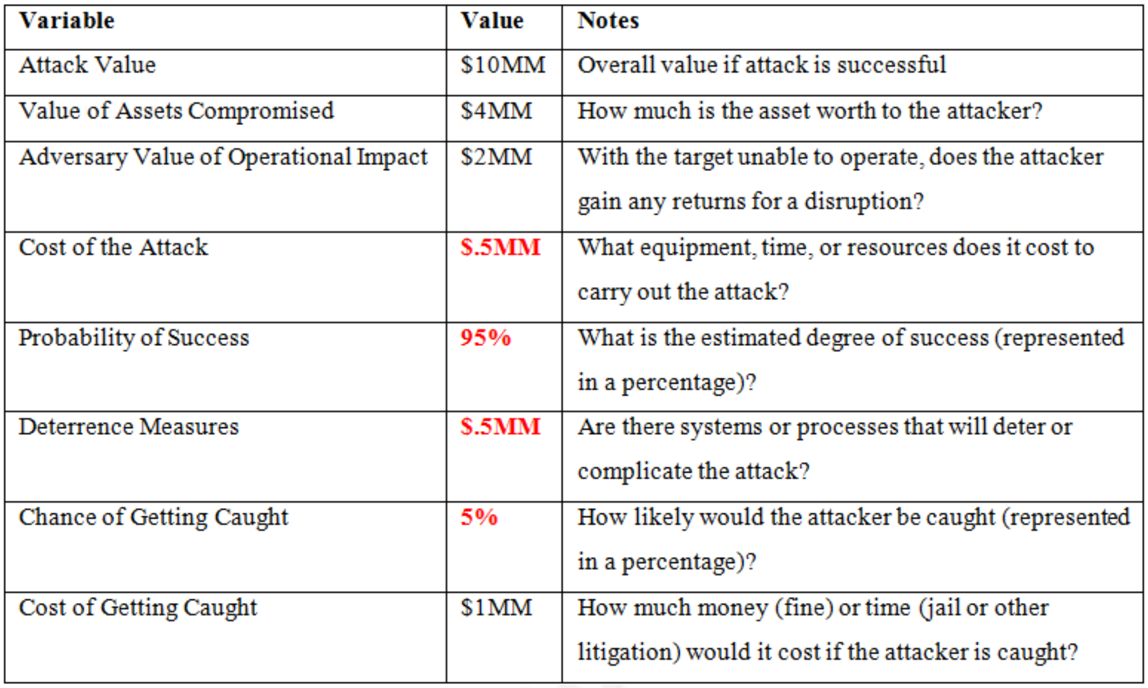
$-\ 1MM\ (95\%\ x\ 1MM)$

$= \mathbf{2}$

In this case, the target would not be as appealing to an attacker, due to a low return.

Figure 5. Results of calculating the AROI against the values in figure 5.

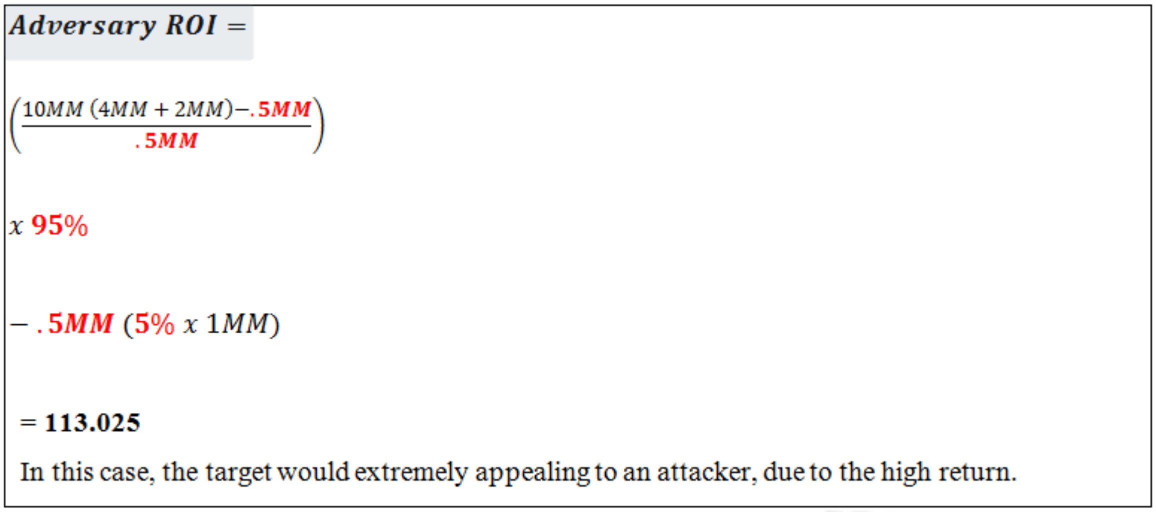
Now, if the organization was not as prudent in their protections, or if the ICS was accessible from the Internet, the appeal and cost to an attacker would be a great deal less. In figure 6, the new values of a less protected system can be found.



Variable	Value	Notes
Attack Value	$10MM	Overall value if attack is successful
Value of Assets Compromised	$4MM	How much is the asset worth to the attacker?
Adversary Value of Operational Impact	$2MM	With the target unable to operate, does the attacker gain any returns for a disruption?
Cost of the Attack	**$.5MM**	What equipment, time, or resources does it cost to carry out the attack?
Probability of Success	**95%**	What is the estimated degree of success (represented in a percentage)?
Deterrence Measures	**$.5MM**	Are there systems or processes that will deter or complicate the attack?
Chance of Getting Caught	**5%**	How likely would the attacker be caught (represented in a percentage)?
Cost of Getting Caught	$1MM	How much money (fine) or time (jail or other litigation) would it cost if the attacker is caught?

Figure 6. The values for a fictitious organization with a level of protection.

The calculation in figure 7 illustrates the same target with inadequate protection or detection capabilities.



$$Adversary\ ROI =$$

$$\left(\frac{10MM\ (4MM + 2MM) - .5MM}{.5MM}\right)$$

$$x\ 95\%$$

$$- .5MM\ (5\%\ x\ 1MM)$$

$$= 113.025$$

In this case, the target would extremely appealing to an attacker, due to the high return.

Figure 7. Calculation based off an organization that does not protect their systems.

The result in figure 8 illustrates a very large target with minimal protection (and possibly a direct Internet connection). The high positive number illustrates that the target would be so much more appealing to an attacker because of the lack of deterrence, probability of a successful attack, low chance of getting caught and a mild punishment. In this case, the ICS is probably being attacked, or the attack is imminent. The AROI undoubtedly shows how appealing a target can be to an attacker.

3.3. Why is the Organization Still Getting Targeted?

For an organization operating an ICS, and specifically for Critical Infrastructure (CI), a negative AROI does not mean an attack is mitigated. A negative return may be still considered by certain adversaries. Arguably, CI operated by a large organization is often regulated. For example, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requires various degrees of protection or detection for security events and incidents (“Cyber Security”, 2012). These requirements are often met with best-in-breed security technology, making for a difficult target from an adversarial perspective. If the adversary has a great deal of resources to expend, the hard target is still a target, nonetheless. The Havex malware was a prime example of an adversary who was able to target and attack several organizations and ICS’ over a long period of time. The ultimate objective is presumed to be financial gain; however, the adversary behind the attack utilized numerous avenues of attack, spread over several years (Langill, 2014). Clearly, this adversary is not a casual attacker; rather, an individual or group with a great deal of resources to spend on achieving the goal, or the AROI is high. If the ICS system is connected, it is exposed and if it runs any type of code, it is vulnerable (Corman, 2013). The only true answer to why the organization is still targeted lies with the adversary and what their objectives are.

4. Threat Modeling to Understand the Adversary

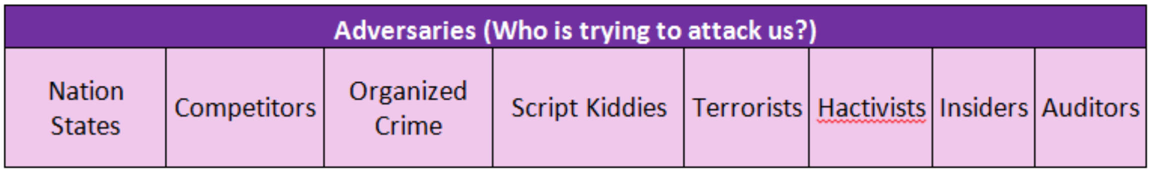
Defending against all and every threat is impractical, and is why the organization must understand who their adversary is, or could be. In Joint Publication 3-12(R), Cyberspace Operations (CO) are predicated by the assumption that all "missions are informed by timely intelligence and threat indicators from traditional and advanced sensors, vulnerability information from DOD [Department of Defense] and non-DOD sources, and accurate assessments" (2013). The scope of CO encompasses both defensive and offensive operations. The offensive aspect of CO is beyond the immediate scope of the AROI, but can be considered when the defensive aspect has been satisfied. Further, this section is not a replacement for a more comprehensive threat modeling exercise. The foundations will be laid and the overall strategy can be set for the organization with these initial elements and will help protect the right areas from the adversaries who are actually targeting the establishment. The key characteristic of CO from the DOD's perspective is that before any of the operations can commence (both defensive and offensive), an accurate view of the adversary, or in the case of CO, intelligence and threat indicators from an adversary, are required.

4.1. Enumerating the Adversaries

Determining who the adversaries are for a particular organization is the first step in formulating the AROI. At the base of the AROI formula is the adversary. Without this knowledge, it is difficult to fully understand the prevention or detection capabilities required to make the target less appealing. "Brainstorming is the most traditional way to enumerate threats. You get a set of experienced experts in a room, give them a way to take notes (whiteboards or cocktail napkins are traditional) and let them go" (Shostack, 2014). Taking it a step beyond just the threats, look into the root of the matter, that is, the adversary. The process of enumerating the adversaries an organization is up against can start in the following fashion:

- Brainstorming exercises from a selection of experts within the organization
- Open source intelligence and research that is freely accessible
- Paid threat intelligence services (ISAC or other)
- Active defense techniques (honey pots, nets or other methods to identify attacker techniques and possibly help identify additional adversaries)

The bigger the cross section, the larger the adversarial base could be; however, it can also help to validate a group or individual's claim. With multiple groups or individuals in the organization identifying a particular adversary, the risk from that adversary might float to the top of the preverbal list. Figure 8 illustrates what the results could look like after a group session.



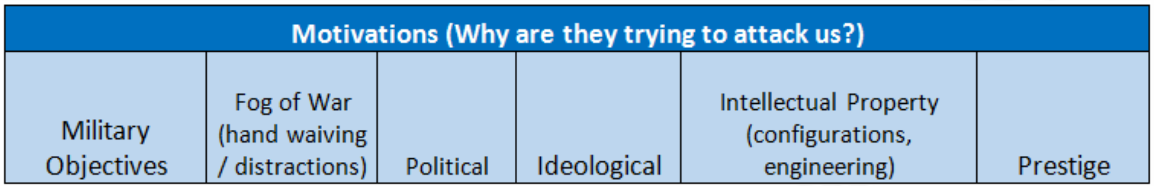
Adversaries (Who is trying to attack us?)							
Nation States	Competitors	Organized Crime	Script Kiddies	Terrorists	Hactivists	Insiders	Auditors

Figure 8. Adversaries identified by an organization's experts (Corman, Etue, 2012).

Building a security program around these adversaries not only provides better concentrated protection around the assets and people that take part in defense, it helps to actually understand the motive of the adversary.

4.2. Understanding the Adversary's Motivation

The next step in the process is to understand what produces the desire to attack an organization. What drives and attacker is different and can span a myriad of reasons. These reasons can be narrowed down when the adversary has been identified. Arguably, the motive of the adversary is one of the most volatile aspects of threat modeling and identifying who is attacking. For that reason, it is imperative that the motivation and adversary are reviewed on an ongoing basis. For example, if a nation state is identified as an adversary and the motivation is military or political, the motivation could be a result of the environment. “Understanding attack motives provides clarity to possible targets, attack vectors, and, consequently, related countermeasures to defend against attacks” (Vélez, Morana, 2015). A trade embargo, war, or other political tensions could mold the motive; however, if these tensions subside, the motive could also. Figure 9 illustrates what a brainstorming session can produce, when focused on CI and the adversaries who are targeting those assets.



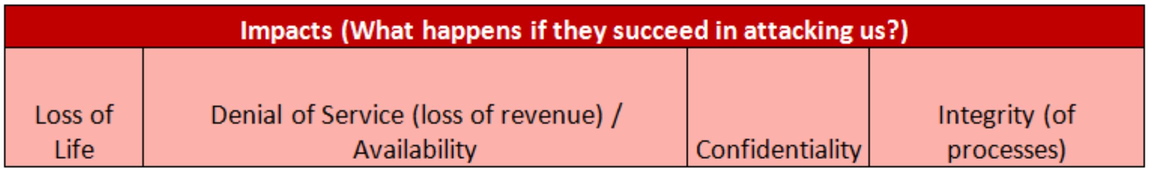
Motivations (Why are they trying to attack us?)					
Military Objectives	Fog of War (hand waiving / distractions)	Political	Ideological	Intellectual Property (configurations, engineering)	Prestige

Figure 9. Motivations of the adversary against an ICS.

For that reason, the iterative process of evaluating the environment must be a discipline conducted regularly. No longer can the geopolitical, market status (business side of things), competitors, or other industrial factors be absent when planning for security. CI ranks high on the risk register because of the implications if an attack is successful.

4.3. Impacts to the Organization from a Successful Attack

The next progression in understanding the adversary’s return on investment is enumerating what would happen if the attack is successful. At this point, the organization should be on the path to understand what would happen if an attack were to be successful. A successful attack on an ICS from an advanced adversary could have far reaching and devastating consequences. Figure 10 is an example of what could happen should an attack, in the most extreme cases, occur. The impacts are for a presumed piece of Critical Infrastructure.



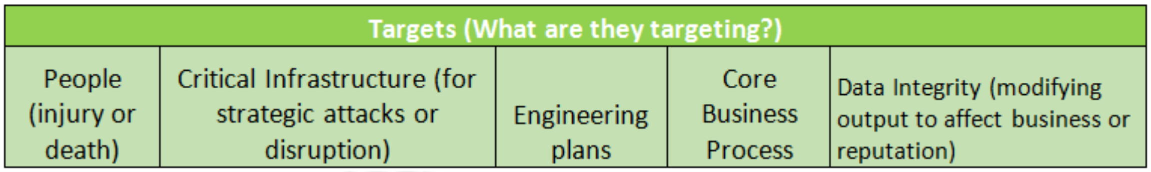
Impacts (What happens if they succeed in attacking us?)			
Loss of Life	Denial of Service (loss of revenue) / Availability	Confidentiality	Integrity (of processes)

Figure 10. The impact on an ICS if the attack succeeds.

Each of the potential impacts could be prioritized based on the exposure of the system or if there are already any mitigating controls in place, such as a Safety Instrumented System (SIS) that could automatically shut a plant or refinery down should a certain threshold be reached. Additionally, the results of a successful attack might require multiple layers of defense or technology to protect against the adversary. In order to have a holistic view of what the adversary is after, the ultimate target or objective will need to be identified.

4.4. Defining What Requires Protection

The final step required in understanding what the adversary is after is to identify what actually requires protection. Understanding what the adversary is truly after will help to structure a more intelligent defense. By now, it is clear who the adversary is, what the motive is, and the damage of a successful attack. The final step is aligning the outlined motives with the actual data or target. Figure 11 illustrates the treasure, or what the organization should be trying to protect.



Targets (What are they targeting?)				
People (injury or death)	Critical Infrastructure (for strategic attacks or disruption)	Engineering plans	Core Business Process	Data Integrity (modifying output to affect business or reputation)

Figure 11. The target an adversary attacking CI is after.

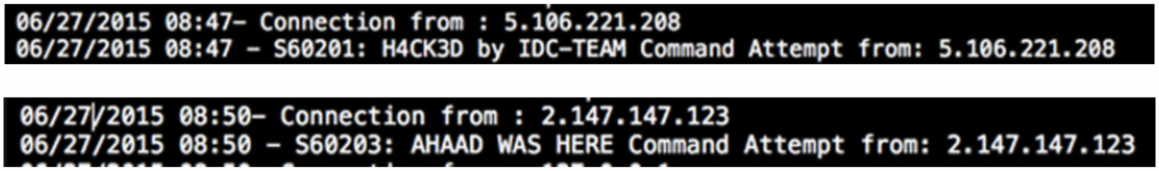
All adversaries are not created equally. The preliminary model is a great start for initial planning and strategy. The next step would be to prioritize the adversaries based on a risk to the organization. Further, the business or organization can help to understand why a certain adversary would be more devastating than another. These threat or AROI packages can be devised to help communicate a real adversary to other areas of the organization and be a subsequent reason for the added scrutiny or security that may be a result. Often, security becomes an impulse reaction, due to fear, uncertainty and doubt (FUD). A headline indicating a critical flaw that can be exploited can have cascading consequences if a process for evaluating vulnerability risk and threats to an organization is absent. Put another way, "As sophisticated malware artists exploit the power of this knee-jerk reaction, more advanced attacks can encompass diversion tactics in order to spread out the presence and effective use of any mitigating processes and controls” (Vélez, Morana, 2015). For that reason, meaningful methods for identifying who the adversary is, are required.

4.5. Techniques to Identify the Adversary

As the adversaries are identified from a high level, the organization can begin to employ technical means to further identify attackers. An age old technique that can prove to be very effective is the use of honeypots. In many cases, this is an obvious choice; however, when dealing with ICS or CI, the intelligence that can be collected from a honeypot can be utilized to validate the high level brainstorming sessions and to identify those adversaries who are actively attacking or trying to fingerprint the ICS who may have not been identified earlier. The caveat to these types of intelligence gathering missions is that most of them will require that the honeypot be deployed in a fashion in which they can be accessed via a public or semi-public connection. Although there is a time and place to deploy canaries or honeypots within an organization, the initial step in collecting information on the adversary should come from an external source. If the resources exist, an entire network, separate from the real network, could be setup with varying degrees of trust zones and honeypot systems. If an adversary were to compromise one system, how do they look to move laterally through the environment? In a recent honeypot deployment by TrendMicro, researchers were able to replicate an ICS and collect some very interesting information.

4.5.1. Gaspot Discoveries

In 2015, TrendMicro researches deployed a series of Gaspot systems to collect information about attacks against ICS. The goal of the research was to collect attack and adversary information on a non-CI gas tank system (Wilhoit, Hilt, 2015). Although, the scope of this paper is looking to ICS and not specific CI systems, the data found with the Gaspot deployment were both relevant and fascinating. From the results, the data presented helped to identify several different attackers. Figure 12 shows a few of the attackers identified and the commands they ran against the system.



```
06/27/2015 08:47- Connection from : 5.106.221.208
06/27/2015 08:47 - S60201: H4CK3D by IDC-TEAM Command Attempt from: 5.106.221.208
```

```
06/27/2015 08:50- Connection from : 2.147.147.123
06/27/2015 08:50 - S60203: AHAAD WAS HERE Command Attempt from: 2.147.147.123
```

Figure 12. Adversaries identified in the Gaspot project (Wilhoit, Hilt, 2015).

The calling cards left by the attackers can tell an organization a great deal about who is attacking. The IDC-Team, according to TrendMicro research, is "also known as the Iranian Dark Coders Team, [and] is a group of security enthusiasts operating in Iran. It is a pro-Iran group responsible for website defacements, information sharing, malware distribution, and hacktivisim" (Wilhoit, Hilt, 2015). That information can be used to further understand the adversary. An open source honeypot exists that can be used by an organization to achieve a similar result as the Gaspot.

4.5.2. The Conpot

The Conpot is an open source honeypot that can mimic an ICS for intelligence gathering about active adversaries. Similar to the Gaspot, the Conpot can be deployed in a distributed deployment to collect broad information about attackers. Alternatively, it can be used to mimic systems that the organization might actually employ to see who might be actively collecting information and launching attacks. According to the Conpot authors, Conpot provides "the basics to build your own system, capable to emulate complex infrastructures to convince an adversary that he just found a huge industrial complex… a custom human machine interface [is possible] to increase the honeypots attack surface" (Rist, Vestergaard, Haslinger, Pasquale, Smith, n.d.). By customizing a Conpot deployment to more accurately represent a real environment, the more real the adversary becomes. Basic setup instructions can be found in Appendix B. Correlating and researching the adversary can take the understanding of an adversary from a best guess, to a fully profiled enemy.

4.5.3. Threat Intel Correlation

Threat intelligence comes alive when an organization has an understanding of who is attacking. Numerous paid and free services exist that provide threat intelligence. These services can be another point of white noise devoid of any background information. Put another way, threat intelligence is useless if there is no context. When the organization understands who the current adversary is and what they are looking to attack, a more structured defense can be created around the actual attacks. Conpot is a mechanism for identifying who is attacking and what they are trying to accomplish. The techniques used can be correlated via a threat intelligence service (IPs, file hashes, or techniques) to see if there are any attacks occurring against other systems or organizations. Knowing who the adversary is and what they are seeking clears up the FUD cloud and can even help address the ROI and ROSI shortfall.

5. The [Incomplete] ROI and ROSI + AROI

The ROI and ROSI fall short in justifying what the organization requires in terms of protection from a security perspective. The reason they both fail in addressing the security issues is that they lack the capability to identify the root of the problem; instead, they focus on symptoms. ROI does not factor in risk exposure or potential mitigation that the ROSI addresses. ROI assumes that the technology purchased will return on the initial investment. This too is a misnomer because it does not actually make money for the organization. Rather it can save money or prevent certain expenditure should a security incident occur and only if the incident occurs. If the adversary changes tactics, the newly purchased security device could become irrelevant.

The ROSI factors in risk and mitigation if a particular technology is purchased. It is more nebulous because it goes off of past attack data, such as the amount of ransomware infections an organization observed over the past year. Leveraging the ROSI for an anti-malware system would require a larger scope of systems or assets, instead of approaching the issue from a risk perspective. If the adversary were after critical infrastructure, it would make sense to protect the infrastructure the adversary would be after and the infrastructure that could have the most impact to the organization.

5.1. What the ROSI Can Do

The ROSI is not entirely useless and does have a purpose; however, it should not be used to mitigate a more advanced adversary. The ROSI can be a good starting point to analyze historical incident data. Based on the data, a security mitigation plan can be devised. “If the method for determining ROSI produces repeatable and consistent results. ROSI can serve as a useful tool for comparing security solutions based on relative value” (Sonnenreich, Albanese, Stout, 2006). An example of malware for which a signature exists could warrant a solution to mitigate the issue. However, this assumption would have to factor in the current environment and the damage, or clean-up, that would be required if known malware were to infiltrate the organization. This mitigating strategy can be useful for dealing with the casual attacker or wayward user. What the ROSI falls short on, the AROI can make up for; specifically, by increasing detection time and reducing the chance of success.

5.2. AROI as a Replacement for ROSI and ROI

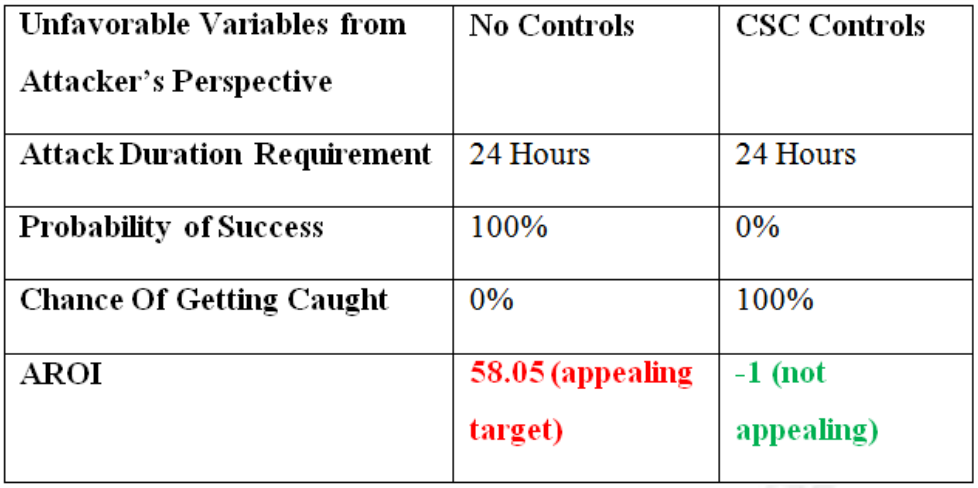
Replacing the antiquated ROSI and ROI with the AROI can help an organization realize where to prioritize defenses. There are several variables that can truly impact an adversary's view or tactics against a particular target. If using the AROI as the formula to determine of an attacker would be interested in attacking an ICS, several variables can help to deter the adversary. Primarily, the cost of the attack, probability of success, deterrence measures, and chance of getting caught are of interest to an organization looking to make a hard target out of their ICS. These variables are what drive down the appeal of the target because the degree of difficulty goes up drastically. What should be noted is that the amount of money spent to increase the difficulty of the attack does not necessarily mean increased security technology and may encompass process improvements or more vigilant system administration. An example of this could be an organization's desire to implement a layer 7 firewall to restrict traffic flow to a particular Human Machine Interface (HMI) over port 80. With ROSI, the case can be justified where previous incidents where attacks over port 502 were successful. Incident response and system restoration could be decreased if those additional ports are restricted. In this example the case could be made that the firewall is worth the expenditure. What this model failed to take into account is that the web interface that is still accessible has a default password still enabled, and is ultimately what the adversary wanted access to in the first place. One method that can be employed is the Critical Security Controls (CSC) to help make a hard target out of an ICS.

6. Decreasing the AROI on an ICS with Critical Security Controls

The Center for Internet Security (CIS), Critical Security Controls (CSC) are an effective method to deter an adversary targeting ICS. In most ICS environments, the systems and infrastructure are relatively static, giving the upper hand for a defender. The CSC fit well in this model, requiring minimal change or burden to the current infrastructure. Further, the Controls work and are aligned to the reality of an active adversary and not a checklist of best practices. “The CIS Critical Security Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals)” (2015). Additionally, the CSC aligns with frameworks in use, such as the NIST Cyber Security Framework. For these reasons, the controls are a proven method for guarding against the most advanced adversaries and sensitive infrastructure. Although, the CSC includes 20 controls, only first three will be examined to illustrate their effectiveness as they relate to an ICS.

6.1. CSC #1 – Inventory of Authorized and Unauthorized Devices

By minimizing the adversary’s ability to remain undetected, the more difficult a target becomes. The focus of CSC #1 is on devices, both approved and illicit. “Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access” (2015). In the context of an ICS, approved devices would be those devices which participate in the control process (PLCs, HMIs, process controllers). The AROI decreases drastically by increasing the variables an attacker would find unfavorable, that is, prevention and detection. From an environment that does not detect unauthorized devices to one that does can mean the difference between detection and not. Figure 14 illustrates, from a very simplistic view, how even the most basic control can be at increasing the unfavorable variables to an attacker. The values used to calculate the AROI was used from figure 4, modifying the probability of success and chance of getting caught in figure 13. According to version six of the CSC, devices should be detected within 24 hours and isolated within one hour of detection (Tarala, Tarala, 2015). The attack duration is added to highlight the default, or minimum recommended time to detect and alert on an unauthorized device found. This figure also assumes that the attack will require 24 hours to be successful.



Unfavorable Variables from Attacker's Perspective	No Controls	CSC Controls
Attack Duration Requirement	24 Hours	24 Hours
Probability of Success	100%	0%
Chance Of Getting Caught	0%	100%
AROI	58.05 (appealing target)	-1 (not appealing)

Figure 13. No controls versus the CSC from an AROI perspective.

CSC #1 is great at detecting and alerting on unauthorized devices. Appendix C illustrates a minimalist approach to this control via a simple script. If the adversary attacks via an authorized device, such as a pivot point, CSC #1 will fail to detect this behavior; this is why the second control is complementary of this foundational control.

6.2. CSC #2 – Inventory of Authorized and Unauthorized Software

The CSC #2 focuses on the authorized and unauthorized software running on an authorized system. Because it builds upon CSC #1, it is foundational that Control #1 is operating correctly. The objective of CSC #2 is to: "manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution" (2015). This control is effective in deterring and detecting systems that are compromised or are used as a pivot point in the environment. Similar to CSC #1, any new software should be noticed within 24 hours and alerted on within one hour of detection (Tarala, Tarala, 2015). The control can start with simple checks such as port scans to identify new software, or as it matures, it can help to prevent unwanted code execution. With an ICS that can support unwanted code execution, such as a Windows OS, the amount of required and authorized software should be small and static. CSC#2 recommends using "application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system" (2015). All of these tests and scanning should of course be vetted through a change management process and thorough testing so there is minimal impact to production systems. The last control to be evaluated is CSC #3.

6.3. CSC #3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The CSC #3 further minimizes target appeal for an attacker by leveraging secure configurations. For CSC #3, the goal is to "establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings" (2015). From an ICS perspective, there may not be an easy way to automate this practice; however, it can be an administrative policy that requires some basic configuration settings. Settings such as changing default credentials, restricting administrative functions to only authorized devices and requiring change management review before making changes can drastically reduce the attack surface of the ICS. "A lack of configuration change management procedures can lead to security oversights, exposures, and risks. To properly secure an ICS, there should be an accurate listing of the assets in the system and their current configurations" (Stouffer, Lightman, Pillitteri, Abrams, Hahn, 2015).These configuration settings further decrease the probability of success and increase the chance of getting caught—all which make the ICS a harder target.

7. Conclusion

Gone are the days of simply of simply using best practices to secure an organization operating a critical Industrial Control System (ICS). To target an ICS, the attacker only requires a valuable target. The target need only meet the adversary's appetite for a return on the attack investment. Numerous attacks have permeated some of the most assumedly secure systems, such as pipelines, centrifuges and power grids. Attack data points to an ever prevalent adversary who is actively looking for vulnerable and critical infrastructure. The issue stems from the fundamental problem of failing to factor in the Adversary's Return on Investment (AROI). This return, if great enough, will lead to or foreshadow an attack. For this reason, it is clear that traditional models such as the Return on Investment (ROI) or more comprehensive Return on Security Investment (ROSI) fall short in providing an accurate estimate for return (or simply cost savings) that an organization strives to get out of security investment. Focusing effort on modeling real threats against an organization can begin to lift the veil and reveal who the real adversaries are. As the cloud of confusion clears up, an organization can more accurately and effectively deploy defenses that focus on the real adversary. The Critical Security Controls (CSC) are a valid and efficient set of controls for decreasing the adversary's return, which could deter or prevent an attack altogether. It is time to rethink how an adversary views critical infrastructure, especially infrastructure that can reap a hefty return.

References

Assante, M. (2016, January 9). Confirmation of a Coordinated Attack on the Ukrainian

Power Grid. Retrieved June 05, 2016, from https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

Carr, J. (2012, June 7). Digital Dao. Retrieved May 28, 2016, from http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html

The CIS Critical Security Controls for Effective Cyber Defense Version 6.0. (2015,

October 15). Retrieved June 04, 2016, from https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER 6.0 CIS Critical Security Controls 10.15.2015.pdf

Corman, J. (2013, May 23). “Best practices” aren’t – that “Good enough” isn’t. Lecture

presented at RMISC 2013, Denver.

Corman, J., & Etue, D. (2012). Adversary ROI [PDF].

Cyber Security — Incident Reporting and Response Planning. (2009, December 16).

Retrieved May 29, 2016, from

http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-3

Flame (malware). (2016). Retrieved June 05, 2016, from https://en.wikipedia.org/wiki/Flame_(malware)#Origin

Homan, J., McBride, S., & Caldwell, R. (2016, June 2). IRONGATE ICS Malware:

Nothing to See Here...Masking Malicious Activity on SCADA Systems « Threat Research Blog. Retrieved June 05, 2016, from https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

Impe, K. V. (2014, December 10). Cudeso/cudeso-honeypot. Retrieved June 05, 2016,

from https://github.com/cudeso/cudeso-honeypot/blob/master/DOC/conpot.INSTALL.md

Incident Summary: 199004220006. (1990). Retrieved June 07, 2016, from https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199004220006

Incident Summary: 199912300002. (1999). Retrieved June 07, 2016, from https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199912300002

Joint Publication 3-12 (R): Cyberspace Operations. (2013, February 5). Retrieved May

27, 2016, from http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Langill, J. (2014, December). Defending Against the Dragonfly Cyber Security Attacks.

Retrieved May 29, 2016, from http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

NCCIC/ICS-CERT Year in Review. (2016). Retrieved May 8, 2016, from https://ics-

cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

Rist, L., Vestergaard, J., Haslinger, D., Pasquale, A., & Smith, J. (n.d.). CONPOT

ICS/SCADA Honeypot. Retrieved June 03, 2016, from http://conpot.org/

Robinson, P., Lasker, L., & Parkes, W. (1992). Sneakers Script - Dialogue Transcript.

Retrieved May 28, 2016, from http://www.script-o-rama.com/movie_scripts/s/sneakers-script-transcript-robert-redford.html

Scarborough, R. (2013, August 18). In classified cyberwar against Iran, trail of Stuxnet

leak leads to White House. Retrieved June 05, 2016, from http://www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/?page=all

Shostack, A. (2014). Threat modeling: Designing for security. Wiley.

Smith, R. (2014, February 5). Assault on California Power Station Raises Alarm on

Potential for Terrorism. Retrieved June 05, 2016, from http://www.wsj.com/articles/SB10001424052702304851104579359141941621778

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment

(ROSI) -- A Practical Quantitative Model. Journal Of Research & Practice In Information Technology, 38(1), 45-56.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015, February).

Guide to Industrial Control Systems (ICS) Security. Retrieved June 5, 2016, from

http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf

Tarala, J., & Tarala, K. (2015). Implementing and Auditing the Critical Security Controls

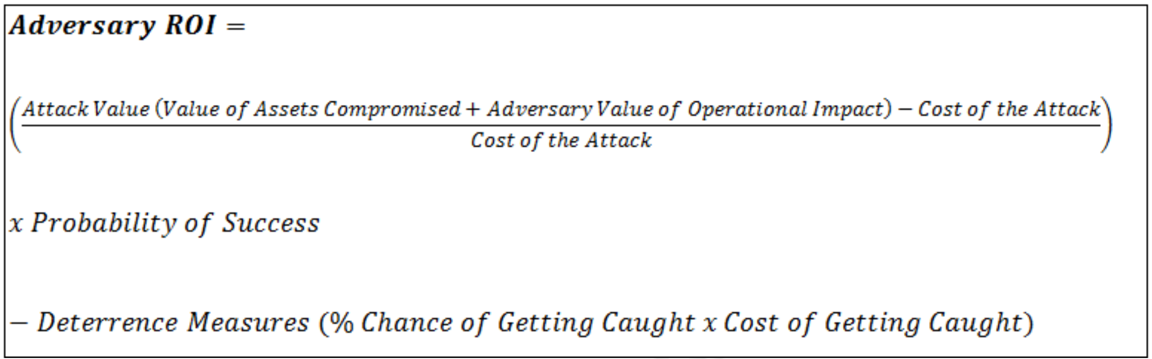
-- In-Depth. The SANS Institute.

Vélez, T. U., & Morana, M. M. (2015). Risk centric threat modeling: Process for attack
simulation and threat analysis. Hoboken, NJ: John Wiley & Sons.

Wilhoit, K., & Hilt, S. (2015, August 06). The GasPot Experiment: Unexamined Perils in
Using Gas-Tank-Monitoring Systems. Retrieved June 02, 2016, from
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_gaspot_experiment.pdf

Appendix A

The Adversary Return of Investment (AROI) Formula



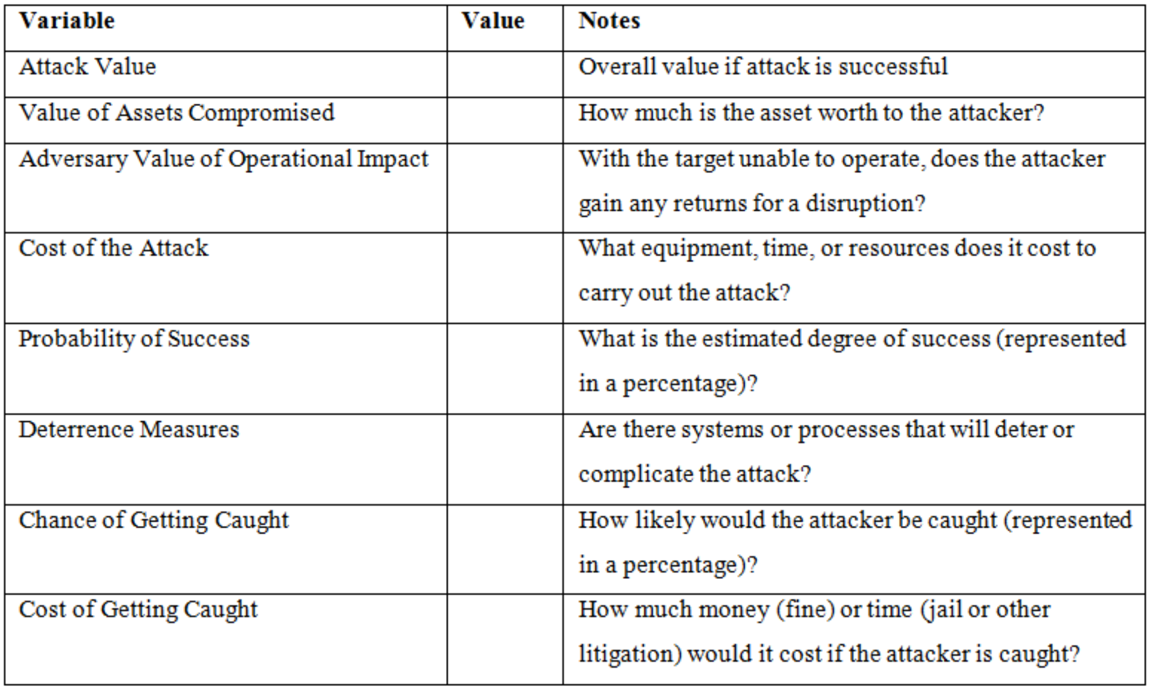
$$\textbf{\textit{Adversary ROI}} =$$

$$\left(\frac{\textit{Attack Value (Value of Assets Compromised} + \textit{Adversary Value of Operational Impact)} - \textit{Cost of the Attack}}{\textit{Cost of the Attack}}\right)$$

$$x\ \textit{Probability of Success}$$

$$-\ \textit{Deterrence Measures (\% Chance of Getting Caught x Cost of Getting Caught)}$$

(Corman, Etue, 2013)



Variable	Value	Notes
Attack Value		Overall value if attack is successful
Value of Assets Compromised		How much is the asset worth to the attacker?
Adversary Value of Operational Impact		With the target unable to operate, does the attacker gain any returns for a disruption?
Cost of the Attack		What equipment, time, or resources does it cost to carry out the attack?
Probability of Success		What is the estimated degree of success (represented in a percentage)?
Deterrence Measures		Are there systems or processes that will deter or complicate the attack?
Chance of Getting Caught		How likely would the attacker be caught (represented in a percentage)?
Cost of Getting Caught		How much money (fine) or time (jail or other litigation) would it cost if the attacker is caught?

Appendix B

Conpot Setup and Initial Configuration

Background video on Conpot: https://youtu.be/x0Pci-jrlRE

1. Install

From http://glastopf.github.io/conpot/installation/ubuntu.html

```
sudo apt-get install libsmi2ldbl snmp-mibs-downloader python-dev libevent-dev
libxslt1-dev libxml2-dev
```

If you get an error **E: Package 'snmp-mibs-downloader' has no installation candidate** then you will have to enable multiverse. Do this with **sudo vi /etc/apt/sources.list ; sudo apt-get update**

Additionally, you might need to run for conpot to work on Debian 7.2.0:

```
sudo apt-get install libmysqlclient-dev
pip install mysql-python
pip install conpot
```

```
cd /opt
git clone https://github.com/glastopf/conpot.git
cd conpot
python setup.py install
```

This will install all the necessary packages and install the conpot python package. The python package ends up in a location similar to **/usr/local/lib/python2.7/dist-packages/Conpot-0.3.1-py2.7.egg/**.

2. Starting conpot

Conpot needs root privileges (because some services bind to ports below 1024). It drops privileges to nobody/nogroup once started. You can start the honeypot with

```
sudo conpot
```

You'll get a list of available templates if you start if with no options

- --template kamstrup_382 ** Kamstrup 382 smart meter ** Services *** Kamstrup (tcp/1025) *** Kamstrup (tcp/50100)
- --template proxy ** Demonstrating the proxy feature ** Services *** Kamstrup Channel A proxy server (tcp/1025) *** Kamstrup Channel B proxy server (tcp/1026) *** SSL proxy (tcp/1234) *** Kamstrup telnet proxy server (tcp/50100)
- --template default ** Siemens S7-200 CPU with 2 slaves ** Services *** Modbus (tcp/502) *** S7Comm (tcp/102) *** HTTP (tcp/80) *** SNMP (udp/161)

If you start conpot with the **-h** option then you get a list of configuration options. The three most useful are

- --template : what template to use
- --config : where is the config file
- --logfile : where to write the logs

The default logging is to a file **conpot.log** in the current directory.

Start it with

```
conpot --config /etc/conpot/conpot.cfg --logfile /var/log/conpot/conpot.log --
template default
```

3. Configuration

The configuration is in the file **conpot.cfg**.

3.1. Services configured for proxy template

By default the proxy template has no http, snmp, etc. service configured.

```
No modbus template found. Service will remain unconfigured/stopped.
No s7comm template found. Service will remain unconfigured/stopped.
No kamstrup_meter template found. Service will remain unconfigured/stopped.
No kamstrup_management template found. Service will remain
unconfigured/stopped.
No http template found. Service will remain unconfigured/stopped.
No snmp template found. Service will remain unconfigured/stopped.
```

3.2. Adding a template

The easiest way for adding a service template is by copying it from an existing one. For example to add the http service template to the proxy template you can merely copy it from the 'default' template.

If you're running conpot from the package then you'll have to reinstall it (sudo python setup.py install).

3.3. Fetching public IP

Sometimes you'll notice outgoing tcp/80 connections when starting conpot. This is because it tries to obtain its public IP. By default the service at telize.com is used. You can change this by altering the configuration setting :

```
[fetch_public_ip]
enabled = True
urls = ["http://www.telize.com/ip", "http://queryip.net/ip/",
"http://ifconfig.me/ip"]
```

3.4. Database configuration

3.4.1. mysql

Out of the box contop will log to a flat file. If you prefer mysql then first create a database, set proper permissions and change the setting in the config file.

```
create database conpot;
mysql> create user 'conpot'@'localhost' identified by 'conpot';
mysql> grant all privileges on conpot.* to 'conpot'@'localhost';
mysql> flush privileges;
```

Do not worry that the database is empty, without tables. conpot will create the necessary tables when it starts. In conpot.cfg change this

```
[mysql]
enabled = True
device = /tmp/mysql.sock
host = localhost
port = 3306
db = conpot
username = conpot
passphrase = conpot
socket = tcp        ; tcp (sends to host:port), dev (sends to mysql
device/socket file)
```

Do not leave out any of the settings. If you are not using sockets you might by tempted to leave out 'device'. This will prevent conpot from starting.

3.4.2. sqlite

Similarly to mysql, you can also configure sqlite in the configuration file. Conpot will use the path **logs/conpot.db** for storing the sqlite database (see conpot/core/loggers/sqlite_log.py)

3.5. Other logging features

Conpot can also log / report to syslog and HPFeeds, these are disabled by default. You'll want to enable and add TAXII support.

Within conpot.cfg, enable the following to log to HoneyNet

```
[syslog]
enabled = True
device = /dev/log
host = localhost
port = 514
facility = local0
socket = dev        ; udp 192.168.1.10:514 (sends to host:port), dev (sends to
device)

[hpfriends]
enabled = True
host = hpfriends.honeycloud.net
port = 20000
ident = 3Ykf9Znv
secret = 4nFRhpm44QkG9cvD
channels = ["conpot.events", ]
```

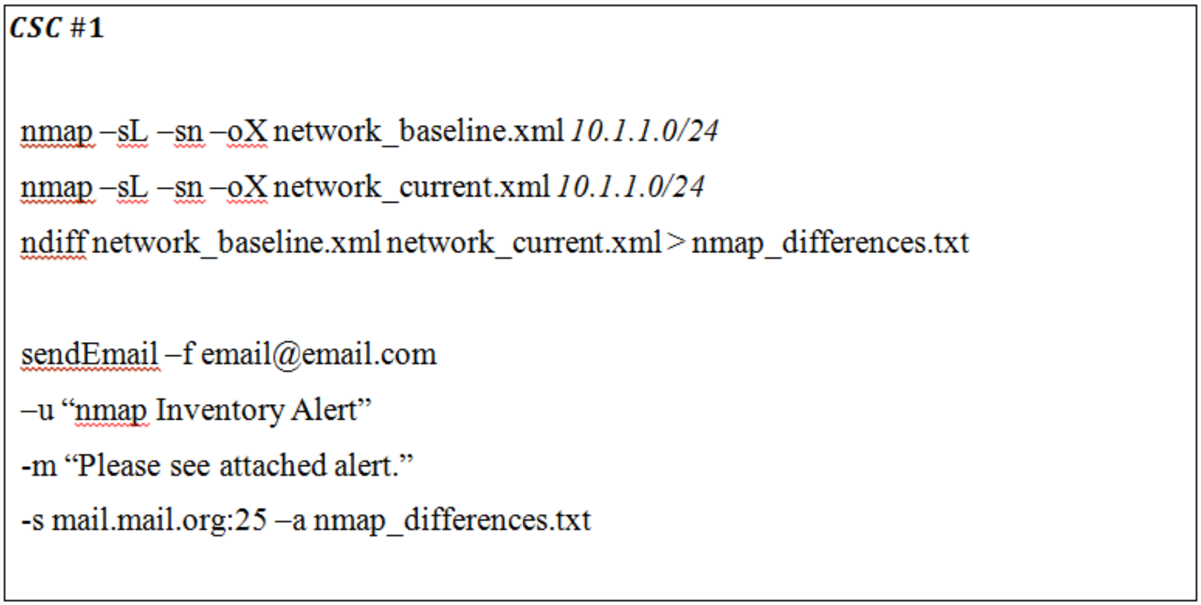
```
[taxii]
enabled = True
host = taxiitest.mitre.org
port = 80
inbox_path = /services/inbox/default/
use_https = False
```

(Impe, 2014)

Appendix C

Critical Security Controls 1 – 3 minimalist scripts

Note: These scripts should be vetted in a test environment before running on live ICS networks. The scripts should be scheduled via a cron job or scheduled task for reoccurring, automated scanning and alerting.

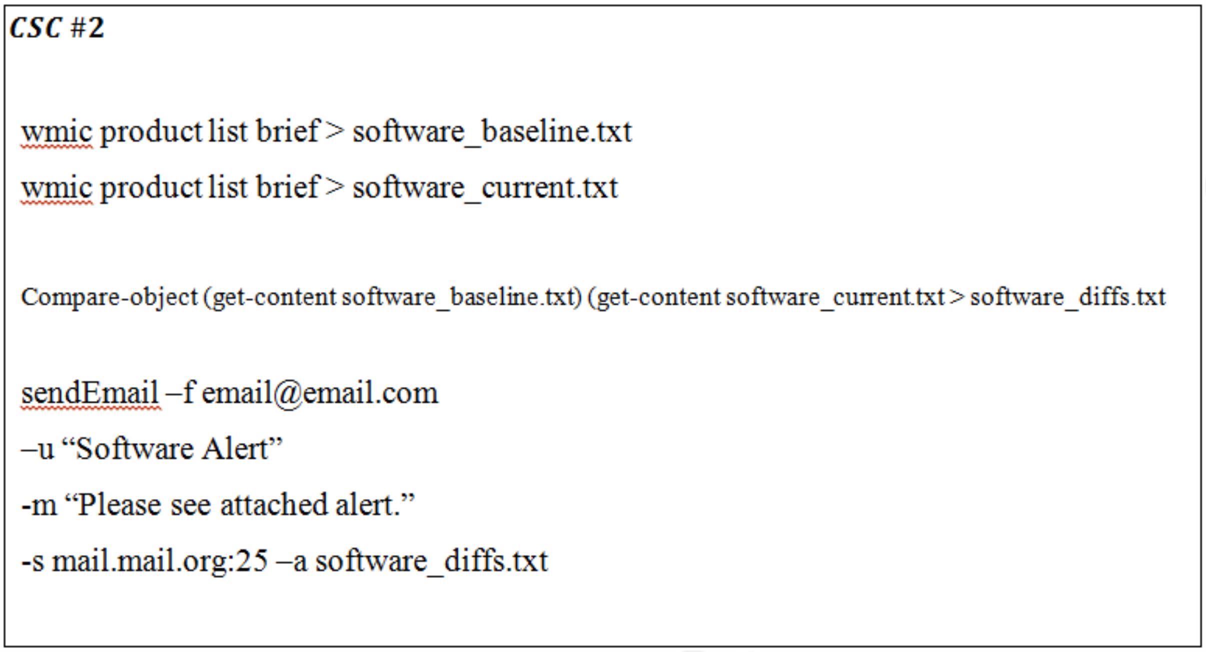


CSC #1

```
nmap –sL –sn –oX network_baseline.xml 10.1.1.0/24
nmap –sL –sn –oX network_current.xml 10.1.1.0/24
ndiff network_baseline.xml network_current.xml > nmap_differences.txt


sendEmail –f email@email.com
–u “nmap Inventory Alert”
-m “Please see attached alert.”
-s mail.mail.org:25 –a nmap_differences.txt
```

(Tarala, Tarala, 2015)



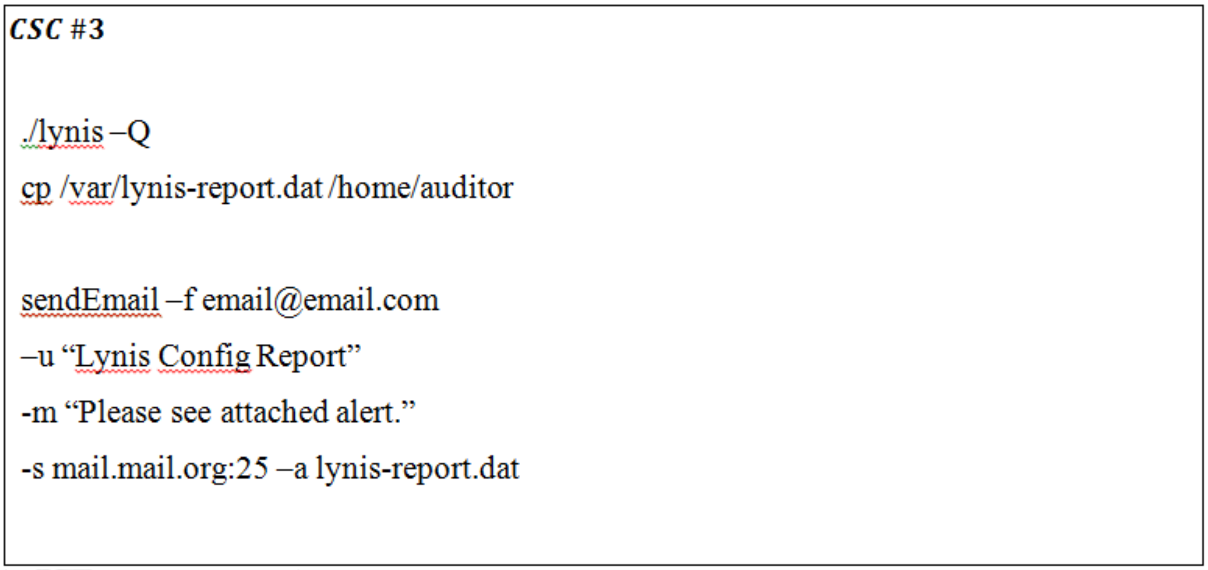
CSC #2

```
wmic product list brief > software_baseline.txt
wmic product list brief > software_current.txt

Compare-object (get-content software_baseline.txt) (get-content software_current.txt > software_diffs.txt

sendEmail –f email@email.com
–u “Software Alert”
-m “Please see attached alert.”
-s mail.mail.org:25 –a software_diffs.txt
```

(Tarala, Tarala, 2015)



CSC #3

```
./lynis –Q
cp /var/lynis-report.dat /home/auditor

sendEmail –f email@email.com
–u “Lynis Config Report”
-m “Please see attached alert.”
-s mail.mail.org:25 –a lynis-report.dat
```

(Tarala, Tarala, 2015)