Risk Management Plan

Tyler Chotikamars University of Arizona Global Campus

CYB 401 Risk Management and Infrastructure

Robert Key

February 28th, 2022

Risk Management Plan

Every organization has data it needs to protect, whether it is customer data or sensitive operational information, there is something that every company wants to keep to themselves in order do conduct business normally. Within this paper we'll be breaking down a risk management plan for Apple and look at risk assessments of existing vulnerabilities and threats, as well as the cost of implementation. Some key points included here will be analyzing potential attackers and motives, summarizing possible attacks, categorizing attacks, developing a risk management plan, identifying stakeholders, addressing stakeholder concerns, completing the risk assessment, and completing the risk analysis. A risk management plan helps businesses like Apple to understand what is at risk and how much damage attacks can do, but having this plan also allows companies to protect themselves and mitigate risk to keep data safe.

The first step in creating a risk management plan is to assess who the potential attackers could be, and what their motivations are. There can be many potential attackers, and some can include foreign nation states, other companies, script kiddies, and professional hackers. The motivation for these attacks can vary wildly as everybody wants something different in this world. Foreign nation states might want to gather data to use against the whole country, companies might want to get ahold of formulas or other data that could be used to gain a competitive edge. Script kiddies might hack a company because they want a data asset or because they simply don't like the company, and this can be said the same for professional hackers. Professional hackers can be employed by nation states or by competing companies, and they have an extensive knowledge of security tools and mastery over programming languages.

Possible attacks that could be carried out range from social engineering to taking advantage of technology. These include systems contracting malware or viruses, phishing attacks, MITM attacks, Denial of service attacks, SQL injection, XSS, Zero-day exploits, DNS tunneling, Email compromises, cryptojacking, password attacks, as well as many other types of possible attacks. With how many different types of attacks that exist, it’s easy to see why having a risk management plan would be sensible for any respectable organization. There is also the threat of internal attacks happening, this can be done by utilizing social engineering to take advantage of the hospitality of unknowing employees. The methodology of these attacks can be categorized by the exposure level of its assets. Some of these categories of threats can include compromises to intellectual property, deviations in quality of service, espionage or trespass, forces of nature, human error, and information extortion among many other (Whitman, 2018.

Security in large organizations must be managed differently since there are more factors involved. Factors can include having more than 1,000 devices along with having full time security staff. To create a risk management plan for a large company, some functions outside the field of technology such as legal and training must be carried out. IT functions that are not carried out by the InfoSec department are done by another IT group and their responsibilities include things such as network and systems security administration and centralized authentication. Things that fit into the InfoSec’s department of responsibilities include risk assessment, systems testing, incident response planning, disaster recovery planning, performance measurement, and vulnerability assessment. These responsibilities must be carried out with legality concerns such as policy, risk management, and compliance in mind. Within creating a risk management plan for a large organization such as Apple, there are some security decisions that are challenging that must be made. These include dealing with how to mitigate security compromises that stem from employee's or failure, as well as budgeting for the plan. Here, InfoSec teams are made up of many different people. There is the CISO, department of compliance, risk assessment/management, and technical services. This can often include 4-5 full time security managers,10-15 full time security administrators/technicians, 5-10 part-time security managers, with about 30-35 full-time security admins/techs. The risk management plan will include components of a security program that includes culture, size, and budget. Some elements of a security program include policy, program management, risk management, life-cycle planning, personnel/user issues, preparing for contingencies and disasters, and computer security incident handling. The risk management process can be broken down into these steps, establishing the context, risk identification, risk analysis, evaluation, risk treatment/control, and monitoring and review.

One important part of the risk management plan process is to identify the roles of stakeholders within the plan. The involvement of stakeholders is needed to improve decision-making by managers. Understanding the interests, expectations and motivations of our stakeholders can help the company better protect its intellectual property. Stakeholders must understand how important security is to their investment into the company which is why communication, consultation, and deliberation is key to their involvement. The goal with involving stakeholders is to create an attitude or culture towards risk management that shares the same values. For Apple, one of the main selling points of their devices is privacy, so it's apparent that stakeholders would like to address privacy within the risk management plan.

Within a company like Apple, threats and vulnerabilities already exist. There is constantly threats and attacks taken against Apple, however they have plans already in place to mitigate the amount of risk that is actually being taken. The first step within creating the risk assessment it to create an inventory of information assets. The next step is to classify and organize those assets, then to assign a value to each information asset. Next would be to identify threated to the cataloged assets, and to pinpoint vulnerable assets. Analyzing risk includes determining the likelihood that vulnerable systems will be attacked, assessing the relative risk factor of information assets, calculating the risks to which the assets are exposed to in their current state, identifying ways that controls can be used to fix attacks, and documenting and reporting the findings of risk the identification and assessment. Evaluating the risk and sizing up the organizations assets towards what could happen is also a part of this process which is made of two steps. These steps include identifying individual risk tolerance for each asset and combining risk tolerances into a risk appetite statement. The next step within this is to treat the unacceptable risk which includes installing controls, overseeing procedures, and determining a treatment/control strategy. The final step is to summarize the findings which concludes the risk assessment and includes the identification, analysis, and evaluation stages of risk assessment (Whitman, 2018). The risk analysis of the cost of implementation weighs out the value that comes from implementing new controls. If new controls can lead to a lower risk analysis then it may be worth considering for big companies, however the cost of implementation is what stops new technology from being used.

Managing risk and assessing how much damage it can do is essential to any business large or small since it effects customers, the company, and enables attackers. Creating a security and organizational culture within the company’s work environment will help with creating a risk management plan. Another important note is that risk management plans need maintenance. Apple already has security functions in place to protect their brand and business, however no matter how well made your plan is, there is always room for improvement. Creating a risk management plan that covers everything from analyzing potential attackers to having a complete risk assessment is a great way to implement security, and when used in conjunction with other security tools a risk management plan can help businesses and people keep their data safe.

References:

Data Security, Integrity, and Retention. (2020). *Library Technology Reports*, *56*(6), 36.

Li, J., Singhal, S., Swaminathan, R., & Karp, A. H. (2012). Managing Data Retention Policies at Scale. *IEEE Transactions on Network and Service Management, Network and Service Management, IEEE Transactions on, IEEE Trans. Netw. Serv. Manage*, *9*(4), 393–406. https://doi.org/10.1109/TNSM.2012.101612.110203

Little, B. (2007). Whose data is it, anyway? [data retention policy]. *Information Professional*, *4*(3), 38–40.

Whitman, M. E., & Mattord, H. J. (2018). *Management of information security* (6th ed.). Cengage Learning