SHORT RESEARCH PAPER #2

SEPTEMBER 17, 2023

BRYANT WATKINS
CYSE 300

When asked to design a security policy for a corporate information system consisting of on-premises web, application, and database servers, there are five important issues that should be addressed in the policy. Given that the database servers store very sensitive data, they must be protected by a staunch security policy. The five most pressing issues that need to be addressed are – security awareness and training, incident response, access management, data/asset classification, and change management. The five listed items are some of the most crucial aspects to an information system security that can make or break it.

Security awareness and training is arguably the foundation of any sound information system security policy. No matter what software safeguards or even physical barriers are in place – if staff and personnel are unable to adhere to upholding policy as well as learn common vulnerabilities to watch for then that security policy will likely prove ineffective. The most vulnerable aspect of any system is the user. Management should establish a training mechanism for all employees that will allow them to learn an understanding of why such policies are imperative for the security of all.

Like any scenario in life that involves protection or a plan – there must be a plan for when things go awry. When things go awry in information system security that typically means a breach or incident has occurred. An incident response plan is precisely what takes this role following an incident. The most critical task in incident response is ensuring employees know who to immediately report an incident to. Once employees are aware who to report to – then the rest of the policy should work establish roles and responsibilities such as recovering compromised data.

Access management is a crucial aspect of any security in any context. Given the vast quantities of data and various methods of entry, access management is especially crucial for

information system security policy. A major pillar of access management should entail usage of the Principle of least privilege (PoLP). This principle basically states that users should only be allotted the absolute bare minimum amount of time and resources necessary while accessing data as a way to curtail malicious activity. With such sensitive data in question, access must be heavily monitored as well as establish a set policy for creating, changing, and revoking access.

With the vast amount of data stored there also must be a system for the classification of such stored data. There are varying levels to the potential harm faced with data. Data risk management is one of the tools available in establishing classification of data. Information system security policies are typically expected to have three or more categories to classify data into. Conducting such a policy also works to eliminate unnecessary waste of resources towards data that is relatively unimportant, this allows these resources to be further allocated for more critical data and information.

The final issue to discuss is change management. Like many other things in life – data or information is very much subject to change and sometimes even daily. With the potential for any form of acceptable change it is imperative to establish a policy regulating this. Any changes to data in the system should go through approval, tracking, as well as managing. Change management is very meticulous and time-sensitive task, a task that requires great accuracy as well as continuous supervision.

References

Security Policy: Development and Implementation. National Center for Education Statistics. (n.d.). https://nces.ed.gov/pubs98/safetech/chapter3.asp

Security policy templates. Information Security Policy Templates | SANS Institute. (n.d.). https://www.sans.org/information-security-policy/