After Action Report #1

Group 2

University of Maryland University College

**Security risks and the methods for mitigation**

Hacking of financial systems and connected industries has led to theft and sabotage of confidential personal information of consumers. Cyber terrorism has increased in recent years, and organizations are now required to establish necessary security controls to prevent malicious parties from accessing the sensitive systems. Based on DTL power’s availability of $13,500,000 budget to enhance or change the security of systems and network components, the IT team has made the decisions to secure the network and systems in order to proactively prevent threats that can exploit vulnerabilities in the future. The Cyber Forensics Examiner/Internal Auditor, Network Engineer, CTO, and Information Security Officer worked together to determine the appropriate controls in order to protect the company and its users from attacks.

**After Action Reports by Roles**

**Cyber Forensics Examiner/Internal Auditor**

The Cyber Forensics Examiner/Internal Auditor oversees the organization’s backup needs, database security, Intrusion Detection Protection Systems (IDPS), SCADA Security, SCADA training, SCADA Vulnerability assessment, Systems Development Testing, training and auditing and training incentives.

The decisions taken for each of these areas were made to increase the security controls already in place. The remote back and SCADA Vulnerabilities spending was increased to a medium level of the allowed capital cost, while cost in SCADA training were kept at its lowest cost. On the other hand, security setting which included degree of interconnection, firewall sensitivity, incident monitoring and remote access point privileges for SCADA were set at the strictest levels. Additionally, password security, privileges control and separation of roles for the database security and systems development testing were set to the most rigorous levels.

In training, all fields were set to a moderate level by focusing training areas such as network vulnerabilities, controls, encryption and penetration testing to only a total of 40 percent. Some incentives for technical certifications were provided and physical audit of equipment was scheduled for every 6 months.

Overall, the main goal of the cyber forensics examiner/internal auditor was to ensure the security of the systems. The current evaluation of the decisions made show that the security index for DLT Power is high, however, improvement to the organization’s morale and productivity is need and this can be accomplished by rising the training policies in the company.

**Network Engineer**

The role of the network engineer at DTL power is to ensure that the entire network is up, running smoothly, and secure at all times. DTL being an energy company that has quite a number of users, it is important to ensure that the network security is tight to avoid attacks to the network which could result in user information getting into the wrong hands. The engineer was responsible for making critical decisions in several categories of the simulation.

The degree of advisory is limited and reliance on federal support are for critical issues only. DNS redundancy was chosen. A secure DNS is a key part of an organization's security posture, protecting both online presence, and internal applications. DNS is one of the most critical components to monitor for website performance, and is also the most vulnerable to cyber-attacks. The traditional DNS setup makes it difficult to guarantee availability and poses a constant risk. Hackers can affect hundreds of websites by targeting a single DNS provider. DNS redundancy is a failsafe solution or a backup mechanism for DNS outages. A single dedicated DNS server may not be sufficient if an attack occurs; deploying multiple DNS providers in different networks ensures DNS availability.

In load management, DDOS protection through delayed binding was enabled this security measures are to ensure that the network is protected both on the internet and on-site hence minimizing the probability of cyber-attacks. Implementing firewall with strict filtering gives a level of security that keeps the infrastructure safe from unwanted traffic. Isolate affected areas as needed. Should an attack occur, the degree of information sharing is medium and non-sensitive disclosure and nondisclosure in a non-crisis situation. In the category of SCADA policy interventions, high risk adverse was chosen for risk management policy and implemented system backups to twice a month. Cloud computing was initially chosen over virtualization with a hybrid cloud hosting model and using the cloud for software as a service. It was changed to virtualization after the first simulation.

**Chief Technology officer (CTO)**

The CTO of the DTL Power’s role is to look at the high-level technical controls that were implemented across the organization. This role is important in order to ensure there is a consistent vision across all systems that are implemented. The organization adjusted the antivirus scanning policy was strengthened in frequency to daily scans to gain more visibility to attacks that could get through to employee workstations which could be rapidly quarantined. For example, access from third-party vendors to patch or update DTL Power’s SCADA systems is made through the use of their own equipment. Additionally, patches were also upgraded to Always Once Released in order to keep the systems with the most up to date patches. Allocation for additional Kerberos servers was conducted for strengthening authentication, and encryption key distribution were enhanced in order to add more security around SCADA equipment data access. In doing so, requests to securely control command to equipment must be made was being further logged and can be audited for security risk assessments (Bartman and Carson, 2015).

Breach notifications are limited to critical and significant incidents, this saves the organization time and money. The IT team was reduced to below average size, but due to popular sentiment, will be raised to average in the next round, with full-time employees being held at 80% of the workforce, with new hires required to have an average of 7 years’ experience. Public relations were kept low, at $50,000 to try and keep costs down, since PR isn’t a critical security function. However, the PR budget will increase in order to protect the company’s reputation.

Physical security is essential in regards to a physical attack, as it is the most fundamental kind of attack (Bartman and Carson, 2015). In order to prevent a physical attack, the organization has isolated the rooms containing essential infrastructure to allow restricted access, and will be granted only for those with a need to know basis. The idea behind this is to limit access to trusted, need to know personnel, since the less people that have access the better.

**Information Security Officer**

The decision areas related to the authorized software policy included type of software that employees are permitted to use; the frequency of software evaluations; and penalties for violation of the authorized software policy – based on these decision was made for only approved software allowed for the use of employees to prevent unauthorized software being installed by users; software evaluation should be permed every six months to ensure the security of used software; and warnings will be given to employees that violate this policy – this decision will be updated to suspension of employees who violate the policy in order to hold employees accountable and prevent malicious software use. Business continuity planning decisions included IT storage redundancy degree set as medium since security controls are established to prevent a failover; IT network redundancy degree set as a medium which will be increased to reduce network failure risk; level 3 maximum power backup redundancy to maintain continuous power to the infrastructure; two backup sites maintained for any failover event; two redundancy backup communication links to maintain continuous communication; and policy review performed every twelve months to ensure the policy is maintained.

The general access policy decision areas included the degree of freedom given to employees on communicating over the internet set as restricted to prevent unwanted communication; freedom for browsing non-business sites as restricted to prevent access to malicious sites; only three login attempts before account locks out to ensure accounts are accessed by the authorized user; password changed and validation performed every 45 days to maintain the secure password policy; minimum of 8 characters required for password to prevent passwords from being easily cracked; non-use of prior passwords as 1 to prevent the same password from being reused; and penalty of violating the access policy begins with a warning. Information privacy policy area decisions include investment on privacy policy at $26,000; appointment of a dedicated privacy officer to oversee privacy issues; budget for employee training on the privacy policy at $10,000 since it is important for internal users to perform tasks to ensure the privacy of information; all information to be retained for backup; and termination of employees who violate the privacy policy – since termination and rehiring new employees add to the cost of operations, employee will only be suspended upon violation. Information sharing policy decisions included 2 people in groups to overlook and enforce the internal information sharing policy so the responsibility will not be a single point of failure; information will only be shared on a strict-need-to-know basis based on role-based access control and external sharing, so no unauthorized users will obtain sensitive information; Infragard communication is set to 28 days since the more frequent the more personnel cost to maintain the communication; violation of the information sharing policy will result in fines.

As the patch management policy is important to ensure all vulnerabilities in the system are addressed, decisions include frequency of patch management is set to all updates; patch testing prior to installation is set to a high as testing should be performed prior to deploying to production; the trustworthiness of the patches is set to trusted, however, will be updated to official to ensure patches released officially by the vendor is deployed to production. The remote access policy decisions include remote access by employee grade to executive management, which will be updated to all professional staff members to include the IT staff to ensure actions or issue resolutions can be performed remotely; access privileges permitted is set to medium read/write access which will be updated to a high – read/write/delete; violation penalty for this policy is warnings which is sufficient with all other set security controls to prevent threat incidents. Training fund is set to $1000, but maximizing training will increase employee productivity.

**Stakeholders**

|  |  |  |
| --- | --- | --- |
| Stakeholder | Interest | Influence |
| Executives | High | High |
| Sponsor | Low | High |
| Internal Users | High | Low |
| Customer | Low | High |

**References**

Bartman, T. & Carson, K. (2015). Schweitzer Engineering Laboratories, Inc. *Securing*

*communications for SCADA and critical industrial systems*. Retrieved from <https://ccaps.umn.edu/documents/CPE-Conferences/MIPSYCON-> Papers/2015/SecuringCommunicationsforSCADAandCriticalIndustrialSystems.pdf