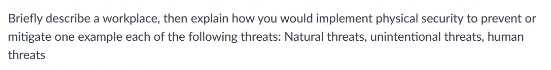


The first law of operation security is: “If you don’t know the threat, how do you know what to protect.” A real-world example of this would be a college institution that hosts its own web servers to hold all student data, and to provide utility for the campus. Threats may come from a digital form, in which attackers use things such as DDOS to disrupt the campus operations, which is something the organization may plan for. However, threats may come in the physical form, that being a student or disgruntled employee gaining physical access to them with the intention of exfiltrating data or vandalization of property to disrupt service. This law can be followed by the college if they consider each utility, set of data, and how valuable they may be to an attacker. That way proper safeguards could be built for both the physical security and the digital security aspect of their operations. If the law is not followed, it could result in the disruption of college services and the leaked information of students and employees. Such an incident would severely damage any college or university's reputation.

The second law of operation security states: “If you don’t know what to protect, how do you know you are protecting it?”. A real-world example of this would be an online shopping merchant such as Amazon that interacts digitally with tens of millions of customers each day. To follow this law, Amazon could analyze the information they store about their customers, such as purchases, credit card numbers, phone numbers, names, addresses, and security questions to label their data sensitivity. After this, they could take the approach of segregating the more sensitive data into different networks to prevent an attacker stealing vital information from all datasets. If the law is not followed, Amazon could come to a situation where an attacker is able to infiltrate their servers and steal a giant pool of customer personable identifiable information. This complete pool of data would fetch a higher price on the dark web because it would be easier to perform a social engineering attack against someone in the leak.

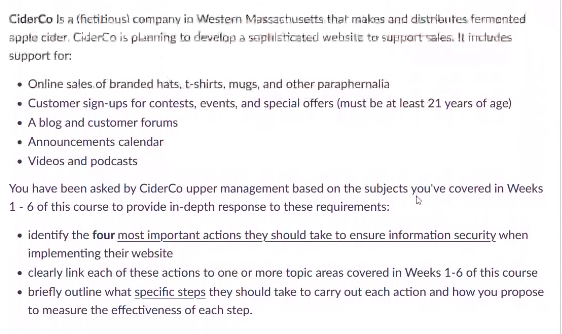
Lastly, the third law states “If you are not protecting it (the information) …THE DRAGON WINS!”. I see this law as implying that if you are not even thinking about the process of protecting your critical information and data, then why are you even storing it? An example would be a healthcare organization. The information stored is critical data, so if they are not going to bother protecting it, why even be in the business of healthcare? The law could be followed by complying to government laws, such as HIPAA, which require a strict handling of customer data. If not followed it would lead to potential fines and a possible shut down of the health care company as whole.



The workplace I am describing is a nuclear facility that provides power to small city in the United States, and employees around 100 scientists and technicians. For a natural threat such as a tsunami or earthquake, an implementation of physical security would be to ensure that the reactors are able to be shutdown in a safe way to protect against nuclear meltdown. This would include having robots in the facility as staff in the case that humans would need to evacuate in an emergency. As we saw in the Fukushima disaster in Japan, it took weeks to get robots into the damaged facility to shut down the reactor. Which is why I would recommend them be a part of operational staff from the onset of the reactor going live as protection, and to mitigate any risk of radiation for humans.

An unintentional threat could be an employee who was previously let go from the company but is disgruntled with how the situation left and plans to modify computer code to make the reactor inefficient, with the hopes of getting the plant decommissioned. A physical security protection would be to have security staff at all entrances, and all access points to critical computer systems. In the case of early termination, no employee should be allowed back onto the site without direct order from a supervisor. Insider threats come unexpected because it can be hard to companies to even realize that the person they let go was disgruntled. Having proper physical security staff on facility campus would help deter any malicious actions.

A human threat could be the possibility terrorists who see a nuclear facility as being a way to cause fear and pain for a country. Since the first goal of physical security at an organization is to keep people safe, I would recommend national guard be stationed at the perimeter of the site. Having those with arms training stationed on site would deter and help prevent any physical attack on the campus. Especially the in the case of a nuclear facility, this is the control of something you would not want to fall into the wrong hands so whatever the cost would be for military staff must be considered.



For a company looking to expand its brand and develop a sophisticated online website such as the one listed, I think the most important action would be to use cryptography like we learned in chapter 5 to secure all connections that a customer may have with the company’s website. For instance, CiderCo wants to conduct online sales, which means the processing of personal identifiable information such as credit card information. Most websites today are served over HTTPS using the SSL which protect against eavesdroppers looking to scrap network traffic for unencrypted communications. Another layer to of this to institute is the use of the Transport Layer Security (TLS) which would handle the security of the credit card processing. TLS 1.2 was created recently with this very idea in mind and helps keep a merchants’ transactions secure and confidential. Without implementing TLS or SSL, it is pointless to even have online commerce as part of the website, because without them, the company faces severe risk of a breach in data confidentiality. A way to measure the effectiveness of this action would be to monitor the website for any potential data leaks to their customers data. If customers or employees do not raise issues about their accounts or credit card information being compromised, then the policies are working.

Since CiderCo wants customers to sign up for contests and events, as well as assure that they are over 21 years of age, it means they will have to store driver license information for validation. This means that cryptography would also be used to protect data at rest. However, another action needed for this is the ability to identify and authenticate verified users. Building on the lessons learned from chapter 2, CiderCo needs to ensure that all company and customer accounts are required to have multifactor authentication when completing account registration. Requiring multi-factor authentication raises the bar for any potential attack on an account who is registered to CiderCo’s website. While we can never stop every attack, we must continue to do our best to use defense in depth by providing as many layers of defense as possible to deter attackers from even trying. I way to measure the effectiveness of this is to monitor how many customers report that their account was compromised. However, it would also be important to see how many customers did not sign up because of the barrier to entry that MFA can cause. CiderCo could measure the effectiveness of this policy by looking at their user data and seeing how many times on average they are asking to reset their password but do not comply with the other factors. This would give a direct correlation to show how the MFA process stopped attackers, but there could be signals in the data that show customers have a challenging time with MFA as well.

The third action that should put in place is access control, seeing that CiderCo wants to have a blog and customer forums where the company and users can post content. Using the principle of least privilege discussed in chapter 3, users’ roles should be isolated to just allowing basic content posts on the website. However, administrators, forum moderators, and employees would also like to use the site and will have a different level of access. It is important here to use a role-based access control to better group the policies and restrictions that each would have. This could be implemented by an access control list which would allow the company to monitor what data a user is changing and modifying on the servers file system. To measure the effectiveness of this action, CiderCo can monitor how many times a user was able to elevate their access on the forum to something other than least privileged.

The last action I would recommend would be enact polices to deal with the confused deputy problem of client-side attacks, such as cross site request forgery and clickjacking. Confused deputy problems are attacks that go after the access control lists of companies, normally looking for software that has a higher level of access than the user that controls it. In the case of CiderCo and their website, while an access control list is suitable for a simple user forum, it would be wise to implement a capability-based system discussed in chapter 3 for the company employees who wish to update the website to post videos and podcasts. This way, when the website is updated, only one person who has the capability at the time can modify the websites content. This reduces the risk of an attacker leveraging the ACL from their user forum to perform a CSFR or clickjack using an invisible iFrames. The steps to implement this would be to generate a one-time access token for any time an employee who wishes to update the website. He/she would be the only one able to modify the website so long as their token is active. Once their task is completed, their token becomes inactive and unsuitable for future use, deterring any attackers goal of confiscating it. The way to measure the performance of this action would be to monitor the use of the one-time access token and see if it is being used as intended. If it is found that there have been no cases of CSRF or click-jacking since being implemented, then the company can feel confident in their decision go with the capability-based control for employees updating content on the website.