Cybersecurity management Report

CSM Schornstein

Remi Chemak
194633IV

Table of Contents

1. Body description

The establishment to be studied is a medium size e-commerce private company, named CSM Schornstein. The company is actually an affiliation of a bigger industry group, which is specialized in chimneys manufacturing. This affiliation is quite young as it has started its business very few years ago. Therefore, it is still in the expansion and development step. The actual premises of the company are part of big building, hosting other companies as well.
The company is run by a manager, working with two marketing and sales analysts, and a developer who is relevant to the IT manager.

2. Business process

The mission of CSM Schornstein is to manage an online shop in order to sell the mother company's products (mainly chimneys). It also has its own depository to assure availability of products and quick delivery.

3. Information and IT assets

The company's IT assets can be classified into two categories: functional IT solutions and business IT solutions. The latter are usually the most critical ones.

3.1 IT assets

3.1.1 Functional assets

Functional assets essentially consist of IT solutions for the general use within the company. These solutions are employed by the company's employees to accomplish their tasks. When those assets are down, it doesn't affect much the company's main business, which is selling its products.

ID	Asset	Description	Main stakes
FA01	Three connected workstations	These workstations are intended for the manager and the marketing employees. They contain all sort of information about the company's sales and business plan, and the customers database, alongside other critical databases	The most important is to maintain their confidentiality and secrecy. Integrity is also very important to assure the reliability of the data the marketing consultants are working on
FA02	Developer's	This workstation is intended for the	Secrecy is important as

	workstation	company’s IT manager to occasional code maintenance, and it’s most of the time disconnected from Internet	the website’s code source is stored on this computer. But the most crucial to ensure is availability, because the workstation from which some urgent code patches are done
FA03	Depository’s workstation	This workstation is placed in the depository, and is mainly used by the depository’s responsible to manage the depository related tasks.	As most data stored on this computer are essentially industrial, it has to assure a certain level of integrity and confidentiality.
FA04	Router and WiFi adapter	It’s the company’s main network material	It should be always available and and reliable
FA05	Multi-functional connected printer	This printer takes its importance from the fact that the company’s contracts and confidential documents usually go through it	Confidentiality and authentification at most

3.1.2 Business assets

Business assets consist of IT solutions which critical for the business itself. This infrastructure is used to provide the company’s services to customers.

ID	Asset	Description	Main stake
BA01	One connected server	The server hosts the company’s e-commerce application	Its availability and integrity is extremely crucial and a high level priority. The confidentiality however is less important; the content is already public through the website (which is actually intended to be public and seen by as many people as possible), and the platform used is open source
BA02	One backup server	The same as the previous server, to use in case of break down of the main server	Once again for the server, it’s mainly about integrity and availability

BA03	Router	This router is what connects the website to Internet, so it has to protect it from possible attacks and hacks	It has to assure availability, confidentiality and non-repudiation

3.2 Information assets

Information assets are all sort of data or information which are of value to the company's business development.

Information ID	Information Asset	Format	Support	Confidentiality	Integrity	Availability
IA01	Customer's database	SQL file	FA01	S2	T2	K1
IA02	Order's database	SQL file	FA01	S2	T3	K2
IA03	Web e-commerce platform	Source code files	FA02-BA01	S2	T3	K3
IA04	Company's contracts	PDF and document files	FA01	S3	T3	K2
IA05	Workstations' logins and passwords	Logs and/or cache	FA01	S2	T2	K3
IA06	Server's security policy		FA02	S2	T2	K2
IA07	Products industrial information	SQL files and documents files	FA01	S1	T2	K1
IA08	Depository's documents (orders, returns,	Document files	FA03	S3	T3	K1

	bills ...)					
IA09	Depository’s internal communications	Document files	FA03	S3	T1	K1
IA10	Depository’s stock information	Document and SQL files	FA03	S2	T2	K1
IA11	Marketing strategy documents	Document files	FA01	S3	T1	K1
IA12	Mounting partners related information	Document files and SQL files	FA01	S2	T1	K2
IA13	Business e-mail service	Web cache files and cookies	FA01	S2	T2	K2
IA14	Stored important e-mails and communication	Documents files	FA01	S2	T2	K1
IA15	Web application’s content	Source code file and document files	FA01-FA02-BA01-BA02	S0	T2	K3
IA16	Server’s configuration	Configuration files	BA01-BA02	S2	T2	K1

3.3 Business Impact Analysis (BIA)

Functional assets: In case of functioning disruption within the common company’s IT infrastructure, the main business functions aren’t directly affected.

Business assets: In case of disruption, it’s the business core of the company which is affected. A malfunctioning of the hardware or the software would result in immediate break in the provided services by the company.

4. Threats and vulnerabilities identification

4.1 Main threats

4.1.1 Environmental

- Internal physical incidents (fire …)
- Extreme temperature (weather during summer or winter) which is critical for machines to work sustainably, especially for the server
- Unrestricted access to the premise’s building
- Sabotage (including state sponsored actions)
- Theft of hardware or sensitive documents

4.1.2 Human

- Undermined custom service requests (social engineering)
- Disclosure of security policy confidential documents
- Disclosure of marketing related confidential documents
- Disclosure of workstation’s passwords
- Disclosure of server’s admin password

4.1.3 Technical

- Power failure which will bring down the server
- Server saturation (after a DDoS attack for example)
- Commercial data manipulation
- Malfunction of company’s network devices (router or WiFi adapter)
- Malfunction of server related network devices
- Unauthorized access to company’s workstations
- Unauthorized access to server
- Manipulation of server’s configuration
- Manipulation of the application’s source codes
- Server penetration (Hack)
- Workstations’ hacking
- Communication eavesdropping
- Encryption of server’s files by a Ransomware

ID	Threat	Category	Type
T01	Natural incidents (fire …)	Environmental	Incident
T02	Extreme temperature	Environmental	Incident
T03	Unrestricted access to the building	Environmental	Malicious
T04	Sabotage	Environmental	Malicious
T05	Theft of hardware or sensitive documents	Environmental	Malicious
T06	Social engineering	Human	Malicious
T07	Disclosure of security policy confidential documents	Human	Incident/ Malicious
T08	Disclosure of marketing related confidential documents	Human	Incident/ Malicious
T09	Disclosure of workstation's passwords	Human	Incident/ Malicious
T10	Disclosure of server's admin password	Human	Incident/ Malicious
T11	Power failure	Technical	Incident
T12	Server saturation	Technical	Malicious
T13	Commercial data manipulation	Technical/ Human	Malicious
T14	Network device malfunction	Technical	Incident
T15	Malfunction of server related network devices	Technical	Incident
T16	Unauthorized access to company's workstations	Technical	Malicious
T17	Unauthorized access to server	Technical	Malicious
T18	Manipulation of server's configuration	Technical	Malicious
T19	Manipulation of the application's source codes	Technical	Malicious
T20	Server penetration	Technical	Malicious
T21	Workstations' hacking	Technical	Malicious
T22	Communication eavesdropping	Technical	Malicious
T23	Ransomware	Technical	Malicious

4.2 Main vulnerabilities

4.2.1 Human

- Lack of human resources training regarding Cybersecurity
- Lack of access control to the company’s facilities
- Employees might connect their compromised personal devices to the company’s network, the latter would then be compromised on its turn.
- Poor password management

4.2.2 Technical

- Vulnerabilities within the web platform itself (XSS, SQL injections …)
- Insecure code from the developer
- OS security holes for the functional machines
- Security holes within the installed software for the workstations
- Vulnerable network hardware configuration
- Bad configuration of the security parameters of the server
- Outdated installed software
- Weak or lack of server’s protection systems

4.2.3 Organization

- Lack of system supervision
- Lack of confidential documents handling procedure
- Unauthorized access to the company’s premises
- Lack of e-mail secure usage policy
- Unrestricted access to the company’s overall building

4.2.4 Infrastructure

- Unstable power supply
- Security holes within the network hardware
- Bad isolation or protection of the servers’ room

5. Risk management

5.1 Risk scenarios

We start by developing some risk scenarios through threats and vulnerabilities impairment. Here we list only the most spread and classical scenarios according to major IT security organisms.

Risk Scenario ID	Threat	Vulnerability	Source	Asset
R01	Social engineering (T06)	Lack of human resources training regarding Cybersecurity	Hacker	Workstations' logins and passwords (IA05)
R02	Disclosure of workstation's passwords (T09)	Poor password management	Hacker/ Internal	Customer's database (IA01)/Order's database (IA02)/Company's contracts (IA04)/Marketing strategy documents (IA05)
R03	Power failure (T11)	Bad isolation or protection of the servers' room	Power station	Web e-commerce platform (IA03)
R04	Commercial data manipulation (T13)	Vulnerabilities within the web platform itself (XSS, SQL injections …)	Hacker	Customer's database (IA01)/Order's database (IA02)
R05	Network device malfunction (T14)	Security holes within the network hardware	Hardware manufacturer	Business e-mail service (IA13)
R06	Server penetration (T20)	Bad configuration of the security parameters of the server	Hacker	Order's database (IA02)/Web e-commerce platform (IA03)
R07	Workstations' hacking (T21)	Security holes within the installed software for the workstations	Hacker	Customer's database (IA01)/Order's database (IA02)/Company's contracts (IA04)/Marketing strategy documents (IA05)
R08	Ransomware (T23)	OS security holes	Hacker	Web e-commerce

		for within the server		platform (IA03)

5.2 Risk impact and probability

Considered probability levels are Rare, Unlikely, Possible, Probable and Certain.
Considered impact levels are Insignificant, Minor, Moderate, Major and Extreme.

Risk ID	Detection speed	Time loss	Probability	Impact
R01	Up to 1 day	3h-8h	Probable	Major
R02	Up to 1 week	3h-8h	Unlikely	Major
R03	Immediate	6h-8h	Rare	Extreme
R04	Up to 1 week	Up to 2 days	Possible	Major
R05	Up to 1 day	2h-5h	Possible	Moderate
R06	Up to 1 day	6h-8h	Possible	Extreme
R07	Up to 1 day	3h-8h	Probable	Major
R08	Immediate	Unkown	Probable	Extreme

5.3 Cybersecurity risk treatment and controls

5.3.1 Risk matrix

We consider five main risk assessment levels which are Irrelevant, Low, Medium, High and Critical.

		Impact				
		Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Probability	**Rare**	Irrelevant	Irrelevant	Low	Low	Low
	Unlikely	Irrelevant	Low	Medium	Medium	Medium
	Possible	Low	Medium	Medium	High	High
	Probable	Low	Medium	High	High	Critical
	Certain	Low	Medium	High	Critical	Critical

5.3.2 Risk assessment and treatment

In order to assess each risk and rank them, we have to consider multiple criteria. The first which is the most important is the the score we deduct from the risk matrix. When two risks get the same assessment, it goes to the impact, then the probability. And finally, we also consider the importance of the targeted information asset.
Adopted treatment measures are essentially four, which are Terminate, Treat (reduce as possible as we can), Transfer and Tolerate.
Decision about the treatment measure to adopt must take into consideration risk assessment and the risk scenario in general, as well as the difficulty of the treatment.

Risk ID	Risk assessment	Risk treatment
R08	Critical	Terminate
R06	High	Terminate
R04	High	Treat
R07	High	Treat
R01	High	Terminate
R02	Medium	Treat
R05	Medium	Treat
R03	Low	Tolerate

6. Cybersecurity controls

6.1 Important controls

6.1.1 Security training

Description: Provide training to all employees about major social engineering scenarios, with relevant examples. Besides, the employees should be aware the targeted data by hackers, so they can be able to detect these attempts.
Responsible: IT manager
Targeted risk: This should be adequate to terminate R01

6.1.2 Backup

Description: Make daily backup of the server's data and configuration. This backup should be saved to the developer's workstation, as well as a separate removable device such as a USB stick. The backup reproduction should be tested upon the backup server, and keep a weekly updated version of the backup

server, which is supposed to be a clone of the live server. In case of an emergency, only minor configurations are required for this backup server before it can go operational online.
Responsible: IT manager
Targeted risk: This should be adequate to terminate R08 and R06

6.1.3 Workstations' security

Description: Protect the workstations with an Antivirus, and keep all software always updated, to be sure to have all recent security patches installed.
Responsible: IT manager
Targeted risk: This should be adequate to reduce risks regarding R02 and R07

6.1.4 Secure development

Description: Always revise code source, as well as the platforms security reports to be up to date regarding latest security incidents and discovered vulnerabilities.
Responsible: IT manager
Targeted risk: This would considerably reduce risks regarding R04

6.1.5 Server's security

Description: Install a SIEM on the server such as Prelude completed with a compatible IDS such as Snort. Both software should parameterized according to business requirements.
Responsible: IT manager
Targeted risk: This should mitigate the risk R06

6.2 Other controls

- Define appropriate firewall rules for the server using iptables for example
- Always use strong passwords
- Segregation between mobile devices and desktop computers as much as possible, and between personal devices and the company's hardware
- Secure remote access to the server according to the administrators needs (for example disable SSH root access)
- Use backup power suppliers
- Audit to the company's IT infrastructure regularly
- Use fire detectors and alarms
- Control access to the company's premises
- Install CCTV cameras in the offices
- Install additional locks for the server's room
- Delete user account when an employee leaves the company

7. Cybersecurity monitoring

7.1 Measures and indicators

Measure	Indicator	Limit value
Website requests received on the server	Number of website requests received on the server	500 requests per minute
User accounts	Number of active accounts	Equal to number of employees
SIEM alert system	Number of critical alerts	Always 0
Update	Last update check	< 1 week
Backup	Last backup	< 1 day
Used software	Number of non-supported software	Equal to 0

7.2 Incident handling

Damage	Procedure		Role	Maximum response time
	Immediate Response	Long term		
Server's data	Power off live server (if not already done within the incident). Then start immediately configuring the backup server, in order to put it online and substitute the damaged server. The website should be restored very quickly.	Investigate the damaged hardware (or software) using Forensics, in order to better understand what happened, and hopefully get the responsible identity. For the long term investigation, and depending on the incident's impact, the help of the BSI might be asked.	IT manager	15 minutes
Workstations compromised	Deconnect machines from the network, clean them up in order to put them back into service as	Investigate the damaged materials, and look for possible incident's causes (rootkit, malware …),	IT manager	1 hour

	soon a possible.	and determine the exploited vulnerability.		
Unauthorized server access	Identify the unauthorized access entry point. Then deconnect, the compromised server and substitute it with the backup server as soon as possible. But the backup server should be configured to eliminate the vulnerability before going online.	Investigate the compromised server and look for the compromised files or information in order to treat this leaks. For example, if it’s revealed that some passwords were compromised, then they have to be reset. Also proceed for a check of possible back-doors installed.	IT manager	15 minutes

7.3 Improvement and optimization

- Check latest vulnerabilities discovered regarding the used e-commerce platform, the server’s OS or the workstations’ software. Thus to be able to anticipate some eventual new threats and risk scenarios, and so implementing appropriate controls to mitigate those new risks.
- Identify the most vulnerable software/hardware and always check for better and more secure alternatives.
- Check regularly for IT security agency’s report (for example BSI in Germany) or other approved Cybersecurity institutions for latest attack techniques, in order to always re-adapt the general security policy and update implemented controls.