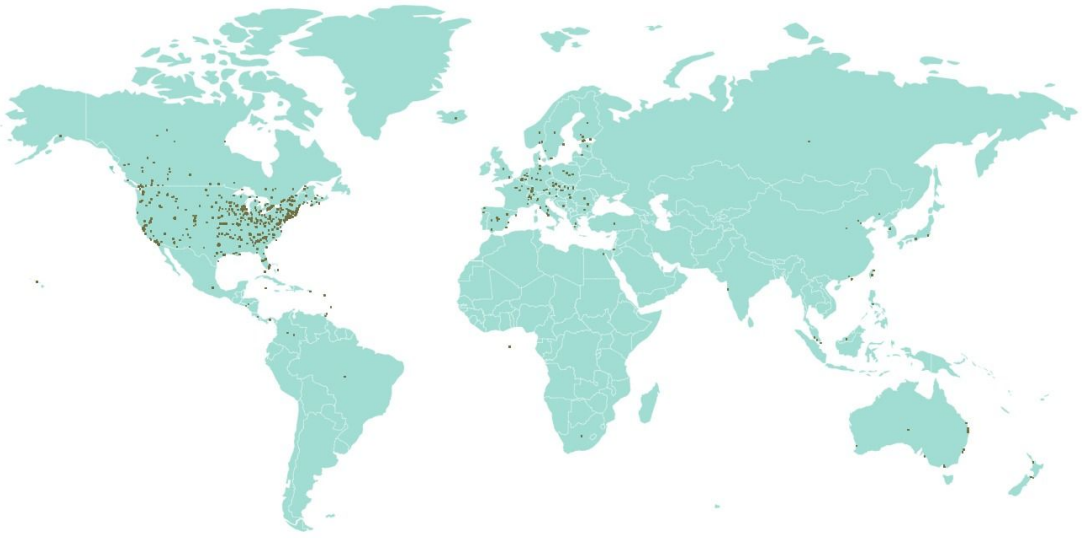
ICS security

Assignment block 4



Summary

During the previous assignments, we have analyzed the variance in security performance in relation to a metric and how different risk strategies can shape this variability. In this assignment, we will focus on the factors that influence this variance. We will do so by taking actors that we have defined in the previous assignment and investigate their incentives for implementing security strategies. We will also look at the consequences that implementing these strategies might have on external parties. In the second part of the assignment, we will assess the security performance of our problem owner.

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.

Actors involved in the security issue

In this section, we will discuss the involvement of three actors in the security issue defined above. In addition, a countermeasure will be defined for which the incentives and disincentives to implement these are analyzed. Because the adoption of a countermeasure generally influences other actors as well, this section will also review the external actors that are influenced by the countermeasure.

Organization

Organizations using Industrial Control systems have a large stake in the problem at hand. The company risks the compromise of one of the devices for which they are responsible. Such an incident could for example lead to a loss in customer confidence, several lawsuits and damaged equipment.

Countermeasure

An important countermeasure an organization can take is adopting a patching policy, to ensure that the firmware of ICS is updated on a regular basis. In older firmware versions usually vulnerabilities are known which gives an adversary means to take over the device. The less time passes after a release of a patch until the firmware update, the smaller the likelihood of an adversary exploiting a known vulnerability.

Cost-Benefit analysis

Costs
Organization

- Better patching policies requires the employment of a new team that maintains the security of these devices or educating the existing workforce on better device maintenance, both of which incurs substantial costs.

Manufacturer

- Having informed and responsive consumers implies that the manufacturers have to be proactive and reactive in learning about vulnerabilities in their devices and coming out with new patches to solve them, which requires them to increase their expenditure on the security of their products and in providing support to their sold devices.

Benefits

Organization

- Improved security of their infrastructure and a team that is informed about the vulnerabilities in their system are the good consequences of having a robust patching process.

Manufacturer

- Well informed and responsive consumers push the manufacturers to improve the security of their devices, while also notifying them of possibly unresolved vulnerabilities.

Underlying incentives and disincentives

Incentives

- With an improved patch policy the number of devices that are compromised reduces, therefore increasing the overall availability of their ICS due to less failing devices. An increase in the organization's continuity increases the revenue of the organization.
- With less compromised devices, the chance of leaking proprietary information to the outside world is reduced.
- In addition, with less compromised devices, less costs are experienced due to deliberately jamming hardware by attackers causing physical damage.

Disincentives

- Implementing and enforcing a patch policy costs an organization time, since an administrator has to oversee the currently installed versions and newly released patches and has to perform the firmware updates.

The role of externalities

Enforcing better patching policies benefits the manufacturers of the device in that lesser of its devices are now perceived as being vulnerable. Poor patching policies might leave several known vulnerabilities unresolved which might cause a less-informed organization to blame the security of their devices. Better patching policies also helps manufacturers learn new vulnerabilities in their latest patches better as poor patching process might not provide accurate data on the success rate of new attacks.

ISP

The ISP that facilitates the connectivity of the critical infrastructure element also has interest in the security issue. The ISP's have access to a lot more information about the packets, their origin and the routing than the organization itself. This makes the ISP an interesting

actor with the ability to analyse attacks on ICS and possibly prevent attacks in the first place. Furthermore, ISPs are indirectly affected by attacks on organizations via their infrastructure. Although attacks on their customer's ICS do not cause direct or immediate damages to the ISPs, consistent successful attacks might lead to distrust amongst consumers about the security of the infrastructure causing damages to the reputation of the ISPs.

Countermeasure

Since an ISP has access to a lot of information about attack traffic, like for example the actual packets, their origin and the routing, they can use this data to analyse attacks and implement filtering of malicious traffic. By implementing mechanisms like traffic egress and ingress filtering, malicious traffic can be filtered out with the goal to defeat attempts of attacking customer ICS. There are proposals and designs for such systems [Abnormal traffic filtering, ISP Filtering]. The downside to this is that according to the law an ISP is not allowed to filter traffic. Even though these regulations are very strict, we propose that the filtering is done in cooperation with the end-client. We also do not propose a system where deep packet inspection is needed, which is illegal to do as third party in both the EU as US. Using this setup, the end-client can choose what will be filtered and data will not be censored without consent. The traffic filtering laws for the ISP might also change in the future with the UK wanting to push a porn site blocking law for certain sites [Porn Blocking]. If some sites will be filtered by law, the filtering rules might be subject to change. If one country implements such measures, other countries will most likely follow as the internet is a cross border medium.

Cost-Benefit analysis

Costs

ISP

- In order to properly filter egress and ingress traffic, expensive hardware will need to be acquired.
- Analysis and maintenance of the filtering devices will also increase overall expenses. These costs will be caused by declined productivity and maintaining a specialized workforce for this purpose.
- Finally, there will be costs associated with false positives caused by the filtering algorithm.This might be in the form of compensation for their consumers or in terms of justifying the issues for the sake of security.

Organization

- Losses in productivity due to the blocking of legitimate access to its devices from a remote location.

Benefits

ISP

- Better understanding and control of the traffic passing through its infrastructure.
- Collection of metadata of their consumers which can then be used to better their services.

Organization

- Reduced illegitimate access to their devices remotely, thereby improving the security of the organization.

Underlying incentives and disincentives

Incentives

- 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 [Network Effects].
- The introduction of a traffic egress filtering allows the ISP to detect illicit traffic and warn their clients on possible attacks. This improves the ISP's reputation as a security aware Internet Service Provider.
- The introduction of traffic egress filtering forms an additional Unique Selling Point towards possible customers, convincing them to take the ISPs services.

Disincentives

- Adopting a traffic egress filtering mechanism induces a cost on the ISP for setting up and maintaining the additional infrastructure.
- A imperfect filtering mechanism raises too much false positives, resulting in false warnings to customers of the ISP. This will result in loss of reputation.
- In order to implement a filtering mechanism, the ISP has to know which data can be deemed as 'normal'. This could differ between customers, so this would mean a lot of work that has to be done in order to fully implement this.
- The law prohibits filtering traffic on ISP level. We think that this can be circumvented with consent of the company, but if there is a loophole in the agreement between company and ISP, a company could sue the ISP for filtering traffic. Therefore creating these agreements is very hard and also riskful, and require constant monitoring of the law.

The role of externalities

If the ISP implements traffic filtering, the organizations that use the ISP lose total control over the data. During the cyber security integration week, we have talked to the ING, who use a mitigation partner in order to mitigate DDoS attacks on their servers. This mitigation partner is not at ISP level, but offers enterprise traffic filtering. ING stated that they were not always in mitigation, only when they needed to. They do this because they want to keep an overview of the total traffic that comes in and out of their company. Mitigating part of the traffic at a mitigation partner or ISP will result in less data showing up at the organization. The data that is not showing up in their logs might be attack data that they want to have so they can see if they are being targeted or not. The ISP has no knowledge over which data the organization might deem useful, and therefore there will be an information gap.

Manufacturer

The manufacturer plays a critical role in ICS security. The manufacturer might not have control over the traffic flows, but it is the only actor that has control over the design and

software of the ICS device. The design plays a critical role in the overall security of the device [Device Security].

Countermeasure

The countermeasure that the manufacturer can take is implementing security by design [Device Security]. Currently, the default settings on for example ModBus is to not have authentication. This is great from an availability standpoint, but is considered to be insecure. In order to implement security by design, there are three core elements that the manufacturer has to take into account. These pillars are:

1. Confidentiality
2. Integrity
3. Availability

The device should be designed with these pillars in mind. This means that a security architecture should be devised by the manufacturer.
By introducing authentication for example, unauthorized remote access to these equipments would be greatly reduced and thereby mitigating the security issue.

Cost-Benefit analysis

Costs

Manufacturer

- The countermeasure that is suggested for the manufacturers requires implementation of design changes that would incur costs in modifying the manufacturing process of these devices.
- An analysis on the new security vulnerabilities introduced by the changes is required which also costs the manufacturers.
- This modification must also be communicated with its consumers which requires higher expenditure on sales and marketing to ensure that the consumers are aware of the improved benefits due to this countermeasure and that the added costs due to it are justified.

Organization

- Productivity loss due to improved authentication process.
- Training costs to get used to the new design.

Benefits

Organization

- Reduces the likelihood of a malicious adversary being able to access and control their devices remotely.

Underlying incentives and disincentives

Incentives

- The reputation of the manufacturer as creator of secure devices improves, which in turn could lead to increased demand for its products.
- The number of devices that are compromised reduces, therefore the number of complaints and customer service cases decreases alongside. This variable cost of product manufacturing is reduced resulting in higher margins.

Disincentives

- The devices will lose their plug-and-play nature, because they will be shipped with all security enabled. This can lead to worse customer experience, which is a large part of the value proposition that an organization offers [Understanding Customer Experience]. Depending on the size of this part, competitors might be perceived better. Furthermore, in order to aid in the installation increased customer service and training material will be needed causing additional costs.

The role of externalities

Multiple externalities can be defined. As first externality, we define the organization that buys and uses the device. Because of the more secure architecture, the organization does not know what is happening inside the device. The most prevalent ICS device manufacturers are hesitant to provide their customers this information [Siemens Modbus]. This means that the organization loses some control over the device.
This additional security implementation might require substantial changes in the protocol implemented by the organizations to use these devices. This could incur one-time losses for the organizations to modify their systems and also risks recurrent productivity losses. These is also the possibility that some organizations might altogether bypass this feature by using a workaround to improve their efficiency and eventually making the system less secure than without the authentication.
The ISP servicing the organization's infrastructure would benefit from the organization procuring the more secure products as attacks carried out using their infrastructures reduce or at least become less successful. But, there is also the possibility that the ISP might reduce its expenditure on security due to the perception of a reduced threat environment.

Reflection

From this section we can conclude that there is not a one size fits all solution. All parties involved have their own incentives and disincentives to offer security, which also affects other parties. Therefore, it is hard to determine where the security layer should be added. Due to this, ISP’s generally do not offer traffic filtering while there are people that argue that the ISP should do traffic filtering [ISP Filtering]. Manufacturers could also offer products with a higher security standard, but they are still seem reluctant to do so. This might change in the future when a cybersecurity mentality becomes more prevalent and organizations will prefer to buy devices that have a higher security. The organization itself will have to evaluate which components of their system model are secure and which need to be modified or replaced. The decision on which controls to strengthen can be done by using a cost benefit analysis. There might be devices which are expensive to secure, but do not have high value for attackers. If such a device exists, these will not have a high priority for organizations to secure and invest resources into them.

Security Performance of the Organization

The organization is chosen to be the actor under analysis, because it is directly linked to the vulnerabilities as well as the number of accessible devices present. In addition, it has been the main stakeholder for our analysis done in the previous assignments and seems to have both the largest interest, and influence on the security issue defined.

Explaining metric variance

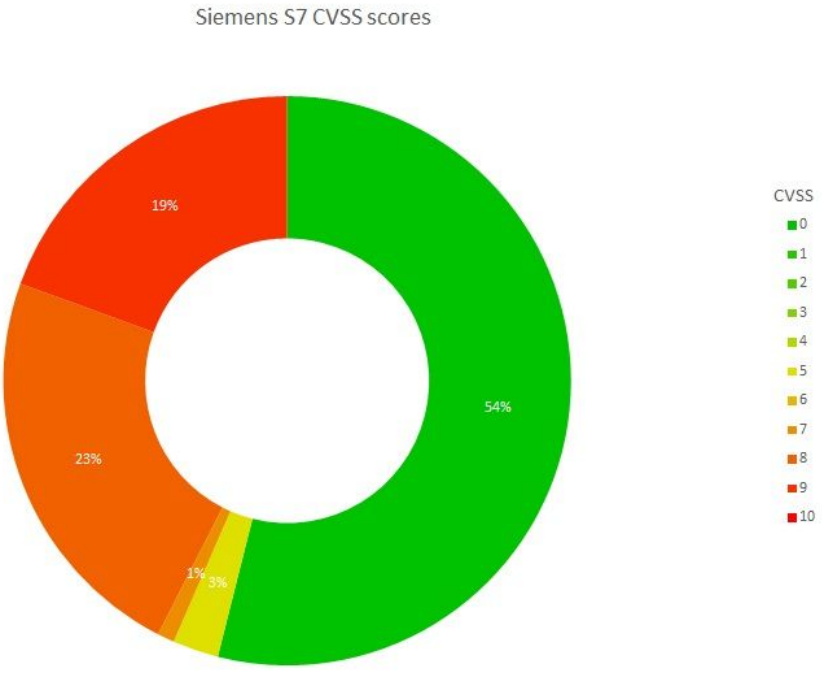
In this section, the different values in the metrics will be discussed and possible reasons will be assessed. This will be done for the number of firmware vulnerabilities and the number of accessible devices per organization.

Number of firmware vulnerabilities

As described in the first assignments, 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 the highest CVSS score for each of the systems is shown. Aggregating the number of occurrences of the maximum CVSS scores of all systems gives an overview of how many systems are at the different levels 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). Do note that in the calculations, 676 devices were ignored as they did not contain any version information and could not reliably be used. 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.

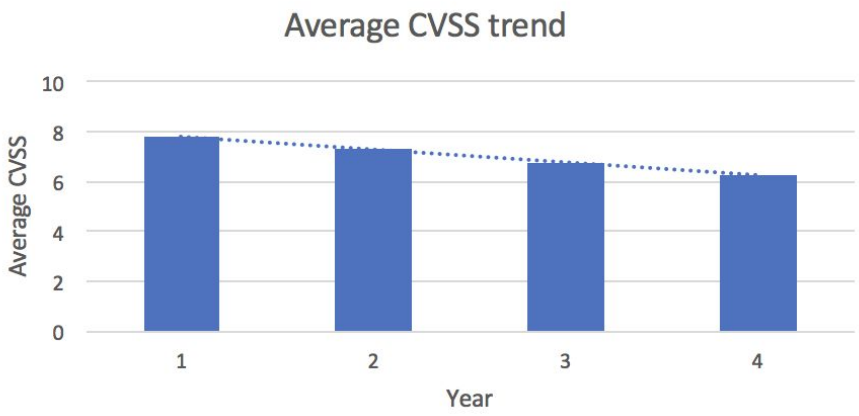
The highest CVSS scored vulnerability of a system will change when security improvements are made. This clear distinction in the metric value allows for validation of the effectiveness of the security measure. When fewer vulnerabilities are present or less severe ones, it is clear that the security situation has indeed improved. Companies that are now in category 9, can then hopefully join their competitors that are currently given a score of 0-3.



The variance in the scores as shown in the diagram is caused by the range of firmware versions that are currently installed throughout all publicly accessible devices. The more insecure firmware versions result in a higher CVSS score than the more recent, secure releases.

The actual scores itself depend on several factors as described in [CVSS Scoring]. The first group of factors is called the base metric group, that computes a score based on both exploitability metrics and impact metrics. The second group are the temporal factors that look at code maturity, report confidence and remediation levels. Finally, the environmental group takes into account the different requirements of the system.

This means that an ICS that runs firmware containing vulnerabilities with a score of 8, will most likely be easier accessible, have a larger impact and a low attack complexity when compared to an ICS that receives a score of 5, which will most probably be harder to compromise. All these different factors cause the variance in this security metric.

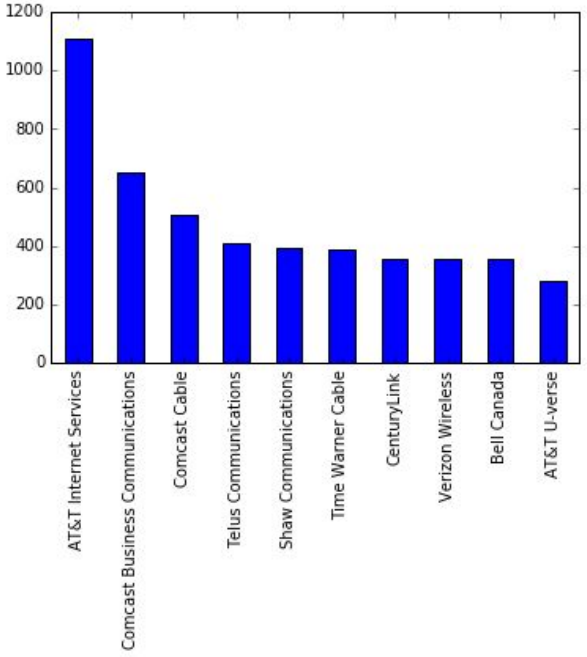


As can be seen in the figure above, the average CVSS score in the above mentioned dataset seems to decline by the year. This means that most probably the software security improves over time causing less critical vulnerabilities to be detected. Therefore, the vulnerabilities present in earlier versions are more intense and thus the reasoning for the variance can be caused by the use of earlier versions. Furthermore, it could be the case that a higher investment in equipment by a company, i.e. premium versions of equipment and more frequent upgrading, will yield lower CVSS scores in their systems. This will be further explored in the next sections.

Number of accessible devices per organization

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

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 number of accessible devices by the amount of physical assets, 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 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

The differences in these ratios can be caused by several different factors. The amount of investments in the recent years leading up to the accessibility incident. The higher amount of investments in terms of PPE (due to higher costs), personnel expenses, and R&D could indicate a cyber security aware path chosen within the organization.

External data on variance

Number of firmware vulnerabilities

In this section, different factors will be analyzed in order to investigate which factors could have a correlation with the CVSS metric. Since identifying the CVSS status of a system based on firmware versions is a very tedious task, in our previous analysis we only focused on the data of Siemens S7 devices. We will therefore continue our investigation on Siemens data and only consider external factors with regards to Siemens S7 systems. The Siemens S7 Shodan dataset lists data for the year 2014, so we will perform our analysis on factors up to 2014.

To inform customers on current security issues, Siemens has employed a team of specialists for responding to potential security incidents and vulnerabilities related to Siemens products. On the Siemens website [ProductCERT] a list of all vulnerabilities can be found, with the affected products and the steps for patching the vulnerability. Siemens also keeps a library of all product notes [SiemensNotes] and releases [SiemensReleases] from the previous years. It would be interesting to see how various Siemens systems compare at different points in time in terms of the number of active vulnerabilities. There could be a link between the number of product notes or patch releases and the most severe vulnerability still present in a system. The reasoning behind this possible relation is that vulnerabilities are patched and warned for by the vendor after they are discovered. In a security aware organization, vulnerabilities are patched soon after discovery, thus reducing the CVSS score of a system. The variance in the CVSS scores could therefore be related to the moments new

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

vulnerabilities are discovered, or are mentioned throughout product notes. Since we have analysed the CVSS scores in Siemens systems for the year 2014, we will try to explore this possible relation for data on the year 2014.
The following table displays all vulnerabilities that are discovered in 2014 aggregated per month. It also displays the number of product notes and the number of firmware updates released by Siemens.

Month	#vulnerabilities	CVSS sum	CVSS average	CVSS max	#notes	#releases
2014-12-01	0	0	0.00	0	4	1
2014-11-01	3	18.1	6.03	8.3	3	2
2014-10-01	3	23	7.67	8.7	2	2
2014-09-01	0	0	0.00	0	5	2
2014-08-01	1	5.6	5.60	5.6	7	12
2014-07-01	6	36.2	6.03	5.3	3	5
2014-06-01	0	0	0.00	0	7	7
2014-05-01	1	4.5	4.50	4.5	7	14
2014-04-01	7	31.1	4.44	7.3	6	6
2014-03-01	16	83.6	5.23	6.5	8	2
2014-02-01	5	23	4.60	7.3	3	3
2014-01-01	0	0	0.00	0	7	0

The following table shows how the CVSS distributions of the publicly accessible Siemens S7 devices varies for the months February till October of the year 2014. Since there were no vulnerabilities with score 1 - 4 or 10 we left these columns out the table. In order to convert the vulnerability distribution to a number that could be correlated with the previously mentioned factors, we computed a severity score in the form of a weighted average of the number of vulnerabilities, using the CVSS scores as weights. This is however biased, since months in which more devices are discovered would now automatically receive a higher score. Therefore, the weighted averages are normalized over the number of discovered accessible devices, resulting in an average severity score per device for each month.

Month	CVSS 5	CVSS 6	CVSS 7	CVSS 8	CVSS 9	# discovered devices	Severity score per device
2014-10-01	13	5	6	112	124	599	3.59
2014-09-01	4	4	2	52	63	307	3.39

2014-08-01	7	9	5	92	79	447	3.51
2014-07-01	14	4	5	156	153	876	3.14
2014-06-01	3	1	5	77	43	386	2.74
2014-05-01	26	31	4	178	112	834	3.33
2014-04-01	0	0	0	0	0	0	-
2014-03-01	2	3	0	19	8	59	4.27
2014-02-01	28	5	9	168	140	878	3.23

Another factor that could explain the variance in the CVSS metric is the difference in PPE investment of the different companies using Siemens S7 systems. A larger PPE investment could be the result of a company buying more premium versions of equipment and more frequent upgrading. We therefore consider the possibility that, in general, larger PPE investments means a more security aware company and therefore less vulnerable devices.
To investigate this possible relation, we performed an additional analysis on the Siemens S7 dataset. For this analysis, the data is aggregated per organization and for each organization both the the number of publicly accessible device, and the distribution of CVSS scores are recorded. It is however difficult to get a precise estimate of a distribution with a limited sample size.. Luckily the dataset follows a power law, containing a group of organizations with a substantial amount of publicly accessible devices. Since the observed distribution is closer to the actual distribution for these organization with more publicly accessible devices, it was hypothesized that we could more precisely verify the relation by ordering the organizations with a descending number of accessible devices. To minimize bias of selecting very similar organizations, the top 30 organizations have been investigated and a subset of 10 organizations having the most variance in, among others, the origin and PPE value have been selected.
The following table shows the results of the analysis on the Siemens S7 devices for the selected organizations. As mentioned before, the columns corresponding to vulnerabilities with score 1 - 4 or 10 are omitted from the table. In order to convert the vulnerability distribution to a number that could be correlated with the PPE investments, the severity score is computed as a weighted average of the number of vulnerabilities and the CVSS scores. To prevent the resulting metric from being biased to organizations that possess more devices, the weighted average is normalized by the number of accessible devices. Finally, the final average severity score per device for each of the organizations can be used in further analysis.

Organization	**CVSS 5**	**CVSS 6**	**CVSS 7**	**CVSS 8**	**CVSS 9**	**# public devices**	**Severity score per device**
Deutsche Telekom AG	10	0	5	166	86	415	5.27

Telecom Italia	6	0	0	58	26	212	3.43
Telefonica de Espana	3	0	0	43	17	179	2.86
TeliaSonera AB	0	5	2	4	10	121	1.37
Verizon Wireless	0	0	10	2	9	96	1.74
Telekom Austria	3	0	1	25	14	90	3.87
Turkcell	0	7	8	5	1	77	1.91
Swisscom	0	0	0	33	8	76	4.42
Turk Telekom	0	0	0	8	28	57	5.54
AT&T	0	0	2	5	0	34	1.59

For each of the selected organizations, the PPE investments are retrieved from the annual reports from 2011 to 2014. The averages over these years will be used to correlate against the organization's severity score, as defined earlier. By using the average over a number of years, the effects of expenditure outliers is reduced. Since security is dependent on consistent spending rather than being instantaneously responsive to investments, a multiple year view gives a more meaningful overview. The amounts shown in the table are denoted in millions of US dollars.

Organization	**2011**	**2012**	**2013**	**2014**	**average**
Deutsche Telekom AG	41797	37407	37427	39616	39062
Telecom Italia	14899	14465	12299	12544	13552
Telefonica de Espana	44501	35021	31040	33343	35976
TeliaSonera AB	61292	62657	64792	69669	64603
Verizon Wireless	88434	88642	88956	89947	88995
Telekom Austria	2462	2426	2308	2246	2361
Turkcell	2709	3061	2748	2542	2765
Swisscom	8222	8549	9156	9720	8912
Turk Telekom	2151	2265	2267	2228	2228

AT&T	107090	109767	110968	112898	110181

This section considered possible factors that could be related to the variance in the CVSS metric. In the next section we will perform a statistical analysis on these factors in order to confirm or dismiss possible relations between them. But first we will continue the investigation of influencing factors by reviewing the number of accessible devices metric.

Number of accessible devices per organization

In this section, different possible correlated factors will be analyzed checking if the factors mentioned above differ between the organizations. These will later be used to statistically check if there is in fact a significant relationship between these values and the security metric.

The reasoning behind the chosen factors in the tables below is explained next. It is assumed that the PPE influences the number of devices since a higher amount invested in these long-term assets would most likely result in a higher number of devices within the organization, or higher quality devices. Ideally, a lower PPE increase over the last years would correlate to higher number of accessible devices. Personnel expenses could indicate a more dedicated workforce that is less spread out, resulting in lower focus. Therefore, we assume that a higher increase in personnel expenses is linked to fewer connected devices. Furthermore, the non-current assets of the firm could include other investments than hardware that might indicate a more intrinsic interest in the long-term health of the organization rather than short term profit leading to fewer available devices. Finally, the operating cost include external hires and consultancy companies that might be used in terms of cyber security. Since there is no more detailed data available, a correlation between these two will be sought.

Tellus	**2014**	**2013**	**2012**	**2011**	**Average**
PPE investments (in millions)	$1,621	$1,612	$1,472	$1,343	$1,512
Personnel expenses (in millions)	$2,424	$2,743	$2,474	$2,258	$2,474.75
Non-current assets	$794	$1,002	$355	$53	$2204
Operating cost (in	$2,400	$2,212	$2,107	$1,965	$19,646

millions)					

Shaw	**2014**	**2013**	**2012**	**2011**	**Average**
PPE investments (in millions)	$782	$642	$585	$564	$643.25
Personnel expenses (in millions)	$757	$721	$669	$601	$687
Non-current assets	$518	$10	$184	$2274	$746.5
Operating cost	$791,52	$765,688	$705,94	$736,88	$573.522

Century Link	**2014**	**2013**	**2012**	**2011**	**Average**
PPE investments	$3,047	$3,048	$2,919	$2,411	$2,856.25
Personnel expenses	$641	$628	$608	$587	$616
Non-current assets	$-19	$-7	$3	$-2	$-6.25
Operating cost	$17,437	$16,642	$15,663	$13,326	$15,767

Bell Canada	**2014**	**2013**	**2012**	**2011**	**Average**
PPE investments	$3,103	$2,014	$2,529	$2,642	$2,572
Personnel expenses	$3,485	$3,410	$3,304	$3,233	$3,358
Non-current assets	$257	$61	$8	$-10	$79
Operating cost	$10,202	$9,859	$9,682	$9,605	$9,837

Analyzing the underlying factors

In this section, relevant statistical tests will show whether or not the explanation of the variance does indeed makes sense. In order to do this, both a Pearson R and a linear

regression test will be done. The first checks whether there exists a relationship between the different variables and the metric value and whether this is significant or not. The latter will return us the R-squared value that show how much variance of the metric value is in fact explained by the given explanation.

Number of accessible devices per organization

As mentioned previously, the differences in the ratio (of the no. of accessible devices and the amount of physical devices) can be explained by the financial expenses of the company in different assets. This can be statistically tested by checking for correlation between the ratio data from our dataset to the financial external data. The financial data values are averages over the years 2011-2014 as using individual yearly data can be misleading. Averaging does not capture the expenditure trend of the organizations, but averaging over a number of years reduces the effects of outlying expenditures as security is dependent on consistent spending rather than being instantaneously responsive to investments.

The values of the Pearson R correlation tests are given below:

	Financial Data (Averaged)			
	PPE Investments	Personnel Expenses	Non-Current Assets	Operating Costs
r-value	-0.9478	-0.3895	0.8960	-0.8035
p-value	0.0522	0.6105	0.1040	0.1965

To give a short introduction to interpret the results of the test, the r-value of the result ranges between -1 and 1 indicating strong negative and positive correlation respectively. Values around 0 implies lack of substantial correlation between the 2 trends. The p-value captures the likelihood of there not being a correlation inspite of having very high or very low r-values.

The test indicates a very strong negative correlation between our data on the normalized accessible devices and PPE investments by the organization, with a very low likelihood of there not being significant correlation. There is also a strong positive correlation with Non-Current Assets but with a relatively higher likelihood that this correlation is not significant.

We can also verify the above results using regression analysis. The regression test can be performed by using least-squared fitting of the ratio values computed using our dataset using the financial data and calculating how much of the variance in the ratio values can be explained by the values obtained from the financial data. The r^2 values of the financial data is shown below:

	Financial Data (Averaged)

	PPE Investments	Personnel Expenses	Non-Current Assets	Operating Costs
r^2 value	0.8984	0.1517	0.8029	0.6456

The r^2 values range between 0 and 1. Higher the value implies better linear relation between the target variable (ratio of no. of accessible devices and amount of physical devices) and the explanatory variable (financial data). This confirms the results from the previous test, there is a strong linear relationship between our data and PPE Investments and Non-Current Assets.

Number of firmware vulnerabilities

We previously considered possible factors that could be related to the variance in the CVSS metric. In this section we will perform a statistical analysis on these factors in order to confirm or dismiss possible relations between them.
Our first approach in explaining the metric variance was looking into the temporal differences in CVSS value. This might be linked to the number of discovered vulnerabilities, released software updates or the number of product notes. The following table shows the results of the Pearson R correlation test, as explained in the previous section.

	Factors correlated to temporal variance		
	Discovered vulnerabilities	Number of published product notes	Number of software releases
r-value	0.7397	0.2340	-0.2732
p-value	0.0359	0.5770	0.5126

The test indicates a significant positive correlation between our data on the CVSS severity scores for each month and the number of discovered vulnerabilities, with a very low likelihood of this being incorrect. The other two factors have only a small correlation with the CVSS severity. Furthermore, there is inconclusive evidence about the significance of the association between the variables due to the very large p-values. Therefore, only the first factor can be considered an actual correlation.
The second approach was to look into differences between organizations. The factor that could explain the CVSS metric variance, is the average PPE investment of the organizations that own Siemens S7 systems. The following table lists the used PPE investment values.

Organization	**Average PPE Investment** [in millions of USD]
Deutsche Telekom AG	39062
Telecom Italia	13552

Telefonica de Espana	35976
TeliaSonera AB	64603
Verizon Wireless	88995
Telekom Austria	2361
Turkcell	2765
Swisscom	8912
Turk Telekom	2228
AT&T	110181

Based on the above listed PPE investment values and severity score for each organization another Pearson R correlation test is performed.

	Correlation to variance between organizations
	PPE investments
r-value	-0.6233
p-value	0.0541

The test indicates a negative correlation between the severity score and the PPE investments. The r-value is not as strong as the correlation between the PPE investments and the number of accessible devices, but it is still a fairly high correlation. Also the p-value is quite small indicating a large likelihood of the correlation being correct.

Next, we performed a regression analysis to verify the above findings using the same approach as in the analysis performed in the previous section. The r^2 values of all four factors are the following:

	Discovered vulnerabilities	Number of published product notes	Number of software releases	PPE Investments
r^2 value	0.5472	0.0547	0.0747	0.3886

The regression confirms that there is no correlation between the CVSS metric variance with neither the number of product notes nor the number of software releases. The other r squared values are not very high, but still show a plausible correlation in the discovered vulnerabilities and the PPE investment factors.

Reflection

The strong correlation between our data on the no. of accessible devices per organization and the financial investment data of the organization shows that the investment and expenditure of the organization has a strong influence on security of organizations in our scenario, which is nicely captured in our metrics. This is understandable as better investments by the organization on its devices could imply a higher budget for security and hence improved performance in our metrics. In addition, the acquisition of higher-end equipment and higher frequency upgrades are more likely as well. Since the tests are done with only a limited number of companies due to the shortage of available data, the results need to be taken as a guideline for future research and not be accepted as an absolute truth.

The correlation test, aiming to explain the variance in the CVSS metric, shows a significant positive correlation between our data on the CVSS severity scores for each month, and the number of discovered vulnerabilities. Furthermore, it can be concluded that it is plausible that a larger PPE investment means the organization invests in more premium versions of equipment or more frequent upgrading. According to the correlation test it seems that larger PPE investments, indicates a more security aware company and therefore less vulnerable devices.

Conclusion

Initially, three actors have been identified, the organizations, the ISP and the manufacturer of ICS equipment. Each of these actors got assigned a possible countermeasure. For each of these countermeasures, different factors have been analyzed. In order to explore whether this countermeasure is feasible, the costs and benefits of implementing the countermeasure, as well as the incentives and disincentives play a role. It became apparent that countermeasures also impact other actors than just the primary implementer, and these externalities have also been analyzed.
In the second part of this assignment this assignment, explanatory analysis on the variance in security performance between organizations has been conducted for two different metrics that attempt to quantify the security of an organization. Both the number of accessible devices per organization, as well as the number of software vulnerabilities in ICS devices showed correlation with several different financial values collected from secondary sources. The significance of some of these correlations show that the metrics proposed might indeed help to assess the security of ICS devices in practice, and make security the industry standard.

References

Design security
https://www.owasp.org/index.php/Security_by_Design_Principles#Core_pillars_of_information_security

Understanding customer experience
https://hbr.org/2007/02/understanding-customer-experience

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

CVSS Scoring
https://www.first.org/cvss/specification-document

ISP Filtering
https://www.out-law.com/page-11869on

ProductCERT
https://www.siemens.com/cert/en/cert-security-advisories.htm

Siemens Product Notes
https://support.industry.siemens.com/cs/products?ps=100&dFrom=20140101&dTo=20141231&dtp=ProductNote&mfn=ps&pnid=13615&lc=en-WW

Siemens Releases
https://support.industry.siemens.com/cs/products?ps=100&dFrom=20140101&dTo=20141231&dtp=Download&mfn=ps&pnid=13615&lc=en-WW

Siemens Modbus
https://w3.siemens.com/mcms/topics/en/siplus/ric-telecontrol/Documents/ric-docu/modbus-tcp_funktionsbeschreibung_en.pdf

Abnormal traffic filtering
Kim, Byoung-Koo & Kang, Dong-Ho & Na, Jung-Chan & Chung, Tai-Myoung. (2016). Abnormal traffic filtering mechanism for protecting ICS networks. 1-1. 10.1109/ICACT.2016.7423421.

Porn blocking
http://www.telegraph.co.uk/technology/2017/01/26/porn-blocking-legislation-cement-internet-filtering-uk-law/

ISP Filtering
Subbaraman, R. J Netw Syst Manage (2017). https://doi.org/10.1007/s10922-017-9424-1