Research Paper

Thomas Egyed

Saint Leo University

Information is the most critical asset of any company in today's world. This could be information about customers such as names, addresses, or credit card numbers. It could be patient records at a hospital. It could be blueprints or code for a project a company is working on. If any of this information is compromised the company could be in a lot of legal trouble, earn a bad reputation, or even go out of business. This is why companies need to consider everything even if it seems unnecessary when dealing with information security. Being able to identify a threat, understanding the impact that threat could have on the company, and if there is a way to mitigate the threat will prepare the company for real life situations.

There are several key components that need to be thought about and implemented to ensure that a company's information is safe. The first component is dealing with threats. Most companies see IT security as a burden or just not important at all. They think they will never be attacked by hackers. Security is often overlooked because the cost associated with it is considered too high and can be used towards development time. Youngran Hong and Dongsoo Kim said that "it is better to adapt IT security review in all of the system development. However, it is almost impossible to do this because of the cost problem.". Their review system divides the security process into four parts. The first is Compulsory adaptation to some cases. The second is partial adaptation to the important systems. The third is partial adaptation to general systems, and the fourth is simple adaptation to general systems. Compulsory adaptation is for systems that have more than $300,000 investment in development. Partial adaptation to important systems would be relevant to systems that deal with private data such as credit card numbers, social security numbers, and other types of account numbers. If a company's system falls into this category, it should almost always be considered for review because this is very sensitive information. If it were to be lost, stolen, or compromised by other means the company would

most likely be in legal trouble. Partial adaptation to general systems development is every that doesn't deal with important data. This section could be reviewed if the company has taken care of any other important system first and has left over money. Simple adaptation to general system changes is the least important out of the four. It is to review old systems that are already functional but might need to be addressed because of new standards and technologies. By using this standard with the four types it can help determine which systems in a company need to be reviewed. It shows how important security is and emphasizes why it needs to be a priority. By focusing on security a company lessens the chance of a threat turning into a problem.

The next component a company needs to consider when protecting their information is application and networking attacks. The entry and exit to a company's information is their network. The staff needs to be constantly educated on all the new networking attacks that are happening every day. Herzberg and Shulman discovered a new type of networking poisoning attack called socket overloading. Socket overloading essentially sends short low-rate bursts of packets to the victim host. It exploits the clients port with the overload to create packet loss between kernel interrupts. From there The attacker then uses the loss event to determine if it is the correct port and then can proceed with the attack. The victims network interface determines the destination socket of incoming packets and places them in the appropriate queue. It the queue is full the packet is then discarded. The network interface card (NIC) is attacked with malicious packets until the queue is full and starts to overload. This type of attack might not end with company information being stolen but could overload the network and shut it down. If the network is unavailable, the company will most likely not be able to do business. They cannot access their customer records, payments, inventory, or other things. If the company cannot

operate then they will make no money. This is extremely harmful for the companies that offer services on their networks such as file hosting, gaming servers, and video content.

The next component Application and Host security is about securing devices and system software that companies use. Corcoran, Peter, and Claudia Costache believe that smart phones will play a big role in companies today because they are extremely popular. They said that "Biometric systems are used to establish or confirm a person's identity by detecting, analyzing, and then comparing patters in physical characteristics against enrolled records of those patterns." The simplest form of biometric verification is photo identification. You hand someone a driver's license or passport and they check the photo on the card against your face. If it matches, then you are allowed access. Using biometrics as an everyday form of authentication is not necessarily a good idea. In the future you might need to use your thumbprint to pay for something or use an iris scan to check in for an appointment. The problem is if this information gets stolen, you cannot get a new thumbprint or eye. It can lead to permanent identity theft with no way of recovering. Instead you could use a smart phone "to generate an enrollment key and that is what is stored, rather than the biometric itself. This eliminates a key risk. If the key is stolen, it is a straightforward process to generate and register a substitute enrollment key." Companies should follow this practice if they allow their employees to use smartphones to access sensitive information within the company. It could also be possible to use biometrics to access accounts such as a bank account or credit account. There would be no central database of credentials which would mean there is nothing that could be compromised and would essentially eliminate credit-card fraud. If a company allows their employees to bring their own devices or give out company phones for them to use they must understand that those smartphones hold valuable and sensitive data which needs to be protected. The two most popular smartphone operating systems,

iOS and android, have a security feature that enables a type of sandbox mode which isolates an application from the kernel and other data. It is in a shielded environment in which it cannot be compromised. This feature is great for keeping the device secure but the problem is not necessarily with the device itself but with the owner of the device. Many users simply accept any permission an app wants without even reading it. Doing this defeats the entire purpose of security features. The user is giving them access to the entire device, even the areas with valuable information.

The next component companies should consider is cryptography. Many people are storing their files on cloud services. When they do this they have no direct access over their files. A new type of cryptographic tool that could help with this issue is Oblivious RAM also known as ORAM. It is designed to conceal access patterns when a client executes a sequence of reads and writes to outbound data. Implementing this type of cryptography will help strengthen the companies walls from outside attackers. It secures the customers connection to the information which is one less area for attackers to probe. Companies also need to consider the future of cryptography when protecting their information. Quantum computing is no more science fiction and becoming more of a reality. It will have a huge impact on cryptography's modern security and privacy. Normally a 2,048-bit RSA key would billions of years to crack using a typical computer. Using quantum computing it would only take a few seconds. The companies that choose to only use cryptography to protect their information would be at great risk. It would only take minutes to obtain all their information and secrets if a group of hackers could access a quantum computer. Because of the potential risks the US National Security Agency is developing quantum-resistant algorithms because they do not want to take any chances.

The next component is ensuring a company's network is secured. When running Ethernet cables or fiber optic cables throughout the company the route of the cables needs to be considered very carefully. The cables should be enclosed in a shroud that cannot be cut or tampered with. Servers and computers should be kept away from outside walls incase an attacker could penetrate it. Servers and networking equipment should be in a locked room with appropriate alarms and equipped with the necessary tools to deal with natural disasters. Another aspect of physical security to consider is jamming and eavesdropping attacks. An attacker could be at the perimeter of the company attempting one of these attacks. To mitigate a jamming attack the company could implement more antennas. This will weaken the jammer because the extra antennas will be compensating for the interference. To prevent an eavesdropping attack the idea is to make sure that the confidential information being transmitted between the legitimate transceivers cannot be retrieved by the eavesdropping attacker. A solution is to implement a jamming or artificial noise device inside the company to prevent an eavesdropper from obtaining information. The walls and windows of the organization could also be lined with a film or type of shield to block signals from going in or out. If the company is using optical networks they are vulnerable to several types of attacks at the physical layer which can lead to security breaches, loss of privacy, revenue losses, and more. The company could implement a software defined networking (SDN) as a solution. A SDN simplifies control and management of optical networks. The SDN shifts the control logic from routers and switches to a centralized controller acting as a networking operating system. Several types of programmable software applications can be installed on this networking operating system and interact with the physical networking cables and devices underneath. Traditional networks only secure the perimeter with firewalls, switches, translators, and other devices which leaves the internal network open to attackers if they get in.

These types of devices cannot keep up with real-time decision making needed from the incredible amount of data going through the equipment. Switching to a software based network makes every part of the network protected by several layers, it is more efficient, and costs considerably less compared to tradition methods of protection.

The next component is managing company account and authentication security. Traditionally online transactions are secured through issued certificates. This system is flawed because the third party issuer learns too much information about the transaction or the receiving party learns more attributes than necessary which makes them a target for hackers. A solution to this problem of access control and account management is to use private credentials. By using private credentials the certificate issuers do not have to be involved during authentication process and users disclose only the attributes required by the relying parties. And this whole process can be done without being easily tracked across the transactions. The company should also have a database of every employee and all their access rights. Every login on the system should log the time, location, user, and information they are accessing. This is a good practice because if something were to happen the company they could easily go back and review the logs.

Privacy breaches are one of the worst things that can happen to a company and can be very expensive to resolve. Companies need to change their outlook on risk management for privacy breaches. The Google v. Vidal-Hall case is a prime example for a company to gain insight because it is “a good testing ground for determining where the boundaries of personal data lie in English law.” Google placed a cookie on devices using the Safari browser and collected user data without their consent. It ended up costing them over 22.5 million dollars in the various settlements. Understanding what personal data means in the eyes of the law allows businesses to develop risk management strategies that would normally be overlooked or not dealt

with at all. The more that is considered in the risk management plan the better of the company will be in case a disaster happens.

Another option companies have to consider with risk management is continuous monitoring and risk scoring (CMRS). It is superior to traditional reporting and risk assessment because it constantly monitors and collects data through feeds. Being able to have constant up to date information a company can then assess risks more frequently. The first platform to introduce this type of risk assessment is iPost. Which was developed by the US Department of State. The two greatest challenges for CMRS is information aggregation and risk quantification. With such a large group of information that needs to be collected they need reliable sources and machines that can capture a large amount of data. They also need to consider the risks of this information and make sure it is accurate, credible, and secure.

There is a forever going list of things that a company can do to help keep their information secure. These several components will help and the more the company focuses on spreading security awareness the better off they will be. It is not a matter of if the company will be attacked, it is when the company will be attacked and what they can do to mitigate it. Technology is always improving and so are the number of attacks against companies which is why information security must be a priority.

Hong, Y., & Kim, D. (2015). A Study on the Information Technology Security Review Process in Finance. *Proceedings of the 17th International Conference on Electronic Commerce 2015 - ICEC '15*. doi:10.1145/2781562.2781607

Herzberg, A., & Shulman, H. (2013). Socket overloading for fun and cache-poisoning. *Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC '13*. doi:10.1145/2523649.2523662

Corcoran, Peter, and Claudia Costache. "Smartphones, Biometrics, and a Brave New World." *IEEE Technology and Society Magazine* 35.3 (2016): 59-66. Web.

Latsiou, A., & Rizomiliotis, P. (2014). The Rainy Season of Cryptography. *Proceedings of the 18th Panhellenic Conference on Informatics - PCI '14*. doi:10.1145/2645791.2645798

Mailloux, L. O., Ii, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. *IT Professional, 18*(5), 42-47. doi:10.1109/mitp.2016.77

Zhao, N., Yu, F. R., Li, M., Yan, Q., & Leung, V. C. (2016). Physical layer security issues in interference- alignment-based wireless networks. *IEEE Communications Magazine, 54*(8), 162-168. doi:10.1109/mcom.2016.7537191

Skorin-Kapov, N., Furdek, M., Zsigmond, S., & Wosinska, L. (2016). Physical-layer security in evolving optical networks. *IEEE Communications Magazine, 54*(8), 110-117. doi:10.1109/mcom.2016.7537185

Liyanage, M., Abro, A. B., Ylianttila, M., & Gurtov, A. (2016). Opportunities and Challenges of Software-Defined Mobile Networks in Network Security. *IEEE Security & Privacy, 14*(4), 34-44. doi:10.1109/msp.2016.82

Li, Qing, and Greg Clark. "Mobile Security: A Look Ahead." *IEEE Security & Privacy* 11.1 (2013): 78-81. Web.

Camenisch, J., A. Lehmann, and G. Neven. "Electronic Identities Need Private Credentials." *IEEE Security & Privacy Magazine* 10.1 (2012): 80-83. Web.

Evans, Katrine. "Vidal-Hall and Risk Management for Privacy Breaches." *IEEE Security & Privacy* 13.5 (2015): 80-84. Web.

Kott, Alexander, and Curtis Arnold. "The Promises and Challenges of Continuous Monitoring and Risk Scoring." *IEEE Security & Privacy* 11.1 (2013): 90-93. Web.