The Security Mirage

**Part 1:** Choose one of these topics (or another that you identified while viewing the video) and respond in depth to one of the following instructions:

* Explain why you disagree with Mr. Schneier,
* Explain why you agree with him,
* Describe a situation you know of that relates to his presentation, or
* Describe why his perspective is surprising to you

Triangle = Feelings + Reality + Models

I agree completely with Mr. Schneier when he talks about thinking of security in terms of being a tradeoff. What comes to mind for me when thinking about this is the tradeoff cryptography algorithm designers must make when it comes to protecting information confidentiality. Theoretically we could have perfect security in the digital world, and every message sent would be unbreakable, but it would not be practical. It would lead to horrendously slow encryption/decryption because the key space would have the match the message size. This would lead to an enormous waste of bandwidth, and much slower applications and digital communications in general.

That is why when designing cryptography algorithms, instead of going for perfect security, they produced the idea of computational security. Meaning there is a minimum amount of work that is required to crack the algorithm, but the time it takes to do that work could exceed many human lifetimes, making it impractical to do so. This one brilliant tradeoff has allowed the entire world to have faith in digital encryption, allowing us to build a global economy on the internet. It is not to say it is perfect by any means, but it is strong enough to a point where it deters most people from attempting to break it. Which is why most cyber-attacks do not actually target the encryption algorithms themselves, but prey upon people with phishing emails, or social engineering.

That is why signing up for any website, application, or store rewards program is another trade-off. We know that there is inherent risk with giving out our personal digital information, yet most people still do it out of convenience. Also some people, sadly, still use the same password at every website. The trade-off for those who do this is the simplicity of remembering one password for everything, while having the false sense of security based on the strength of their password. Browsers have tried to help deter that habit by introducing password managers, but still, many do not even know they exist.

These two examples I touched on are just a couple of ways in the security field that tradeoffs can work as both a benefit and be harmful. I tend to believe the convenience factor will most always be on the top of the list for the average user, so it is important for us in the cyber security field to balance their security with that fact in mind.

# Week 2: Threat plus Vulnerability = Risk

No unread replies.No replies.

In the *Basics of Information Security,* Andress writes: "Risk is the likelihood that something bad will happen. In order for us to have a risk in a particular environment, we need to have both a threat and a vulnerability that the specific threat can exploit. For example, if we have a structure that is made from wood and we set it on fire, we have both a threat (the fire) and a vulnerability that matches it (the wood structure). In this case, we most definitely have a risk."

Thinking about your personal information security, what do you assess to be your most significant current **vulnerability** and associated **threat**?

My most significant current vulnerability is just the sheer number of websites that I have signed up for in the past with my email and the old password I used to use for everything. I have been online since Christmas of 1999, so I have lost track of the exact amount, but according to my Chrome password manager extension there are over 570 websites that I have given out my personal digital information to. It seems like an alarming number, but I have done my best over the past few years to go to all the major websites I use and have a unique password. For instance, none of my social media, banking, or shopping accounts use the same password or email. I also have two factor authentication on all of them to increase the depth of security on them. However, I am only human, and I could have missed something important.

The biggest associated threat I have is an attacker who is willing to purchase my information from the darknet and using that to perform a social engineering attack. I have used tools such as [www.haveibeenpwned.com](http://www.haveibeenpwned.com) and I know that my old passwords are available for anyone to find which is quite troubling. Taking that and knowing that a lot of my personal information is on the internet, an attacker could gather enough of it to try and get my cellphone provider to assign my cell phone number to a new SIM card to bypass two-factor authentication on my major accounts. This type of attack is called a SIM swap attack and it is used more often now to try and get into the high-reward accounts of users such as banking. SIM swap attacks are a troubling trend and is why even more companies are requiring multi-factor authentication, which includes some type of biometrics such as a fingerprint or face scan, to help protect against this type of attack.

# Week 2: What should Jashopper do?

Based on your interpretation of this week's readings, which, if any, of the proposals presented by Secom should Jashopper accept? Why?

Copmany needs:

5 servers for internet functions and to host the website

Can fit on one-fourth of a rack sapce

Six global IP addresses

Take the Advanced housing proposal along with the Secom Passport for Web.

For a company the size of Jashopper, with the aspirations to eventually launch an IPO, I believe the best route to go here would be to take the second alternative proposal from Secom, along with the addition of the Secom Passport for Web. The second proposal consisted of advanced housing, which includes both physical and cyber security for servers hosted in Secom's secure data center. The SDC improves security of the site by minimizing the threats of viruses and hackers by using a fault-tolerant environment. It also includes an identification and access-control system which is done with Secom's ID ONE card. The card shuts out access by unauthorized individuals, and it is another layer of deterrence for employee crime. These solutions work for the company in its currents size and give them the flexibility to scale up as it continues to grow, which is exactly what it needs.

The Secom Passport for Web is also another important part of the proposal that I believe Jashopper needs because it gives the website SSL certification capabilities which was missing from the advanced housing piece of the proposal. The Secom Passport for Web allows the data in all transactions on the website to be 128-bit encrypted, ensuring customers communication privacy. Along with the passport, Secom helps promote the websites security policies with an authentication sticker placed on the Jashopper website after passing Secom’s Aduit policies. As we learned from the video with Mr. Schneir and learned in this reading, it is important for the company to present a feeling of security to its customers, even though the reality is nothing is 100% secure.

The total cost for the proposals I chose to accept is around 2.5 million yen per year. The idea was not to break the bank entirely, but to ensure a reasonable level of security. For a company that just passed 1 billion yen per year in revenue and one that aspires to launch an IPO, I believe the money would be well spent. Not only would it comply with the law, but it would also give investors future reassurance, which is the goal for a company wanting to go public.

# Week 2: The Risk Management Process

No unread replies.No replies.

Figure 1.4 in *The Basics of Information Security* illustrates the five-step risk management process:

1. Identify assets
2. Identify threats
3. Assess vulnerabilities
4. Assess risks
5. Mitigate risks

Identify which **ONE** area of this process you would **MOST PREFER** or **LEAST PREFER** to work in and explain why you feel this way.

For me personally, the process I would most prefer to work in is assessing vulnerabilities due to its depth of work covering both the physical and logical aspects of cyber security. Not only could I test software applications, operating systems, and networks but I would enjoy thinking about the design and implementation of the physical controls put in place which protect our data. Being able to either be behind a computer working with software or in the field would give me enough variety to keep me interested in the work a long time.

When it, the process I would least prefer to work in would have to be identifying assets. To me personally, it sounds like boring work to determine what has the most value to a company or organization, and not something I would wake up in the morning excited to do. I am much more of a hands-on, tinkerer type of person so anything having to do with administrative or clerical work would take the creative drive right out of me.