10

University
of Victoria

UNIVERSITY OF VICTORIA

SENG 460 - Practice of Information Security and Privacy

Case Study 2 – Information Security Policy and International Standards

1. Analyze the issue.

Corporations and organizations are vulnerable to the process of revealing and stealing their information that stored on their employees laptop, because a new research shows that even if computers lost their power, still DRAMs retains their contents for seconds or minutes which gives an opportunity for someone with physical access to this laptop from revealing the cryptographic keys in memory images and get access to the information.

This issue becomes very critical to the CIO and the security team of ABC corporation due to the sensitive information that stored on their employees laptops, so they think of finding and applying security solutions to reduce the risk of his issue, so they deployed Microsoft's BitLocker disk encryption software which enhanced the protection against this attack but the CIO still receiving reports about cold boot attack cases.

The CIO finally decided to initiate the development of a security policy to mitigate the risk of cold boot attack.

2. Define the purpose of this policy development task.

To protect cryptographic keys in memory images in DRAMs when an employee lose his/her laptop or when a person steals the employee's laptop and consequently preventing the revealing of DRAMs contents.

3. Identify and analyze risks, threats and vulnerabilities of the attacks addressed in the Princeton video clip.

	Risk	Threat	Vulnerability
Cold boot attack	- Stealing contents in the DRAM. - Disruption of the organization reputation. - Affecting trust relationship between stakeholders. - Significant financial loss	-Data alteration -Stealing laptop by thief. - Installing spyware software. - Installing malware software. - Replacing internal components of laptop with other suspicious ones.	-Data remanence property of DRAM for seconds or minutes. -Using portable device (laptop) can be moved and put anywhere easily. - Lack of employees awareness about these attacks - Lack of training sessions for employees.
DMA/Firewire attack	-Stealing encryption keys.	-Attaching external hard disk or USB	-Leaving the laptop on mode sleep, on, or

	- Get access to sensitive information. - Obfuscating the organization transactions. - Civil litigations against the organization.	memory that contains the attack script (bit unlocker). - Loss of application software - Stealing passwords of internal systems in the organization	off. - Underestimating the impact of these attacks. - Lack of communication and cooperation between stakeholders. - Having no disaster recovery plans.

4. Search for both policy and technical security controls to mitigate the identified risks and threats in the previous step.

1.5

Policy security controls:

- Keeping laptops out of sight when not in use.

- Not leaving laptops on the car seat of a parked car.

- Carrying laptops in something other than a laptop bag to avoid an obvious target.

- Keep an up-to-date backup of all data to ensure that work isn't lost if a laptop goes missing.

- Contact the IT staff in case you have question, you are not sure about specific operation, or you have suspicion about weird action.

- Attend the training sessions that are held by the IT department.

- Educate yourself about information security risks, threats, and the protection measures associated with it, by reading information magazines and visiting online websites.

Technical security controls:

- Each employee should use USB token device as a second authentication mechanism

- using BIOS password to access the laptop.

- Installing tracking software in the laptops to determine the location of it in case of stealing.

- Installing time bomb software that for instance deletes all the important critical files if the laptop is not connected to the Internet for specific period of time.

- Using cable lock when laptops are left unattended.

- Using biometrics authentication systems like (fingerprints, voice recognition system, iris scanner)

- Disable the USB ports on the laptop when they are not used.

- Install anti-malware and anti-spyware software to detect any suspicious action.

- Secure all the data stored on laptop using AES 256-bit encryption

5. Analyze the impact of deploying the chosen controls to business and procedures.

Business –

- Protecting the information of the organization
- Adding more cost to the budget of an organization
- Mitigating the risks and threats of cold boot attack.
- Mitigating the risks and threats of DMA attack.
- Protecting the assets of the organization
- Maintaining the reputation of the organization
- Enhancing the trust relationship between stakeholders

Procedures –

- Increasing the efficiency of the business procedures
- Increasing the effectives of the business procedures.
- Requiring stakeholders to be aware of new technologies and systems.
- Avoiding interruption in the procedures.
- The availability of information used by the procedures.
- The confidentiality of information used by the procedures.
- The integrity of information used by the procedures.

6. Identify stakeholders and define their security roles and responsibilities.

Stakeholder	Roles	Responsibilities
Data owner	Like the head of HR department or finical controller who has	Ensure compliance with organization policies and regulations.

	administrative access and account to the dataset that assigned to him/her based on his/her department or level.	Specifying appropriate mechanisms for obtaining access to information assets.
Data custodian	Like system administrator who has technical control on the organization dataset and also has and control the root account access.	Responsible for granting and removing access to information based on requests from the data owner. Responsible for collecting logs about information access provided to others. Applying appropriate security controls to protect information and organization assets.
Data user	Like employee or third-party provider who has critical role to protect and maintain information system (i.e. data on laptop). Data user usually is authorized by data owner.	Follow policies, standards and procedures that assigned by the organization. Report any suspected or weird activity to appropriate person.

7. Define compliance metrics.

- How mobile is the laptop?
- What are protective measures are in place?
- Are employees trained in security measures?
- Does the organization have security training programs?
- Is there any disaster recovery plan?

8. Provide standards and guidelines supporting the policy, if necessary.

ISO/IEC 27002:2013

9. Based on the findings, write up a policy to mitigate the risks of attacks addressed in the Princeton video clip.

The Policy

2

1.1.1 All laptop computers must be protected with security controls against cold boot and DMA attacks.

a) Intended users
b) Cold boot and DMA attacks
c) Risks and Threats
d) Security controls

Purpose: To protect cryptographic keys in memory images in DRAMs and information stored on hard disk on laptop.

1.1.1 a) Intended users

Any stakeholder of the organization who has access to laptop computer and could be but not limited to one of the following stakeholders (Data Owner, Data Custodian, Data User) should be aware of the risks and attacks that are associated with the usage of laptop computers and the security controls that should be taken to mitigate these risks and threats.

1.1.1 b) Cold boot and DMA attacks

There are many physical attacks associated with laptop computers such as cold boot attack and DMA attack.

- In cold boot attack, an attacker with physical access to a laptop is able to reveal encryption keys from a running laptop after using a cold reboot to restart the machine.
- In DMA attack, a.k.a Firewire attack, an attacker with physical access a laptop can steal the cryptographic keys by getting direct access to the physical memory address space of the computer.

Following the security controls that are mentioned in this policy mitigate the risks and threats associated by these attacks.

1.1.1 c) Risks and Threats

The inappropriate usage of laptop computers could lead to successful implementation of cold boot and DMA attacks which lead to critical threats and risks which are but not limited to the following:

- Losing laptop computers.
- Stealing contents in the DRAM.
- Installing spyware and other malware scripts by attacker.
- Disruption of the organization reputation.
- Affecting trust relationship between stakeholders.
- Stealing encryption keys and decrypts the hard disk to get access to information stored on it.
- Obfuscating the organization transactions and operations.
- Civil litigations against the organization.
- Loss of application software.
- Data alteration and modification.
- Stealing login information that gives access to other systems in the organization.

1.1.1 d) Security controls

Minimum protection measures for the use of laptop computers against the previous attacks include but not limited to:

- Keeping laptops out of sight when not in use.
- Not leaving laptops on the car seat of a parked car.
- Carrying laptops in something other than a laptop bag to avoid an obvious target.
- Keep an update backup of all data on another device to ensure that work isn't lost if a laptop goes missing.
- Using a USB token device with BIOS password as a second authentication mechanism to be able to access laptops.
- Installing tracking software in the laptops to determine the location of the laptop in case of stealing.
- Installing time bomb software that for instance deletes all the important critical files if the laptop is not connected to the internet for specific period of time.
- Attend the training sessions that are held by the IT department.
- Educate yourself about information security risks, threats, and the protection measures associated with it, by reading information magazines and visiting online websites.
- Contact the IT staff in case you have question, you are not sure about specific operation, or you have suspicion about weird action.
- Using cable lock when laptops are left unattended.
- Using biometrics authentication systems like (fingerprints, voice recognition system, iris scanner)
- Disable the USB ports on the laptop when they are not used.
- Install anti-malware and anti-spyware software to detect any suspicious action.
- Secure all the data stored on laptop using AES 256-bit encryption

Standards:

ISO/IEC 27002:2013.

Metrics and Enforcement:

- Do employees have the permission to take laptops out of the organization building?
- Are employees using cryptographic techniques in the organization?
- Are employees trained in the process of how to backup information?
- Does the organization have security training of how to mitigate cold boot and DMA attacks?
- Is there any disaster recovery plan?

Other References:

ISP 3 – Asset management
ISP 4 – Information security awareness, education and training
ISP 5 – Equipment security
ISP 6.4 – Protection against malicious mobile code
ISP 6.5 – Information backup
ISP 6.7.2 – Media handling