Husnan Ejaz

Study.com

Computer Science 331

July 2023

Cybersecurity Research Paper

Executive summary: As the Chief Information Security Officer (CISO) of Store My Bits International (SMBI), I have been tasked to perform a full cybersecurity analysis. This plan should target the recent phishing vulnerabilities and how to strengthen our company’s security in order to reduce exposure to further breaches. This plan encompasses three core concepts: the identification of vulnerabilities, proper incident response, and contingencies put in place in order to ensure a thorough set of standards to protect our data.

The first element of our cybersecurity analysis plan is to be able to identify vulnerabilities, after all, the first step to solving a problem is to identify the problem. In order to mitigate the risk of missing vulnerabilities within our infrastructure, it is important to implement various kinds of vulnerability identification. First and foremost, regularly conducted vulnerability assessments in the form of penetration testing would be at the forefront of vulnerability identification. Penetration testing grants our experienced team permission in order to ethically hack into our systems in order to identify threats, exploit vulnerabilities, and in turn strengthen our weakest links. Proper penetration testing allows for a collaborative effort amongst our cybersecurity team in order to identify weaknesses and ensure they are not exploited by bad actors. The second method of vulnerability identification in this plan is the integration of threat intelligence. While it may seem daunting, the use of threat intelligence serves one main purpose – to stay on top of developing threats. This is most notably implemented within network security; as intrusion detection systems (IDS) and intrusion prevention systems (IPS) both identify malicious incoming traffic, threat intelligence firewalls proactively update their defenses to new attacks.

Furthermore, one key element of vulnerability identification employee awareness. After all, the attack that breached into our environment and costed over $2 million to eradicate was a phishing scheme. Phishing schemes are successful primarily due to lack of awareness of their victims, and use a technique known as social engineering to manipulate and deceive in order to gain access to sensitive data (Cybersecurity Vulnerabilities: Definition & Types). By implementing security awareness training for employees, we can create an environment and culture in which safe practices are encouraged.

The second sector of our cybersecurity analysis plan addresses incident response. In short, incident response is the process of investigating and identifying the source, effects, and mitigation of any threat when it occurs (Information Security Plan: Examples & Incident Response). By creating and explicit incident response plan, we aim to set a standard, protocols, and synergy amongst our staff. A detailed incident response plan that outlines duties, responsibilities, and procedures to follow in the event of a security breach will be implemented here at SMBI. With that being said, it is important to establish an incident response team who will be designated to respond to attacks at the time of occurrence. This team will be comprised of experienced individuals from our company from several departments such as IT, communications, and security. It is important to keep this incident response team concise, as too many members can decrease disaster response efficiency, and only designated members of each department will be assigned this great task.

Now that we have established the members of the incident response team, it is just as important to define the roles of each individual within the team. In order to break this down to adhere to the cybersecurity industry standard, we can categorize our incidents by severity and create a tier of escalation. With security analysts across all tiers, we can define an escalation process when certain threats have greater impact and need to be escalated to either management or a team of experienced security analysts. In addition to having a tier of escalation, a strict guideline for containment, eradication, recovery and communication must be adhered to. This is referred to as our security playbook, and they contain step-by-step regulations and direction. One part of incident response is making sure your team is adequately equipped in order to handle attack situations when they occur. In order to do this, mock drills are an essential part of testing the incident response teams capabilities without causing harm to company data. Lastly, and most importantly, communication amongst those involved with the company is crucial. Conducted a lessons learned review post incident is a great way to document and track progress as a firm to ensure we are constantly evolving our data protection methods. Stakeholders, customers, and employees must also be notified with proper documented communication to ensure that everyone involved with the company is being notified of events as they occur.

The third and final component of our cybersecurity analyst plan is a contingency plan. By definition, a contingency plan is a written risk management document that provides instructions, recommendations, and considerations for a company on how to recover their IT services and data at the event of a security breach, disaster, or system disruption (Cybersecurity Contingency Plans: Purpose, Development & Implementation). A well thought out and organized contingency plan is crucial to the success of our business in the event of a disaster. The first characteristic of our contingency plan constitutes data backup, we will keep redundant backups both on-site and off-site to ensure accessible recovery in the event of any type of emergency. This redundant data should also be encrypted, so that it is not accessible by unauthorized users wrongfully. Additionally, disaster recovery plans and business continuity plans must be established in order to have guidelines for employees to follow in the event of a security breach. Industry standards have paved the way for business continuity and disaster recovery, one example that demonstrates the significance of these plans is Aaron F Brantly’s article in the Oxford Journal of Cybersecurity. Briefly put, because Brantly’s team had immensely detailed disaster recovery and continuity plans, they were able to adhere to the strict protocol of their company. When the incident response team was able to nullify the attack vector, Brantly and his team quickly sought to resume the cadence of the business by restoring back ups as suggested by their plan. Brantly recalls this event as monumental to his career, as dealing with finances can be very stressful, he adds, being able to patch and recover lost data is part of the job duty of a cybersecurity professional (Brantly).

In addition to the three elements that create a solid foundation to our cybersecurity analysis plan, it is important to not get complacent. Constant improvement is the true indicator of success, as cybersecurity threats grow strong each and every day. In order to gauge progress, the plan includes a means to track metrics. For example, key performance indicators can be outlined and targeted in order to see if we are meeting our security goals. One indicator may look like a reduction in false positive or false negative flagged events by our intrusion detection systems, or a reduction in escalation of tickets in our incident response team. Another key way to monitor and track our progress as a company would be to set up a security operations center. If the funds allow, we can create a 24/7 monitoring system that is sufficient enough to handle incidents around the clock. While it may seem expensive at first, there is no price you can put on the confidentiality, integrity, and accessibility of the data infrastructure here at SMBI.

In conclusion, our comprehensive cybersecurity plan for SMBI was created with the goal of strengthening our data infrastructure. With the scope of our plan being vulnerability identification, incident response, contingency planning, and performance indicators. We addressed each of these elements of the plan by following tried and true industry standards, such as playbooks and disaster recovery plans, all while assigning our own parameters here at SMBI. While we strive to protect our data, we should keep in mind each element of this plan and always remain vigilant to threats to our infrastructure.

# References

Brantly, Aaron F. *Risk and Uncertainty*. 23 February 2021. Web. 28 July 2023.

"Information Security Plan: Examples & Incident Response." Study.com, 26 September 2016, study.com/academy/lesson/information-security-plan-examples-incident-response.html

"Cybersecurity Vulnerabilities: Definition & Types." Study.com, 9 May 2018, study.com/academy/lesson/cyber-security-vulnerabilities-definition-types.html

Cybersecurity Contingency Plans: Purpose, Development & Implementation." Study.com, 11 November 2021, study.com/academy/lesson/cybersecurity-contingency-plans-purpose-development-implementation.html