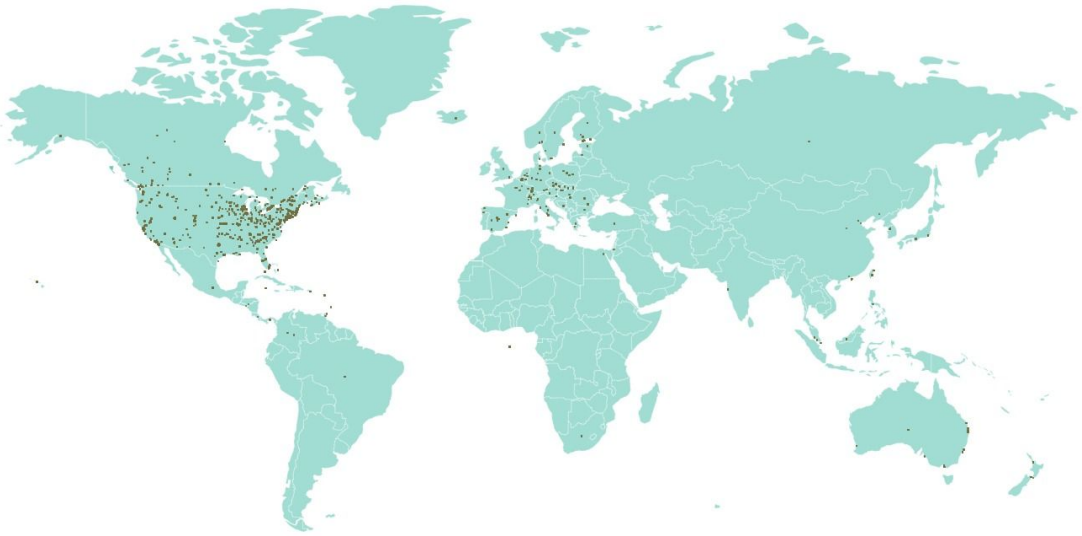
ICS security

Assignment block 3



Summary

During the previous assignment, we have analysed a security issue caused by the accessibility of ICS devices. Using this security issue and a single stakeholder (the organisation that owns the device), severable metrics have been identified which can be used in order to measure the security of such devices. In this assignment we will focus on identifying the actors that play a role in the security issue, as well as analysing the possible security strategies and their feasibility to mitigate the security risk.

TU Delft

Harm Griffioen	-	4303598
Lars van de Kamp	-	4501829
Harikrishnan Manikandan	-	4613201
Hans Schouten	-	4314891

The security issue at hand

First let us introduce the security issue at hand as described in the previous assignment. Industrial Control Systems (ICS) are part of critical infrastructure that companies, and society as a whole, heavily rely on. When access to these systems is granted to the wrong people, this could lead to large disruptions in everyday life. The Shodan ICS dataset [Shodan ICS] lists numerous Industrial Control Systems that are publicly accessible via the internet. Even when these are password protected, the systems should not be accessible from anywhere else in the world other than on-site or from specific control rooms. In addition, using password bruteforcing or exploitation of vulnerabilities in the firmware any publicly accessible Industrial Control System could get compromised. The high impact that the underlying infrastructure makes on civilization as a whole, makes the analysis crucial to fortify the defenses around the globe. This analysis on the threat on ICS devices is done by analyzing the situation from the perspective of the organizations that own the equipment. The actor that we therefore define for the use in this document are the organizations that use the ICS devices.

Problem owner of the security issue

Definition problem owner:
In most cases he or she is the one affected by the issues to be solved or indicates those who would benefit from the solution [Problem Owner].

In the first assignment, our main focus was on the organizations that owned the industrial control system and view of the security issue. This perspective helped to create several metrics that are able to assess the current situation and can act as a guideline to validate the effectiveness of new investments or controls. In addition, several other stakeholders are involved in the security issue and hand and will be elaborated upon next.

Stakeholders

Due to the vast presence of industrial control systems around the world, there is a huge variety in stakeholders in the security of those devices. These different stakeholders can be divided into direct stakeholders, those that are directly linked to the systems, and indirect stakeholders that are impacted by the indirect results of a possible attack.

Direct stakeholders

- Organization, the organization obviously has a large stake in the problem at hand. The company risks the compromise of one of the devices that they themselves are responsible for. This could for example lead to a loss in customer confidence, several lawsuits and damaged equipment. These different consequences increase the probable loss magnitude through several loss factors as defined in the FAIR framework [FAIR].
- Customer, the end consumer of the organization's services is also impacted by the security issue. For some examples, the end consumer might be difficult to formulate, or could even be the government, but the agreed upon service might be disrupted due to a successful attack by a threat agent.

Indirect Stakeholders

- In certain scenarios, the environment can also be severely impacted. Due to the malfunctioning of an ICS, the surrounding flora and fauna can be harmed. For example, in case of a flooding due to a malfunction dam this could change the entire ecosystem at its base.
- Society, in addition to direct stakeholders, other individuals that initially have no direct relationship with the system can be impacted. This means that people that do not consume energy from the above mentioned dam, are still impacted by a potential attack. This also includes third party businesses, who can incur loss of revenue and reputation due to the inability to offer their usual service.
- Insurance industry. Even though this can also be considered to be a third party business, the size of the impact on this industry warrants a bit more detail. The damage caused by an attack will largely impact the insurance industry in that region due to the large amount of claims that will be incurred. Therefore, the large importance and huge impact surface of these systems, also makes this industry an indirect stakeholder.
- The ISP that facilitates the connectivity of the critical infrastructure element also has interest in the security issue. The attacks are conducted through their infrastructure and offering security as a service with the help of the information they have on a service provider level might give them an edge over other ISP's. The ISP's have access to a lot more information about the packets, their origin and the routing than the organization itself. Furthermore, ISP's can implement mechanisms like egress traffic filtering to filter out malicious traffic and possibly prevent attacks on ICS in the first place. ISPs are also indirectly affected by attacks on organization, using their infrastructure as mentioned before. Although such attacks do not cause direct or immediate damages to the ISPs, consistent successful attacks might lead to distrust amongst its consumers about the security of its infrastructure causing damages to the reputation of the ISPs.
- Manufacturer, The manufacturer produces the hardware used in the installation. Their configurations and brand name can attain bad publicity due to an attack and might cause a lowered demand from there on out. The incurred damage would mainly be caused by external loss factors [REF], since the actual asset is not owned by the manufacturer anymore.
- Besides governments being potential customers as well, they can also be indirect stakeholders. First of all, the impact of an attack can strain international relations when looking for potential wrongdoers. When critical infrastructure of a country is attacked, it can be seen as an attack on the nation (and its allies) as a whole shifting the global geopolitical situation. In addition, the government has a fiduciary duty to protect its citizens and when the critical infrastructure is not functioning properly, it might be very difficult to uphold this responsibility. Finally, although they may not be the actual security provider, security consumer or the security industry a number of successful attacks in their soil could perceived as weak policies or their implementation, rightly so or not. This could lead to some services that have geographic mobility to move to other countries with better perceived risk scenario.

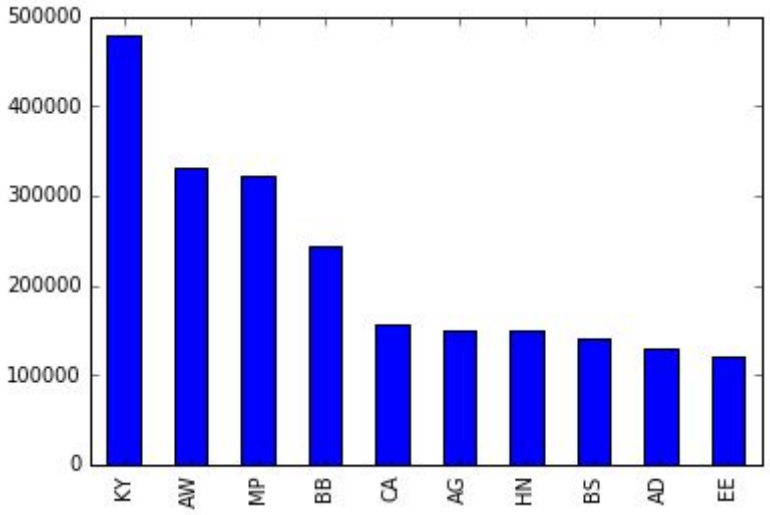
Even though, the organization owning the equipment is identified as the main actor for our initial security analysis, it is believed that all above mentioned stakeholders in their own way have a role in the security issue.

Relevant differences in security performance with the metrics

This section will analyse the metrics defined in the previous assignment and elaborates on how each of them exposes the security issue. It will show insights on how various companies perform on the different security metrics.

The number of accessible devices per location

This metric estimates the no. of accessible devices that are accessible, per country. This is normalized with the ratio of IPv4 addresses assigned to that country and the total IPv4 space. Using this metric on our dataset reveals the top 10 locations to be:

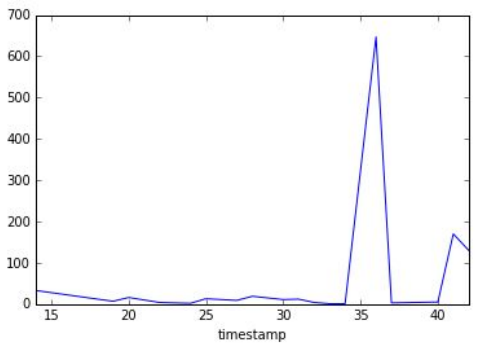


Accessible devices per location

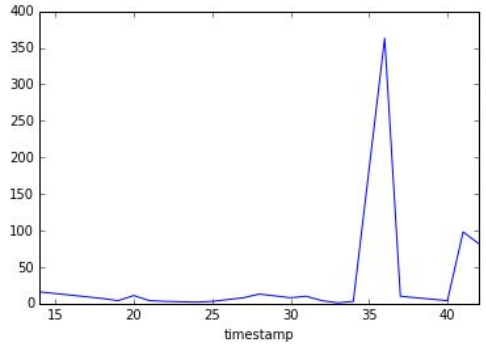
The top 10 countries are Cayman Islands, Aruba, Northern Mariana Islands, Barbados, Cambodia, Madagascar, Saint Helena, Bahamas, Antigua & Barbuda and Cocos (Keeling) Islands. Their high score in this metric is due to the normalization with their IPv4 space ratio. This metric indicates that devices in these countries might have a higher chance of being accessible online. This metric could be flawed as the IPv4 space of the industrially developed countries is much larger than the top 10 countries, thereby exaggerating the results for these countries.

Number of publicly accessible devices over time

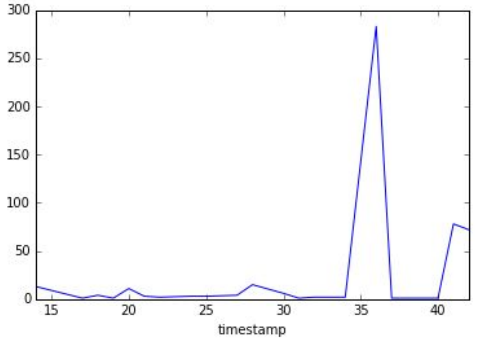
This metric is the time series of the number of devices accessible per company. This helps to assess the trend for an organization with respect to its competitors. Below are the trends for the companies with the highest number of breaches and the overall trend:



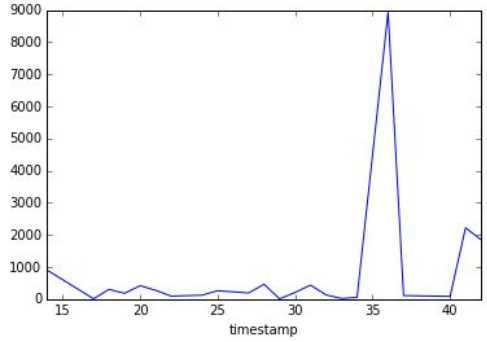
AT&T Internet Services



Comcast Business Communications



Comcast Cable

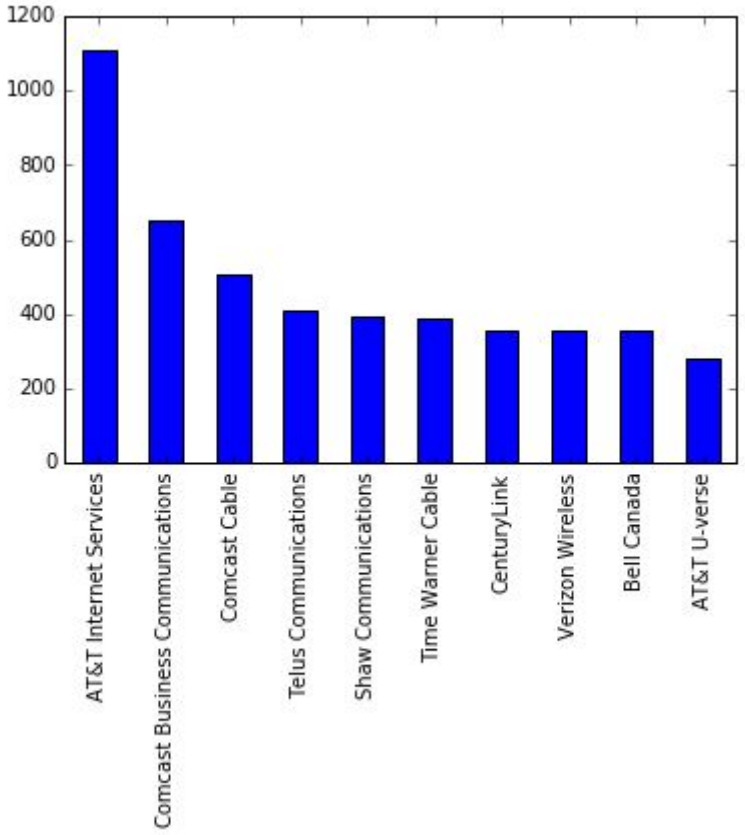


Overall

Since the number of breaches is not normalized per company, we only observe the trends for the companies. We can see that there are 2 big peaks around the 35th and 41st weeks for all the 3 companies and in the overall trend. This could imply that all the companies were vulnerable to a particular attack and this isn't due to lacking security measures in any single one. In addition, the availability of certain ICS systems could have sparked a hype to check whether more are actually online. Therefore, this period could resemble a large group of individuals locating accessible ICS devices and reporting it to be included in this dataset. Most probably, it resembles a flaw in the dataset since it does not represent the introduction of , but the discovery of the accessibility.

The number of accessible devices per organization

This metric shows the number of device accessible per organization. The top 10 organizations are:



The number of accessible devices per organization

As this metric could not be normalized, this is more probabilistic than the normalized metrics. Since AT&T and Comcast have similar market capitalization values, the higher number of accessible devices in AT&T Internet Services could imply that it is less secure than its competitor. The table below shows different demographics for the organizations from the top 10 that are not divided into departments. From these demographics, the Net Property Plant & Equipment is the most notable. This is the total worth of physical assets the company owns minus the depreciated value[1].

	Tellus	Shaw	CenturyLink	Bell canada
Nr of employees	39000	15000	40000	49968
Revenue	$ 9.97	$ 3.91	$ 17.47	$ 17.21
Operating income	$ 1.84	$ 1.78	$ 2.33	$ 6.84
Net income	$ 1.10	$ 0.63	$ 0.63	$ 2.18
Total assets	$ 22.31	$ 9.20	$ 47.02	$ 32.97
Net Property Plant & Equipment	$ 7.85	$ 2.78	$ 19.44	$ 13.33

When dividing the amount of physical assets by the number of accessible devices, we attain the following ratios. This indicates that Shaw Communications has more accessible devices per billion dollars of physical assets then the other three analyzed companies. From this one

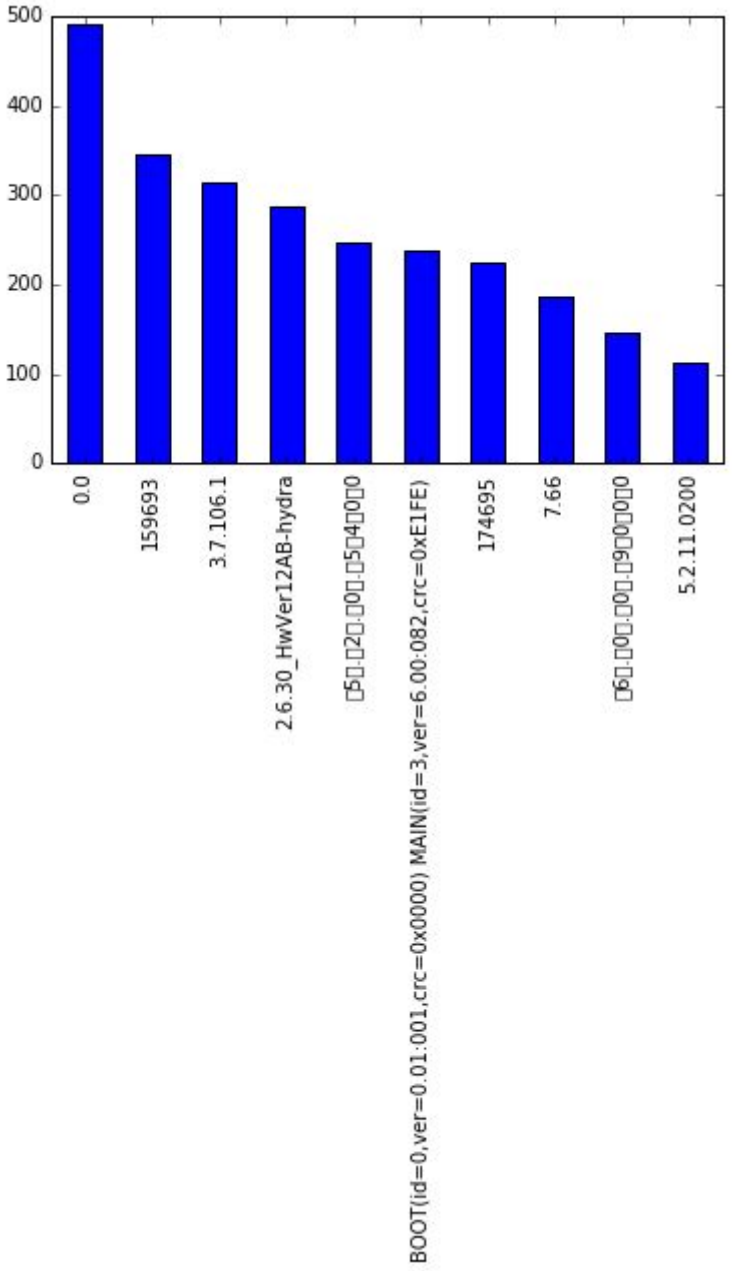
[1] All values are USD, Canadian dollars are converted at the end of 2016 exchange rate.

could conclude that the security awareness of this firm is lower than that of the others, whereas the exact opposite could be said for CenturyLink.

	Tellus	Shaw	CenturyLink	Bell canada
Devices per Billion $ of net PPE	17.93	41.30	7.76	10.92

Update frequency

The firmware versions with the highest breaches are:



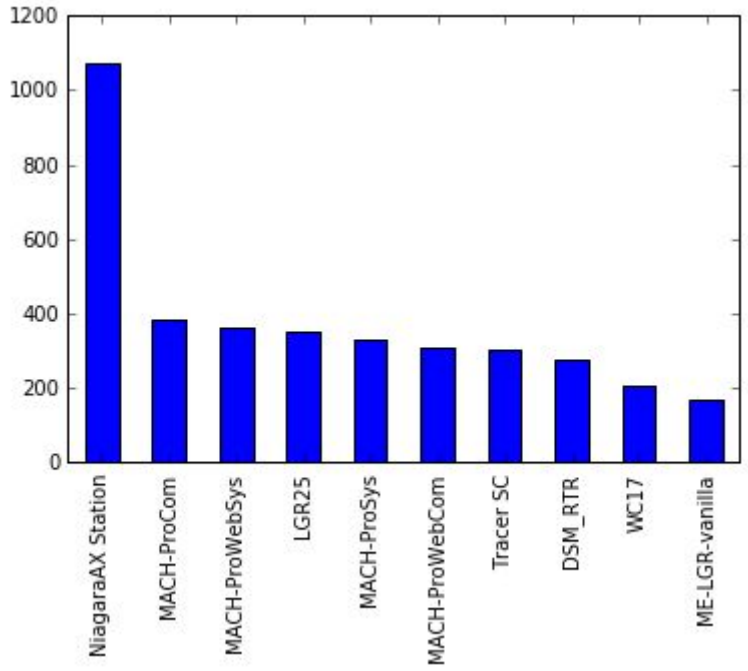
Number of breaches per firmware version

This metric has little to no use as the version numbers are missing for most of the entries in the dataset and the existing ones are not properly structured either. This cannot be used to

assess the security performance of the devices. In an ideal situation where the appropriate data would be available this metric could very nicely review an important part of the security situation but unfortunately this would not help us identify security improvements based on applied strategies.

Manufacturer

The device manufacturers with the highest number of breaches are below:



Number of breaches per manufacturer

Since this metric isn't normalized, it is hard to gauge the security performance of these devices standalone. There is a need for knowledge on the market capitalization, but this information isn't easily available. Hence, an educated idea of comparison of market shares has to be considered. For instance, if the market shares for NiagaraAX Station and MACH-ProCom are close, then it can be understood that the devices from NiagaraAX Station fare poorer in security and are more likely to be accessible online.

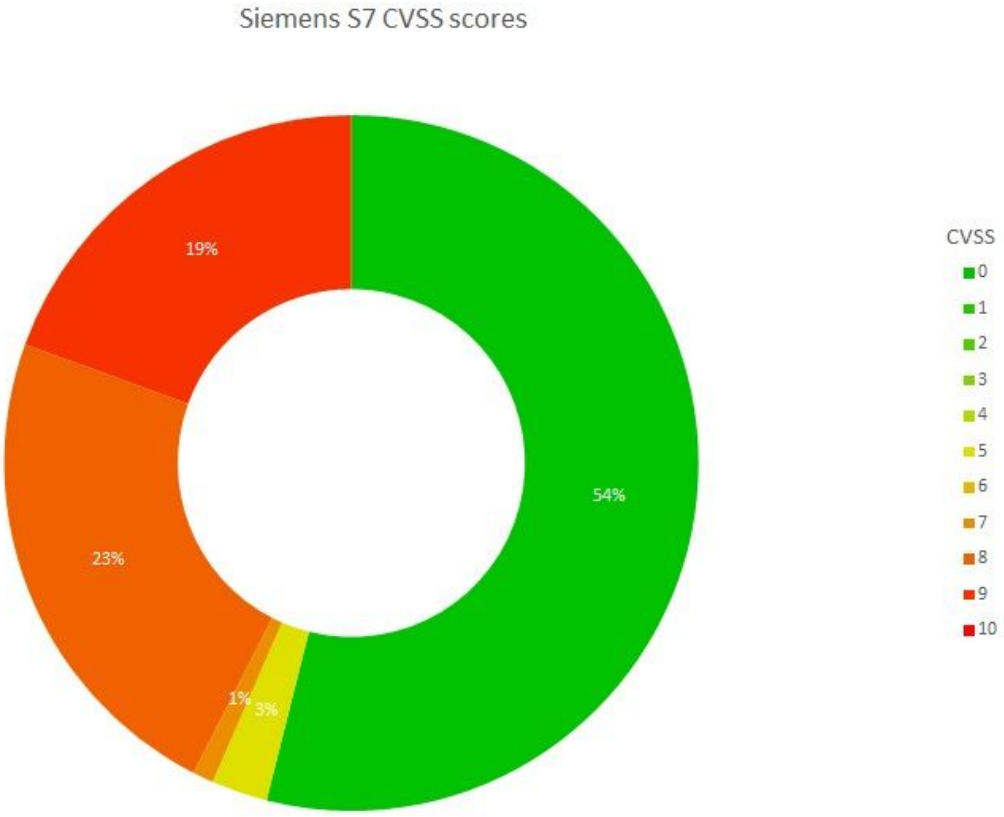
The number of firmware vulnerabilities

As described in the first assignment, by cross-referencing the current version numbers with a list of known vulnerabilities for specific versions [CVE Details, NVD], the score of the most critical vulnerability can be used as a metric defining the lack of security in a specific system.

In the figure below, the distribution of the resulting scores is shown. The highest CVSS score is tracked for each of the systems. Aggregating the number of occurrences of the maximum CVSS scores of all systems gives an overview of how many systems are at each level of security deficiency. Since these amounts in itself do not yield much information, they are normalized over the total number of Siemens S7 devices in the dataset (3710). In the calculations, 676 devices were ignored as they did not contain any version information. The resulting numbers show that 19% of the successfully scanned Siemens S7 devices have at

least one vulnerability of criticality 9. Since 23% of all devices have at least one vulnerability of criticality level 8, almost half of all systems have a vulnerability with high criticality on the CVSS scale.

The CVSS score will change when security improvements are made. This clear distinction in the metric value allows for validation of the effectiveness of the security measure. When fewer vulnerabilities are present or less severe ones, it is clear that the security situation has indeed improved. Companies that are now in category 10, can then hopefully join their colleagues that are currently given a score of 0-3.



Risk strategies that reduce the security issue

The risk management strategies the problem owner could follow can be divided into four main categories: risk reduction, risk acceptance, risk avoidance and risk transfer.

Risk Reduction

By applying technical and organizational measures, vulnerable assets can be protected to reduce the likelihood and severity of loss events. Among technical measures, more controls can be adapted like for example implementing physical and remote access control as well as adding an Intrusion Detection System, a demilitarized zone and firewalls. With respect to the previous assignment *the number of publicly accessible devices over time* metric can be drastically reduced by implementing proper network segmentation. Furthermore, penetration tests and red teaming can be performed to identify vulnerabilities in an organization's

systems and policies. As soon as vulnerabilities are discovered, they should be addressed, resulting in an improvement of our *number of firmware vulnerabilities* metric.
Possible organizational measures that can be applied are reducing the risk of successful social engineering attempts by providing awareness training and reducing the loss of, and accelerating the recovery after, incidents by setting up a Computer Emergency Response Team. Also implementing a software patching policy is a recommended organizational measure when possible. This measure will improve on the *update frequency* metric as defined in our previous assignment.

Risk Acceptance

The security issue can also be addressed by accepting parts of the risk imposed on the problem owner. This is a favourable option if no other risk management instrument is economically viable. The defined metric: *amount of accessible devices per location* is a clear example of a metric that could be deliberately ignored. If a company is forced to operate in a certain area, they can hardly improve on this metric and might choose to accept the risk instead.

Risk Avoidance

Another approach is to avoid certain factors of the risk. By following this strategy the security risk is reduced as a result of adjustments in the organization's operations. As an example, the problem owner could opt for Industrial Control Systems of highly trusted vendors that take a lot of effort in ensuring high security standards of their devices. Practising this strategy yields an improvement on the manufacturer metric, as previously defined.

Risk Transfer

The final strategy is to transfer the risk by drafting a contractual agreement with a third party to compensate the risk owner for losses incurred due to the realization of risk. In our last metric, it is mentioned that certain high profile institutions might be more attractive targets due to their larger potential impact on society. If more hackers are interested in a system, due to a higher potential impact, the likelihood of an attack increases. Therefore, it may be beneficial for these type of organizations to transfer risk to an insurance company. In this situation risk transfer presents the risk owner with a suitable strategy to further reduce its security risk.

Actors that influence the security issue

As introduced in the first question, there are a number of stakeholders in this security issue. Other actors, apart from the organization (security consumer), who can significantly influence it are:

- The Manufacturers of the devices, which can be considered to be the security provider.
- The ISPs whom connect the devices to the network who also are security providers.
- The Government who could impose rules and mitigations concerning the threat at hand.
- An Attacker also plays a vital role in the security issue and could amplify the intensity of an attack by remaining unnoticed.

Risk strategies for actors

Obviously a threat agent such as the attacker, has completely different incentives than the other identified parties. Their way to mitigate risk purely focuses on untraceability and not getting caught. For the other parties such as the manufacturer, this focus largely lays on improving internal security policies and standards to deliver a higher level product, but the primary goal of a manufacturer would be to maximize profit rather than to deliver a secure product. Finally, the ISP and Organization have fairly similar strategies as it would involve testing the system for vulnerabilities, disconnecting the systems, and providing physical access control.

Strategies over time

Originally, the manufacturers were mainly focused on attaining profit & cost efficiency and placed much lesser emphasis on the security issues arising from the socio-technical layer of the cyberspace. Due to their disconnected nature, the need for security was extremely limited from their perspective and required hardly any attention. Now on the other hand, the potential reputation loss, resulting in customer loss, causes them to change their strategy reducing the risk of an attack with every step.
In general, all actors have become more aware of the security situation and are attempting to switch their strategy in such a way that the security issue is in fact reduced. Due to the abundance in attacks that have occurred over the last period, the probability of their systems being affected increases and the incentive to act has grown a lot. In addition, governments have stepped up, realizing the importance of the situation, deploying their own protective measures or legislation. An example of such a method is the ICS-CERT of the United States government [ICS-CERT], whose aim is to reduce risk within all critical infrastructure sectors.

Each of the different actors can implement different security measures. In the following section we will go into detail on what these are and how they will help in reducing the risk of the security issue.

Manufacturer

- Manufacturers can mitigate the risk of reputation loss by implementing higher security standards in their devices. Producing devices with better security, reduces the likelihood of being used in successful attacks and hence reduces the chance of dissatisfied customers. This will decrease the time to market of new products and will require a higher research and development budget. This part of the strategy can be seen as increasing control strength of the asset, thereby reducing the vulnerability of the system at hand [FAIR].
- It is also important for the manufacturer to ensure that the manufacturing process is secure. During the manufacturing process, devices could be altered by malicious persons. This could also happen during the manufacturing of individual components. Therefore it is vital to know where different components come from and whether it is advisable to outsource or insource the production of those components. This mapping would require the creation of a complete system model and all possible ‘attack paths’ in this model that could compromise a device [Weakest Link]. A good

strategy in this aspect will reduce the devices with security flaws made by this manufacturer. Therefore, it might lead to a decrease in publicly accessible devices.

- By default, a lot of devices ship with security settings disabled. For example, modbus does not have any authentication by default. This ensures that the device is plug and play and therefore the manufacturer does not have to help as much with troubleshooting. To create higher security standards, organizations must be forced to use the security standards which are placed in the devices. For example, modbus should be shipped with authentication enabled by default. This will reduce the number of publicly accessible devices from the manufacturer, again through an increased control strength.

Internet Service Providers

- ISPs run the risk of lagging behind on their competitors. If competitors offer more extensive protection against various kinds of attack scenarios, this will be disadvantageous for a less security aware ISP. This is called the 'Network Effect' which states that you only have to be more secure than your peers since the least secure will most likely be targeted [REF]. This risk can be mitigated by adopting protection methods against attacks like for example traffic egress filtering.
- System logging is also a vital point in increasing the security from the ISP's perspective. These logs can help identify malicious or anomalous network traffic and help in incident investigations that occur when the system has been breached. This will improve the organization's ability to detect and respond to threat events that have already occurred or are occurring, improving their ability to properly respond and reduce the loss incurred in terms of organizational loss factors [FAIR].
- The introduction of an Intrusion Detection System can allow the ISP to notice illicit traffic and warn their clients on the possible attacks. This could help their reputation instead of harming it, and could even be offered as an additional security system to their end-clients.
- Furthermore, a dedicated red-team could be assembled to test the multiple ICSs linked to their network. Their privileged position could allow them to gain economies of scale and execute these penetration tests in a more affordable and efficient way.

Organization

- Before the interconnectivity of ICS systems, updates were rarely needed. Now the organizational processes would need to change in order to facilitate a due process. In order to do this, the steps proposed in Enisa [2016] can be followed. Here it is proposed to create a clear overview of all the assets and connections present in the environment. This includes all assets with their current version and purpose in the system, all interconnections between the different actors, a detailed user lists combined with access rights, and the locations of all factors mapped on a system diagram. This system model could allow the organization to use different attacker models and see what their most likely attack paths will be and thus where the weakest links in the system are [Weakest link].
- Just like mentioned for the ISP, logging is also a vital process for the organization. It is not a labor intensive measure but can be a gateway to faster problem resolution and new techniques. This could increase the awareness of the accessible devices of

the organization. Logging is also a vital step in incident response. This helps the organization to respond quicker as it is easier to see what is going on.
- The devices maintained by the organization should also be subject to clear configuration management. When reviewing the known vulnerabilities, one should make sure that none are enabled due to a faulty configuration of the device.
- By introducing periodic red-teaming exercises, a third-party will test all aspects of the organization's security, identifying vulnerabilities. This lowers the number of active vulnerabilities on the devices, although this can be a rather expensive recurring cost. Nevertheless, it could lower the loss event frequency due to less successful attack paths into the system [FAIR].
- By implementing a password policy, employees are required to use more secure passwords, lowering the number of devices that are easily accessible with some guessing or by using rainbow tables.
- By providing awareness training to employees the risk of for example successful social engineering attempts can be reduced. This prevents otherwise secured devices to accessible to adversaries.

Attacker

- The attacker can mitigate the risk of getting caught by using an anonymous networking service like Tor.
- In addition, it is recommended for the attacker to use a secure location. This ensures that if a successful trace is conducted, nothing can be linked back to a person. This means that a place without camera's would be preferable, or a place where an attacker does not stand out of the crowd.

Return On Security Investment

The previous section identifies the risk strategies that the actors can adopt to address the security issue. This section will elaborate on computing the expected annual losses with and without implementing these strategies. From these values, the Return Of Security Investment will be derived.
In order to properly do this analysis, we have chosen to do so for two different actors. The organization and the ISP are both in a position to severely impact the security issue. Therefore, we will compare both and see whose strategy would have the most effect and whose would be the most efficient.
First, we state the general assumptions made throughout the computations. After which, the assumed annual losses of an attack are shown. This is followed by a scenario analysis of the frequency and magnitude of these attacks and the cost of our proposed security strategies. Finally, the percentage of the attacks in either frequency or magnitude is estimated and the ROSI's are computed.

General Assumptions

Before we can put numbers on the annual losses, general assumptions on which the cost benefit analysis is based should be defined. First of all, the target organization is within the United States. We make this assumption because the US is well represented in the dataset. Furthermore, we will define the amount of employees in terms of FTE (Full Time

Employment). This way, it does not matter for the calculations if the employees are working part time or full time. The total number of working days are assumed to be 230 (or 1840 hours) per employee per year. This takes into account weekends and holidays and possible sick days. There are 260 weekdays in a year, on average 10 vacation days [Public holidays USA] and 8 paid sick days [Sick days]. In addition, there are twelve paid holidays [Paid vacation days]. When computing the final number of working days we get 260 - 12 - 8 - 10 = 230. There are more assumptions that are being done, but they will be explained in their respective sections.

Loss analysis of Organization

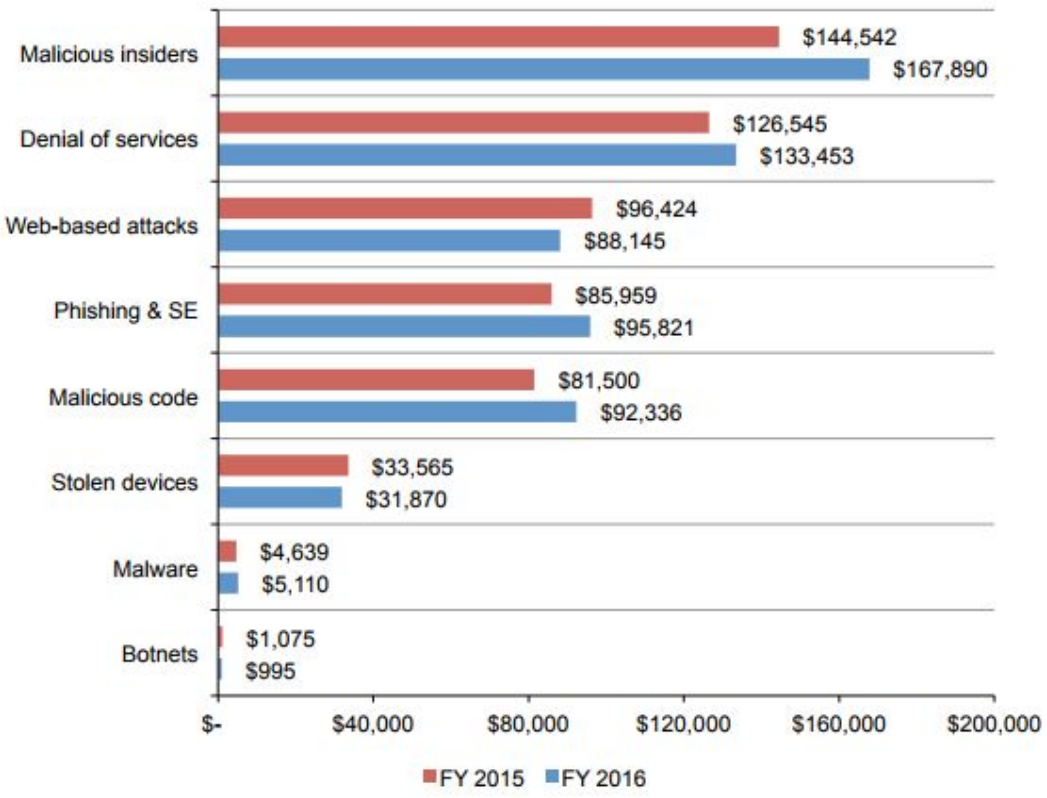
Annual Losses for the Organization

In order to quantify the annual losses of the organizations using ICS, the statistics of a recently published report by Business Advantage and Kaspersky LAB on industrial cyber risks [The State of Industrial Cybersecurity 2017] will be used. Another used source of information is the report on Cost of Cyber Crime Study & the Risk of Business Innovation from 2016 from Ponemon Institute [Cost of Cyber Crime].

Annual losses originate from different risk sources, we will therefore focus on the following eight attack vectors:

- Malware
- Phishing and Social Engineering
- Web-based attacks
- Malicious code execution
- Botnets
- Leakage by stolen devices
- Denial Of Service
- Insider threat

Some attack vectors, like insider threat, are quite rare but have a high impact and will therefore induce large financial losses. Hence, it is needed to normalize losses by their rate of occurrence to come up with the annual loss. The study from Ponemon Institute has analysed cyber crime incidents of over 237 separate companies throughout 7 countries, and computed the average annualized cyber crime cost weighted by their attack frequency.



Average annual cyber crime costs per attack vector, weighted by attack frequency

The figures in the graph show that an average organization experiences a loss of $618,620 annually.

The figure above does not take into account ICS devices, but rather companies using software. We believe that for a company using ICS devices the loss will be higher. This occurs due to the fact that there are a lot more indirect losses involved with ICS devices and the attack impact is much higher. In order to illustrate this, we take an hydroelectric power plant located inside a dam in a rural area in the United States. We will list direct and indirect losses below.

Implications of an attack on the power plant:
Direct losses

- Physical damages to the power plant due to the attack, there are different ways the power plant can be shut down but there is a large chance that some part will be broken/damaged.
- The loss of revenue due to not being able to provide their service to their customers.
- Damage claims from the down-time, companies lost business when the power is out (depends on the contract).
- As the power plant is inside a dam, floods could occur.

Indirect losses

- Third party company losses due to lack of internet and power in general.
- Consumers that have loss of trust in the power company.
- Negative media coverage.

- There are several possibilities, even though unlikely, that due to a loss of power incidents will occur that could cause death. Think about all the traffic lights that will be inoperable all of a sudden.
- Because of the nature of the issue, a malicious attack, the problem might not be the loss of power, but the overloading of the power grid. If there is more power supply than demand which is all distributed over the network, infrastructure might break because of an higher load than expected.

It is obvious that there are a lot more costs involved in an attack on ICS devices than on a company that only uses software. These costs occur because of the direct consequences that device malfunction has on the environment and society. Therefore, we believe that a certain multiplication factor is needed for the annual loss that was defined before to be $618,620. The amount of multiplication is hard to determine, as malicious insiders for example would be able to do devastating amounts of damage, while DDoS attacks are not really applicable. In order to make a solid assumption, we take our power plant example. If we take the Shasta Dam in California, the production capacity is 1,806.5 GWh [Shasta Dam]. This means that the production capacity is about 5 GWh per day. The average cost of one kWh in the US is $12 cents [Electricity Cost]. This means that each day, this power plant is capable of generating 600,000 USD in revenue. If we estimate the attack frequency to (in total) cripple the facility for one day each year, the loss of revenue alone would almost equal the annual loss defined before. We assume that the indirect costs at least equal the direct costs, and therefore we think that a multiplication factor of 2 is needed in order to compare ordinary companies with ICS companies.

Do note that we assume that the loss is distributed in a normal distribution, where there are attacks that will result in a loss lower than this value as well as higher, but it is concentrated around this point.

Scenario analysis for the losses incurred for the organization

As explained in the above chapter the conservative estimate of the losses for an organization are around $1,236,166. This estimation has to be extrapolated for different scenarios of threat environment as we need better estimations of the losses incurred specific to our threat environment. We will look at three scenarios for the loss amount analysis that differ in terms of frequency and indirect loss impact.

- Scenario 1 (Conservative scenario) - Such a location is intrinsically secured to a certain extent from digital attacks due to the poor connectivity between the infrastructure and the internet at the loss of lower efficiency and technological capabilities. We assume that such a location might also have higher frequencies of stolen devices and insider threats due to the lack of sophisticated technologically enabled control mechanisms. Overall, we assume a low yearly occurrence of two attacks per year.
- Scenario 2 (Average case scenario) - Using the standard direct loss estimations, and increasing the indirect multiplication to 3 we create a more realistic scenario. In this scenario due to an more impactful location the indirect loss increase significantly and the number of attacks also increase to what we see more likely as being 5 attacks per year.

- Scenario 3 (Highly advanced and interconnected infrastructure location) - In this scenario, the digital threats are assumed to be higher due to the high integration of the company infrastructure with the internet to have greater capabilities in remote monitoring and control. Thereby, the frequency, and hence probably losses, due to threat paths like phishing, DDoS, web-based attacks, etc. are amplified. At the same time, we can also assume that the general digital awareness of the workforce from such a location would be higher than average. In addition, we assume that the indirect costs are amplified as well due to the interconnectivity of the location. The multiplication factor of 2 is changed to a multiplication of 5 since we assume that this is a significantly large part of the loss. Due to the high potential impact we assume that the attack frequency will increase depending on the attack which is incorporated in the individual attack costs.

The direct losses in these threat environments are naturally different and an estimation for each of the environment based on the individual vulnerabilities are shown below:

Scenarios	**Losses (in $)**								
	Malicious Insiders	**Denial of Service**	**Web-based attacks**	**Phishing**	**Malicious Code**	**Stolen Devices**	**Malware**	**Botnet**	**Total Loss**
Scenario1	251,836	66,727	44,073	95,821	92,336	63,740	2,555	995	618,083
Scenario2	167,890	133,453	88,145	95,821	92,336	31,870	5,110	995	615,620
Scenario3	167,890	200,180	176,290	76,657	92,336	19,122	7,665	1,990	742,130

This means that the total losses for each scenario will become:

Scenarios	Total Direct Loss	Multiple for Indirect	Total Loss	Loss event frequency	Total yearly loss
Scenario 1	618,083	2	1,236,166	2	2,472,332
Scenario 2	615,620	3	1,846,860	5	9,234,300
Scenario 3	742,130	5	3,710,650	8	29,685,200

Cost analysis for ISP

The losses suffered by ISPs due to attacks on the organizations it serves are almost purely external as mentioned previously. These losses are incurred through the loss of reputation and ceding market shares to its competitors. Hence, we will analyse the losses incurred through losses in market shares. Obtaining data on possible losses in market shares due to prolonged attacks is not easily possible, so we will make assumptions on the possible losses in market shares and also that the revenue of organization remains constant. For our case, we will take the ISP to be Comcast, one of the largest telecommunication companies in the US. The total revenue of Comcast is about 80.4 billion dollars [Comcast Earnings]. We will

consider market share losses of 0.05%, 0.1% and 0.15% due to the attacks that occur in a year.

Scenario analysis for losses incurred

As mentioned previously, the losses incurred by an ISP are taken as losses in market shares. The scenarios under our consideration are 0.05%, 0.1% and 0.15% loss in market shares. The actual amount of the loss is shown below for the three scenarios. This includes the amount of loss for an attack * the average number of organizations. This assumes a 0.00125%, 0.0025%, and 0.00375% loss per organization attacked with an average of 40 organizations connected to an ISP as can be seen in the graph below.

Scenarios	Loss	
	Percentage (in %)	Amount (in $)
Scenario 1	0.05	40,200,000
Scenario 2	0.1	80,400,000
Scenario 3	0.15	120,600,000

Monetary loss per scenario

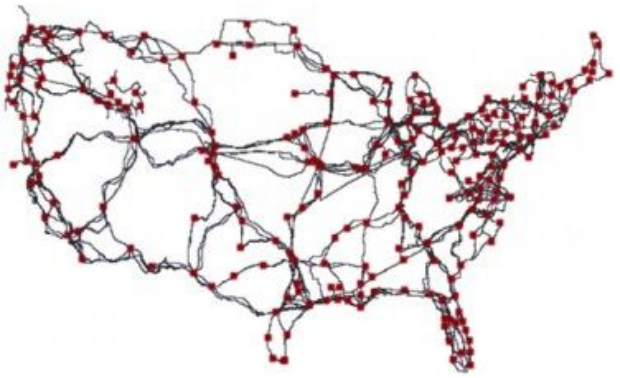
Costs of implementing mitigation strategies

Internet Service Provider

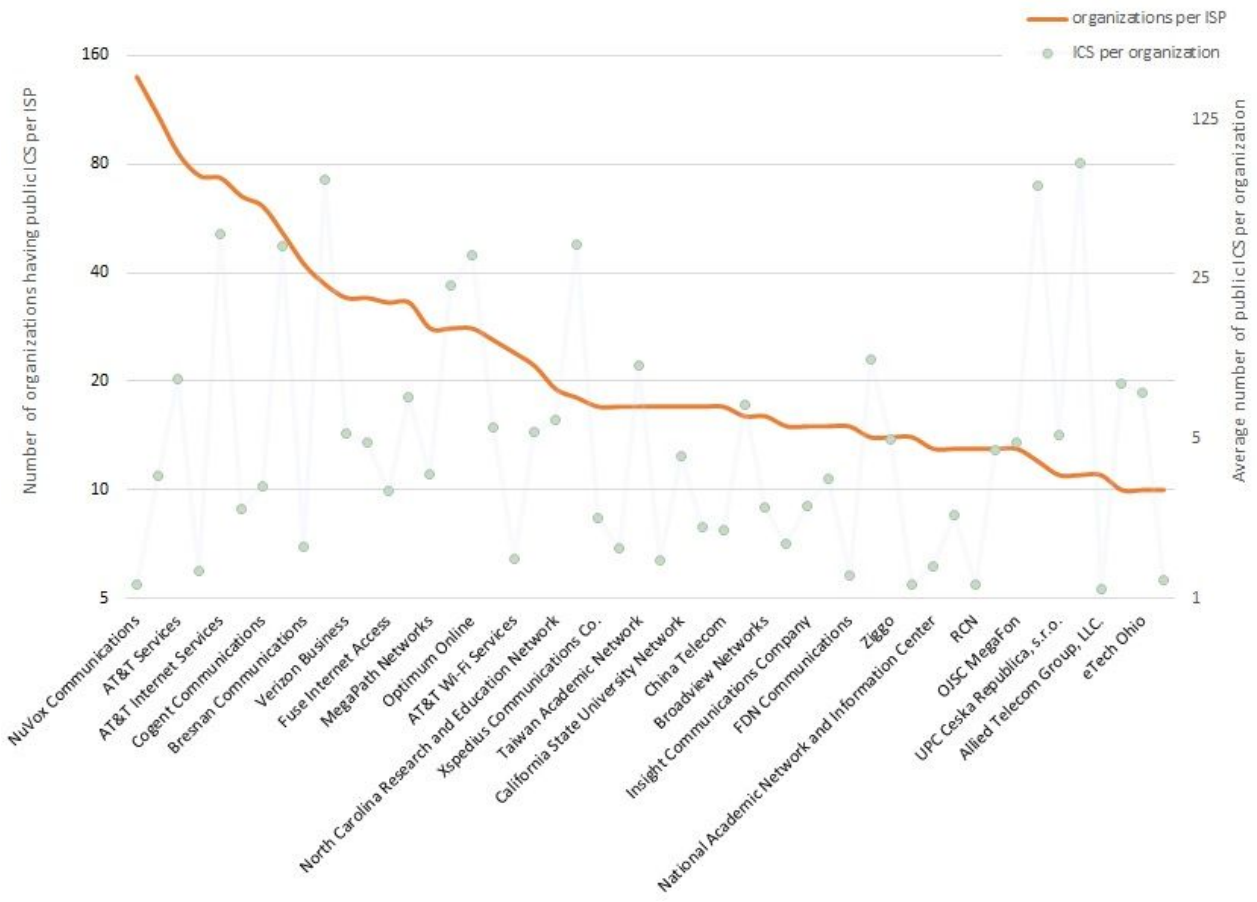
For the ISP the following costs have been identified:

- In order to adopt new protection methods (like traffic egress filtering), it has to be implemented, but most importantly, it has to be maintained. In order to do so, the ISP could start a Security operation Center (SoC). In a small organization, a small SoC would be enough. A small SoC can be maintained by 3-4 people, meaning that about 4 FTE is needed in order to implement this. Due to the immense size of ISPs, some having more than 200,000 employees, this team would not suffice. To manage this, we estimate that the SoC should consist of around 60 employees working full-time. This means that this will cost 60 FTE on a yearly basis.
- In order to implement logging, we believe that one full time employee would be able to do this. We have spoken to the person that is in charge of logging in the Department of Justice in the Netherlands. His job is to ensure that all legal documents that are sent from attorneys to judges can be tracked at every step of the way. This ensures that no documents can be lost and human error can easily be tracked. He said that he has one year of full time employment in order to implement this logging system and that this is a feasible time. Therefore, implementing logging will cost 1 FTE. Analysing the logs and acting accordingly should be done in a SoC, see point above.
- To implement an IDS, the most obvious solution is to have a SoC (see the first point). Specialized hardware is also needed in order to do this, the most common way of doing intrusion detection is to mirror all network traffic to the SoC where it is analysed. Mirroring the traffic can be done using enterprise switches, which retail at

around $900 each. The amount of switches needed depends on the extent that the ISP wants to monitor the traffic. If the IDS is optional and has to be paid for, the ISP does not have to implement this for every company and therefore needs less specialized equipment. The data that comes into the SoC also needs to be analysed. This is mostly done using GPUs as they have a high data throughput and can easily be parallelized [Sathik, 2012]. A NVidia Quadro P6000 is rated at 432 GB/s and retails at around $5000 excl. VAT. The amount of GPUs needed is also dependent on the extent of monitored traffic. These devices will be accounted for in our cost analysis using depreciation of 20% yearly. We assume that the ISP would need an IDS at every connection point to the backbone of the internet [Internet Backbone] which can be seen in the figure to the right. These are assumed to be able to handle all traffic aimed at critical infrastructure and would result in approximately 150 devices. This would lead to an annual depreciation of $180,000 per year.



- Creating an ICS dedicated red-team at the ISP to test organizations in their network will need a lot of people. Red-teaming is not done in a day, but requires planning and a report has to be made afterwards. Based on our conversations with penetration testers at DongIT we assume that it will take a team of 3 people about one weeks to red-team a company. After combining all Shodan ICS dataset [Shodan ICS], we created an aggregation of the number of organizations with publicly accessible ICS per ISP. The data shows a clear power law, with a few very large ISPs and a long tail of small ISPs. The figure below shows the top 50 ISPs ranked on the number of customers having publicly accessible ICS. Note, that the actual numbers will be larger since companies using ICS that are not publicly accessible are not present in the graph. Assume that one on 5 companies using ICS have a publicly accessible device, then each of these ISP has at least 50 customers which can be offered red teaming twice a year. With 2 teams of 3 security specialists, taking into account about 4 weeks of holiday per person, 96 assessments can be performed per year. So each of these top 50 ranked ISPs could at least employ 2 red teams to full time test their customers. This will cost an ISP 6 FTE, but enables them to offer this service to a lot of their customers.



Number of organizations with publicly accessible ICS devices per ISP

In order to implement all mitigation strategies, an ISP would need a SoC (60 FTE), Logging (1 FTE for 1 year), IDS Hardware: (180.000 USD per subnetwork mirror) and Red teaming (6 FTE). This means that in total, 71 FTE are needed in the first year and 70 FTE in subsequent years. Additionally, 5900 USD per subnetwork mirror which recurs every few years (if something breaks). One FTE of a computer professional costs on average $121,245 [Salary costs], including all fees and expenses such as retirement. Therefore the constant costs of these solutions are $8,667,150 per year, and some variable costs.

Organization

For the organization the following different cost parameters have been identified:

- Due to the large nature of the organization in the dataset, creating a clear overview of the entire ecosystem is a vital, but an extensive process. In the initial setup of this organizational map, it will require 8 FTEs (Full-time employee) for the first half a year to set up the initial version. It is assumed that in order to successfully do this in the long-term, 4 FTE (Full-time employee) should be dedicated to this process. The overview will continuously change, and firmware versions should be monitored. In addition, in order for these full-time employees to map the organization, several other actors need to provide them with the required information. This will lead to a lowered productivity that we assume to add 4 additional FTEs.

- Just as mentioned in the cost specification for the ISP, logging is defined to cost approximately 1 FTE for a year in order to setup and maintain the infrastructure.
- Monitoring the logs, and applying configuration management, should be the responsibility of two system managers. These individuals shall monitor the logs for any conspicuous intelligence and make sure that the devices are monitored properly. This will cost 2 FTE.
- Hiring an external company to periodically test the organization security would cost approximately 250 euros per person per hour. This amount has been established during our interview with the red-team present at DongIT [DongIT penetration tests]. Additionally, the duration of such an assessment would be between 5 and 7 days for a single site with a three person team. The benefit, of hiring an external company would be the novel insights and dedicated expertise that is gathered in the industry, compared to a more biased or tunnel-vision approach that an internal team would offer. If we assume this would need 5 days, three persons working 40 hours on this would cost €30.000. This would be 35,191.50 USD. Due to the criticality of the infrastructure we assume that two yearly test need to be done.
- Finally, awareness trainings and password policies can be delivered by the same company that provides the red-team, often these services are combined. Similar costs per hour would be incurred as mentioned for the red-team. However, only a single person would hold a seminar for a day. Better awareness will increase the security of the company, however it will come with the cost of some productivity loss due to the fact that employees cannot continue their usual work during the training sessions. Assume that awareness trainings take 8 hours (preparation and training). Using the same costs per hour as penetration testing, this would mean that an awareness training costs 2,346.10 USD. Assuming 20 people in a training losing productivity of approximately 12,000 USD assuming an internal hourly rate of 75 USD. If this training is done periodically for different departments with 10 trainings per year we will have a yearly cost of 143,461 USD.

To fully implement the mitigation strategies as an organization, one would need a clear overview of the dataset, logging, system managers, awareness trainings and penetration tests. In order to implement this, one would need 11 FTE in the first year and 11 FTE in the years after that allocated differently. The constant costs also include the penetration testing and awareness trainings and using the salaries that were also used for the ISP part, the constant costs each year will be: 1,547,539 USD.

Percentage mitigation

The damage mitigated by implementing the security measures in the previous section will have an effect on the direct and indirect costs. Some of the mitigation strategies focus solely on direct cost mitigation, some on indirect cost mitigation, and some have impact on both direct and indirect costs.

Internet Service Providers

The usage of an intrusion detection system, traffic egress filtering, and detailed logging will allow for faster response to incidents and thereby, reduce the impact on its reputation.

A dedicated red-team will improve the reputation of the ISP while locating possible vulnerabilities. This reduces amount of vulnerabilities, which we assume will lower the attack frequency. At the same time, the team can be used as an emergency response allowing attacks to be mitigated faster limiting indirect costs.
Therefore, we assume that based on this strategy, the frequency of the attacks will be reduced by 50% due to the vulnerabilities found by the red team. However, the red team will mostly stop low skilled hackers and script kiddies. Because of the attack vectors for ICS devices, nation state actors and high skilled hackers will also be interested in these ICS devices. Therefore, the total amount of damage reduced will not be 50%, as the higher skilled attackers will do way more damage. We therefore assume a frequency reduction of serious attacks of 5%. On the other hand, the response measures greatly reduces the impact of an attack on the indirect costs reducing this by 25%. Here the reduction of the indirect cost is fairly large since we assume that due to the indirect relation of the attack, the effort would severely impact the reputation loss.

For example, for scenario 1, which previously was 0.0025% · 40, would become 0.001875% ·38 = 0.07125%. This means a reduction of 0.00.02875%, meaning 28.75% of the previous total.

Organization
Creating a system model will lead to a more detailed and up to date overview hopefully reducing the number of outdated firmware versions, thus disabling possible attack paths. The same goes for the configuration management added together we assume will remove 20% of the number of attacks. The awareness training, password policy both prevent an additional 10% reduction in the number of attacks limiting insider attacks and successful phishing attacks. The red team will reduce an additional 10% of the number of attacks on top of the already prevented vulnerabilities. In addition, it helps with the response to the attack as does the logging like mentioned in the ISP section. This should reduce the indirect costs by only about 10%, since we believe that the indirect costs largely depend the fact that this happened rather than the mediation since reputation loss is only a small portion.

Type of reduction	Number of attacks	Indirect costs
ISP	5%	25%
Organization	40%	10%

Computing ROSI

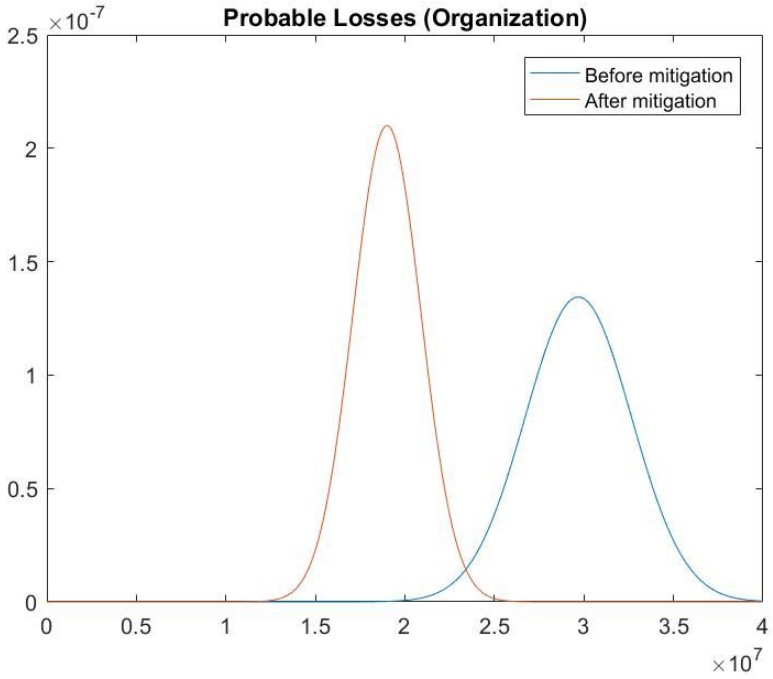
With the values that we have carefully estimated in the previous sections, we can compute the ROSI using the following formula:

$$ROSI = \frac{(Cost\ of\ Loss\ Event * \%Mitigated - Cost\ of\ Solution)}{Cost\ of\ solution}$$

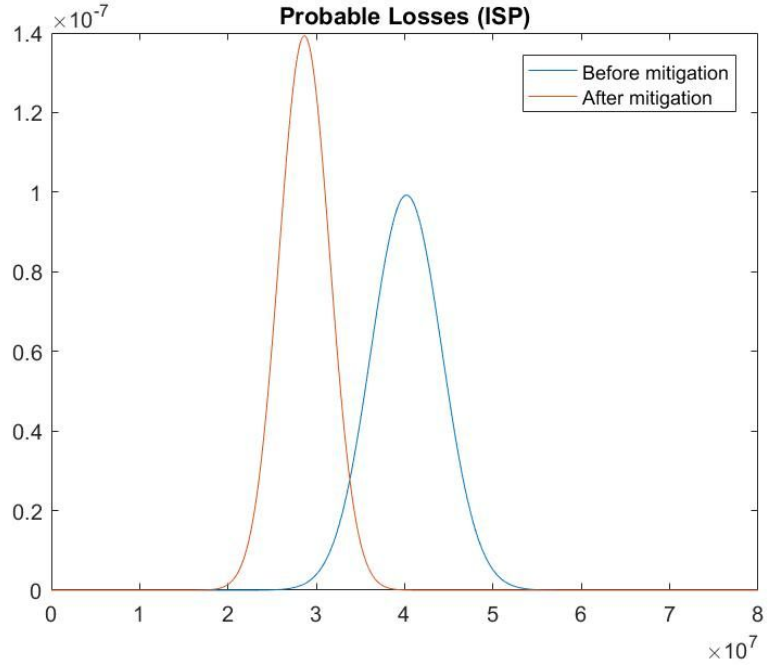
	Cost of loss event	% Mitigated	Cost of solution	ROSI
Organization				
Scenario 1	2,472,332	46%	1,547,539	-26.51%
Scenario 2	9,234,300	46%	1,547,539	174.49%
Scenario 3	29,685,200	46%	1,547,539	782.38%
ISP				
Scenario 1	40,200,000	28.75%	8,667,150	33.35%
Scenario 2	80,400,000	28.75%	8,667,150	166.69%
Scenario 3	120,600,000	28.75%	8,667,150	300.04%

Comparison and reflection

A number of scenarios are considered for both the organization and the ISP. The scenario that is most applicable for the organization is Scenario 3. This is due to the fact that we assume a medium sized organization located in the US, which is on the higher end of technological advancement. The Scenario 3 assumptions of high digital connectivity, hostile threat environment and relatively well educated workforce is appropriate for our case. As we can see from our ROSI computation for this case, the return on investment for the security measures is substantial, especially considering that critical infrastructures provide vital services that can have ripple effects on the whole country if attacked. Below is the graph of probable losses for the organization before and after mitigation. We assume the standard deviation of the losses to be about 10% of the mean losses that we have computed previously. This is because we assume limited variability in the loss due to a large portion of the cost being contingent off an attack happening, not the secondary factors.



For an ISP operating throughout the United States, we assume that scenario 2 is the most applicable. The ISP has customers throughout the country, so in the more remote areas as well as in the highly interconnected parts, like for example near the larger cities. Averaged over all its customers we can expect a medium digital connectivity, leading to scenario 2. The graph of the probabilistic losses for the the ISP is computed similar to the organization and shown below, using the same earlier mentioned assumption of a normal distribution.



The analyses assesses the losses incurred and the cost of mitigation strategies of both the organization and the ISP to analyse where the issue can be resolved best. Security

strategies are best implemented by the ISP as it raises the security of all the organizations it serves and forces its competitors to provide the same or better, apart from the fact that the ISP stands to prevent substantial reputation losses by investing in security, as seen from ROSI. This way the whole environment can be made more secure. But, ISPs are not incentivised to improve their security as the their primary goal is increasing their consumer base, which might be difficult with the inclusion of added costs in their services due to added security. Hence, this has to be handled at the governance level of the cyberspace [NIST, NERC] by implementing laws conducive to security.

For a medium sized organization it is feasible to adopt most of the defined mitigation strategies. Awareness training and the periodic penetration testing is performed by external parties which are becoming widely available. Once the decision is made to adopt these strategies, the burden to deal with this is taken care of. Depending on the current state of the organization's IT infrastructure, the other strategies would be straightforward or more of a challenging task. However, we made our estimations for mapping the infrastructure and implementing logging and configuration management on the conservative side, also taking into account less well-organized IT departments.

As for the ISP, the strategies are viable but their ease of implementation depends on factors like the size of the ISP, which might make it more challenging. However, since an ISP is a highly technical company, adopting a Security Operation Center guarding their infrastructure should be a feasible project, since a lot of knowledge about networking and dealing with large amounts of data is already present in the company. Setting up red teaming as a service is also an obtainable goal. By creating a dedicated department and employing highly skilled people, it can be seen as a separate segment that does not influence the ISPs core business. Although it is feasible to adopt, the effectiveness of a dedicated ICS red teaming does depend on external factors like for example the number of customers interested in ISP red teaming at their location. On the other hand, this is not an issue as the red teaming is an additional service which the ISP does not rely on.
In this analysis for the ISP we have focussed on the worst case in terms of risk, by looking at the risk of reputation loss. The upside potential of the risk, namely the opportunity, is not yet considered. By providing these suggested services an ISP can gain reputation and potentially increase its revenue. This additional boost in sales should, in an ideal world, incentivize the ISPs to use their advantageous position to improve security as a whole and meanwhile improve their bottom line.

Conclusion

The analysis above shows that both the ISP and the organization are able to significantly improve their security by implementing our proposed strategies, under our used assumptions. We believe that the scenario analysis performed allows potential users of this analysis to decide which parameters are most useful to their situation and see the sensitivity of their assumptions at the same time. It gives a detailed overview of the different cost factors both direct and indirect of the mitigation strategy, as well as the effectiveness of the proposed controls. The above insights highlight the importance of security for ICS systems and show that financially, they are feasible as well.

References

Sathik, A. P. M. (2012). *Parallelizing a Network Intrusion Detection System using a GPU*. University of Louisville.

The State of Industrial Cybersecurity 2017
https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Cost of Cyber Crime 2016
https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Shodan ICS, a map and data sets of publicly accessible Industrial Control Systems
https://icsmap.shodan.io/

Problem Owner
https://www.igi-global.com/dictionary/problem-owner/23507

DongIT penetration tests
https://www.dongit.nl/diensten/penetratietesten

Symantec Government Report
https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

Industry standard for sick days
The Industry Standard for Sick Days | Chron.com

Paid vacation days
Paid Vacation Time: How Do You Stack Up? - Gusto

Public holidays USA
https://en.wikipedia.org/wiki/Public_holidays_in_the_United_States

Salary costs
https://www.asme.org/career-education/articles/early-career-engineers/engineering-salary-survey-your-value

Shasta Dam
https://en.wikipedia.org/wiki/Shasta_Dam

Electricity costs
https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html

Internet Usage

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

Internet Backbone
https://www.technologyreview.com/s/540721/first-detailed-public-map-of-us-internet-backbone-could-make-it-stronger/

FAIR
http://www.fairinstitute.org/

Comcast Earnings
http://www.cmcsa.com/earnings.cfm

ICS-CERT
https://ics-cert.us-cert.gov/
The State of Industrial Cybersecurity 2017
https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Cost of Cyber Crime
https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

North American Electric Reliability Corporation (NERC)
http://www.nerc.com/Pages/default.aspx

NIST
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Effects
https://www.youtube.com/watch?v=zBx0hcj9_AU

Weakest Links
Defining "The Weakest Link": Comparative Security in Complex Systems of Systems