Option #1: Propose a Security Policy for an Organization

Liam Bergerson

CSU - Global

ITS460-1

K. Gregar-Skillman

1/15/23

Option #1: Propose a Security Policy for an Organization

In a world dominated by technology, thousands of organizations fall prey to data breaches that compromise their sensitive data. As technology evolves throughout the years, the methods threat actors use to breach the organizations evolve as well. Even more techniques are developed and existing techniques are advanced. It's crucial that there are security measures that mitigate data breaches that organizations suffer from. In order to achieve that, several organizations are created to provide clients with security measures to protect their sensitive data from data breaches.

For my hypothetical organization, that vision is no different. My hypothetical organization will be called PenSafe. PenSafe is an organization that provides its clients with several different types of security measures that will protect them from data breaches from as many angles as possible. Security measures such as anti-virus software, firewall configurations, education/training, authentication methods, proper implementation of encryption, incident response procedures, etc. PenSafe will also provide penetration testing for any of its clients that wish to have their security measures checked for any vulnerabilities. The overall strategy that PenSafe wishes to implement is a loop of providing security measures to clients and testing those security measures by means of penetration testing so those security measures can be improved upon. That cycle will continue until those security measures are as refined as possible to minimize the rate of data breaches towards its clients.

Analysis of Relationships

PenSafe's relationship goal will be providing a sense of trust to the clients. Since their organization will be safe from data breaches by using PenSafe's security

measures, their belief in PenSafe will increase and more services will be used to protect the clients' organization. The relationship goal within the staff and management is to provide a positive environment where members can come together and create new ideas for new security measures and improving existing ones. The environment will remain positive via a code of ethics that will protect all parties. The relationship goal towards the stakeholders of PenSafe will be to ensure that stakeholders keep investing in PenSafe because of their belief in the security measures used to protect its clients from data breaches. Word will spread to other stakeholders and clients about the effectiveness of PenSafe so that the value of PenSafe increases exponentially.

Vulnerability Assessment

McKeever et al. (2022) provides an excellent vulnerability assessment process that will be used at PenSafe to test the vulnerability of all systems, networks, databases, etc. A vulnerability assessment is the systematic review of vulnerabilities within information systems (McKeever et al., 2022). It essentially reviews systems, networks, and databases for vulnerabilities and rates those vulnerabilities based on severity level if those vulnerabilities were to be exploited. The vulnerability assessment process that will be used is a four-step process. The four steps consist of testing, analysis, assessment, and remediation. The testing step is the identification of vulnerabilities. It basically identifies all vulnerabilities towards a system, network, or database. The analysis step is to identify root causes to these vulnerabilities. For example, an old version of a patch could be used or default credentials are still being used on network configurations. The risk assessment step is categorizing vulnerabilities based on the severity level if it were to be exploited. The vulnerabilities with a higher severity level will

be prioritized first in the remediation process. Finally, the remediation process is the actual closure of vulnerabilities.

Security Policy

Remedial Measures

PenSafe will harbor sensitive customer data that requires protection. In order to achieve that, the organization will also have remedial measures to protect our own systems, networks, and databases. Data security software will be one of many remedial measures that will be implemented at PenSafe. Data security software assists organizations in patch management. Patch management is one of the most crucial aspects of security. The constant patches are what secure your system because each patch fixes a certain vulnerability. If systems are not patched, threat actors will be able to capitalize on vulnerabilities and breach the organization. Data security software allows for all patches and updates to be centralized so that patches are not missed (Stanfield, 2021).

Access control will be required within PenSafe. Access control is what controls the access that is given to each and every employee. In order to achieve proper access control, every employee should not be given admin privileges. Threat actors will have many more entry points if every employee has admin privileges. A best practice is to implement the principle of least privilege. The principle of least privilege ensures that every employee is only given access for what they need to do to achieve their work operations and nothing more. The specific access control that will be implemented is role-based access. Role-based access control is a non-discretionary access control method that restricts access for employees based on a role they have (NIST, n.d.).

Instead of assigning individual employees access, they will be assigned a role and access will be assigned to the role.

Mobile device management will be required at PenSafe. Most people in society have smartphones and they could easily be the reason why a threat actor has breached the organization. It's important to ensure that there are policies in place to prevent threat actors breaching the organization through smart devices. A Bring Your Own Device (BYOD) policy will be implemented to achieve mobile device management. A BYOD policy will limit the actions an employee will do through their smart device on the business network that will pose a vulnerability. Some common examples of bad internet habits are freely surfing the internet, downloading random links, etc. The ethical trade-off of a BYOD policy is that you are limiting the freedom an employee has with using their smart device. However, it's better to limit the freedom of using their smart devices while they are on the business network than having to pay thousands of dollars worth of damages because of a data breach.

Backups will be crucially important for PenSafe. Data will inevitably be lost; it's only a matter of when. Backups will prevent data being lost because a copy of that data will be elsewhere. Backups will be made once a week and there will be two backups being made. One backup will be on-site and another will be made off-site on the cloud. That will ensure maximum redundancy so that even if the on-site backup is lost, the cloud backup will remain. Data-at-rest for both the main repository and the backup repository will be encrypted with symmetric encryption. Symmetric encryption uses one key for both encrypting and decrypting. If a threat actor breaches the network and finds the data, they will not be able to read it because it is encrypted. Asymmetric encryption

for data-in-transit will also be used. Asymmetric encryption uses two different keys; one for encrypting and one for decrypting. One example of data-in-transit that will be seen at PenSafe are emails. Emails can easily be intercepted so it's important that email is also encrypted.

Multi-factor authentication (MFA) is a simple but an incredibly effective concept that will be used at PenSafe. Every user logs in to a computer or website using a username and a password. However, there are many methods a threat actor can use to figure out what the username and password is. To prevent that, MFA will be used. MFA requires the user to additionally verify into the system after the username and password is input. This usually is a randomly generated number code from a third-party application.

Education/training is another crucial concept that will be required at PenSafe. Human error is one of most leading factors for data breaches. If human error is mitigated, the number of data breaches will be reduced. Education will come in the form of how to create strong passwords, securing internet habits, and how to spot phishing attacks. Strong passwords must be at least eight characters with the inclusion of both upper and lowercase letters, numbers, and special characters. Bad internet habits such as clicking on every link that shows up on websites, posting on random discussion boards, viewing inappropriate content must be identified and discouraged. Phishing is a method threat actors use to try and trick users into giving up their credentials such as their usernames and passwords. Phishing usually comes in the form of an email and it's important every user knows how to spot a phishing attack.

Anti-virus software, firewalls, and intrusion detection systems will be implemented at PenSafe. Anti-virus software will protect systems from being infected by a virus if a user accidentally installs a virus. Firewalls will limit the data entering or exiting the network based on rules configured by admins. Intrusion detection systems will notify the admins if something malicious has entered the network.

Code of Ethics

A code of ethics is important for every organization as it defines ethical behaviors that are to be followed by every employee. This will ensure that there is a safe environment to maximize efficiency for every employee. The following elements will make up the code of ethics for PenSafe. All employees must be in compliance with every state and federal laws, rules, and regulations at all times. Employees must refrain from conflicts of interest. A conflict of interest arises when an employee receives a benefit as a result of the employee's position with a client. Insider trading is prohibited. Insider trading manifests when employees trade their stocks in the company based on information not available to the public. Information that is not disclosed to the public that is being traded between other employees also qualifies as insider trading. Discrimination and harassment will also be strictly prohibited. All employees will do their part in maintaining the health and safety of the work environment in compliance with health and safety standards. Employees are prohibited from discussing prices or making any agreements with business competitors. Employees are strictly prohibited from bribing, or accepting bribes from, any colleagues or clients. All PenSafe records must contain full, fair, accurate, and timely data. The code of ethics will be reviewed annually and documents must be kept in appropriate detail and comply with the law. All

employees must read through the code of ethics annually and sign a document that requires compliance with the code of ethics.

Legal/Compliance Requirements

As mentioned earlier, all employees must attend a cybersecurity training/education session that teaches safe internet habits, how to spot phishing emails, and how to create strong passwords. A bring your own device (BYOD) policy was mentioned earlier but will be discussed in greater detail. A BYOD policy will limit the actions an employee will do through their smart device on the business network that will pose a vulnerability. Certain websites are not to be visited when surfing the internet on a smart device. A list of these banned websites will be provided to every employee. Camera capabilities are to be disabled when entering company premises. Employees are prohibited from transmitting sensitive documents in any context. A list of acceptable applications are to be provided to every employee that will highlight which applications are free to use. Any application not on the list of acceptable applications are to be automatically prevented from being installed on a device. If a device is idle for at least five minutes, the device must automatically lock itself and require some kind of password or PIN number to unlock. A device must be taken to IT support if it is locked out due to five failed login attempts. Jailbroken IOS devices and rooted Android devices are to be prohibited from connecting to the network.

All employees are prohibited from connecting to open networks with company devices. A hotel network, for example, is an open network. Open networks have no security measures in place that prevent a threat actor from unauthorized connection to a device. If a threat actor were to connect to a company device, sensitive documents will

most likely be found. Sensitive data may also be intercepted when connected to an open network. Specialized software will be used on every company device that will check any network and confirm that the network is secure and has all the necessary security measures in place. When an employee wishes to connect to a network, they must run the software first to make sure that the network is secure.

As stated earlier, all employees must be in compliance with all state and federal laws, rules, and regulations. To ensure that every employee complies with every element stated above, a document will be signed when an employee first joins PenSafe. The employee will be legally held accountable if any of these requirements are broken.

Security Policy Summary/Conclusion

PenSafe is a hypothetical organization that provides its clients with a variety of security tools to protect their systems, networks, and databases as well as provide penetration testing services to clients wishing to have their security measures checked for vulnerabilities. In order for PenSafe to be a trusted organization respected by many peers, a concise and detailed security policy has been made that highlights the security credibility of PenSafe. The security policy includes remedial measures in place that will mitigate data breaches posed by threat actors, a code of ethics that aims to provide a safe and secure work environment, and legal/compliance requirements that all employees will follow. There are a plethora of remedial measures that will safeguard PenSafe as a whole. Patch management will ensure that all systems and softwares are up-to-date in order to minimize present vulnerabilities. Access control ensures that all users have proper permissions into systems, networks, and databases. To achieve this, role-based access is used to assign users to roles instead of assigning them

individually. Mobile device management is achieved through the use of a BYOD policy. Almost every user in this technological age has a smart device of some kind. In order for data breaches to be minimized, those smart devices must be secured. Backups are implemented to ensure that all data is safeguarded from changes, deletion, and corruption. MFA is used to additionally safeguard user accounts by requiring a code to be entered upon login. Education/training is implemented to ensure that users are aware of a variety of tactics threat actors use to deceive employees in order to gain unauthorized access into systems. Finally, firewalls, anti-virus software, and intrusion detection systems are used to secure the network. PenSafe also implemented a code of ethics that defines acceptable and ethical behaviors that all employees must follow in order for the work environment to be safe and efficient. Some elements of the code of ethics include conflicts of interest, insider trading, bribery, discrimination and harassment, etc. Finally, PenSafe has a variety of legal/compliance requirements for all employees to follow to ensure that we are in line with federal and state laws and that employees are safeguarding their internet habits so a data breach doesn't happen.

References

McKeever, G., Rossi, E., Hewitt, N., Rossi, E., Hewitt, N., Hasson, E., Hewitt, N., & Hasson, E. (2022, August 10). *What is Vulnerability Assessment | VA Tools and Best Practices | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/vulnerability-assessment/

NIST. (n.d.). *Role Based Access Control | CSRC*. csrc.nist.gov. https://csrc.nist.gov/projects/role-based-access-control

Stanfield, N. (2021, May 25). *Our Top 10 Data Security Measures To Protect Your Business*. Stanfield IT. https://www.stanfieldit.com/data-security/