CYBER SECURITY RISK ANALYST PORTFOLIO

Author: Yasmin Morshed

November 2021

Contents

Executive Summary 3
Risk Management Qualitative Measurement Methodology 3
1. Risk Matrix 3
2. Risk Register 4
Patch Management Using RACI Chart 6
Conclusion 6
Portfolio 4 7

Executive Summary

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." – Stéphane Nappo

Cyber security risk analysis is essential in identifying threats and vulnerabilities. If correct analysis is carried out and correct mitigations are put in place to minimise the risk of potential threats, the business will save considerable amounts of time and money by avoiding cyber security incidents. In addition, some cyber-attacks can lead to data breaches and very expensive legal implications, which must be avoided. In this report, we will look at the risk management qualitative measurement methodology, including the risk matrix and the risk register to define the severity of the vulnerabilities covered in the previous report. The patch management will then be evaluated using a RACI chart.

Risk Management Qualitative Measurement Methodology

Qualitative risk analysis relies on the use of a risk matrix to define the severity of a risk. The risk matrix ranks the probability of risk occurrence against the potential impact of the risk.

Probability x Impact = Gives us a value which defines the overall **severity** of a risk

1. Risk Matrix

Below, we have used a 4x4 risk matrix. A 3x3 matrix could also be used: although 3x3 is straightforward to use, it is more open to errors. A 5x5 matrix could also be used. However, it would be too complex.

		SEVERITY			
		Catastrophic: 4	**Critical: 3**	**Marginal: 2**	**Negligible:1**
PROBABILITY	**Frequent: 4**	High- 16 No antivirus or malware, no removable media policy, no firewall, not following GDPR, no backup, no password policy (and generic passwords being used), computers not locked when not in use, any file could be accessed (except for files from 2 depts)	High- 12	Serious- 8	Medium- 4
	Probable: 3	High- 12 Sufficient cyber security training has not been provided, access to dubious websites not blocked, important hardware (including server) on side table, sales team have been given laptops and they could potentially connect to unsafe Wi-Fi connections	Serious- 9 Anyone can install software, RDP is on, consumer grade switch is being used, single data line is being used	Serious- 6	Medium- 3
	Remote: 2	Serious- 8 No ID upon entry or reception area	Serious- 6 Same door being used for delivery of sheds and entrance of people	Medium- 4	Low- 2
	Improbable: 1	Medium- 4	Medium- 3	Low: 2	Low- 1

2. Risk Register

* Date identified is same for all columns, 5/11/21

ID	RISK	CAUSE	LIKELIHOOD	IMPACT	SEVERITY	OUTCOME	MITIGATION PLAN
1	Viruses and malware	No antivirus or antimalware in place	Frequent	Catastrophic	High	Infection of company computers, loss of files if no backup has been taken	Download appropriate antivirus and antimalware software and keep them up to date
2	Virus and ransomware infection spread via use of removable media	Removable media being used without any rules	Frequent	Catastrophic	High	Viruses and malware infecting the computer systems when an employee plugs in their removable drive- things are worse as there is no antivirus, no backup	Use of external media should be banned or highly regulated
3	Viruses and cyber attack	Appropriate firewall protection not put in place	Frequent	Catastrophic	High	"Disabling a firewall can leave a business vulnerable to abuse, allowing viruses to infect interconnected devices, and giving cybercriminals the opportunity to execute malicious code remotely."[1]	Appropriate firewall should be put in place
4	Personal information is not protected	Not following GDPR, personal information not protected	Frequent	Catastrophic	High	If GDPR is not followed and personal information is not protected, the business can face serious legal and financial consequences in case of an attack/ data breach.	GDPR must be followed, personal information of customers is an important asset and must be protected. The same applies to payment information.
5	Loss of all files, including customer information, order details	No backup strategy in place	Frequent	Catastrophic	High	If a backup strategy is not in place, all important files could be lost in the event of an incident such as a ransomware attack or physical damage to equipment.	Use appropriate backup strategy. I suggest the 3-2-1 backup strategy. "A 3-2-1 strategy means having at least three total copies of your data, two of which are local but on different mediums…, and at least one copy off-site."[2]
6	Weak passwords	There is no password policy, generic passwords such as 'guest' have been used	Frequent	Catastrophic	High	If a weak password is used, anyone can easily and very quickly hack the computer systems using attacks such as brute force. Hackers will try to break into the computer systems or employee accounts with financial motives. Customer and business details will be at risk.	Generic passwords must not be used. Company should have security police. A combination of letters (both uppercase and lowercase), numbers and special characters should be used. Three random words can be used as well as the above.
7	Unauthorized people accessing computers and company files	Computers are not locked when not in use, all files on the server could be accessed except the finance and personnel folders.	Frequent	Catastrophic	High	If an unauthorized person enters the company, they can easily access the unlocked computers and access any files apart from those in the finance and personnel folders. This could potentially include customer details which should be protected under GDPR.	All computers must be locked when not in use by employees. Each employee should have a password of acceptable complexity to access their account on the systems. Access to files should be limited to authorized people in the corresponding department.
8	Employees not cyber aware so will be lured by scams, phishing	Sufficient cyber security training has not been provided	Probable	Catastrophic	High	Employees could easily be lured by scams such as phishing, ransomware could then be installed on the system, leading to encryption of the computer systems. Access to files will be lost in case of ransomware attack. The attackers will ask for a lot of Bitcoin to reallow access to the	Provide thorough training on cyber security. All employees must be aware of cyber security attacks such as phishing and spear phishing. They must be told not to click on any links in suspicious emails as this could take them to a spoofed version of a website

[1] https://smallbusiness.chron.com/happens-firewall-disabled-62134.html
[2] https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

						systems and even after they have taken the sum, they may not allow access. There has been an increase in ransomware attacks this year.	to steal their details or it could download malicious files onto their computer, infecting the systems.
9	Infection via visiting dubious websites	Access to dubious websites has not been blocked	Probable	Catastrophic	High	Employees may visit dubious websites in their free time and these websites can install malicious files onto their systems, infecting the systems.	Block access to dubious websites in the company.
10	Important hardware at risk	Server, printer, router on side table	Probable	Catastrophic	High	These important items should not be easily accessible. They are at risk by unauthorized people and also at physical risk (in case of fire). If the server goes down, the whole business goes down.	The server must be in a designated area called a data centre. There must be additional controls utilised to ensure it is working and safe. Smoke and water detectors must be installed in the area. There should be a way of monitoring any power failure or overheating. The employees should have cards for accessing printed documents to prevent unauthorized access.
11	Risk of hackers or snoopers gaining access to company files and details.	The sales team have been given laptops which connect wirelessly when they are in the office and to any connection they can find when they are travelling.	Probable	Catastrophic	High	A public Wi-Fi has many privacy and safety issues as it can be hacked.	The employees should use their mobile phones as tethering hotspots or use a Virtual Private Network (VPN) when accessing public Wi-Fi such as those in a coffeeshop or a library.
12	Systems becoming infected with viruses due to software download	Anyone can install software on company computers	Probable	Critical	Serious	Downloading of software by any employee can lead to many problems.	
13	The system is vulnerable to access by unauthorized people who can hack the system by getting administration rights	Remote Desktop Protocol (RDP) is on.	Probable	Critical	Serious		Check and fix issues with commonly hacked ports (including RDP) in security tests.
14	Less flexible and secure	Consumer grade switch is being used	Probable	Critical	Serious		Use small business network switch
15	If data line goes down, there will be no internet	Single data line is being used	Probable	Critical	Serious		Use more than one data line
16	Unauthorized people entering the company	There is no reception area. No form of identification is required to enter	Remote	Catastrophic	Serious	The likelihood of someone entering the company unnoticed has been marked as remote because the company is small, and the other employees would notice this. However, if an unauthorized person does enter the company, they could easily use the computers as they are left unlocked, stealing important information.	There must be a way of checking who is entering and leaving, for example, there could be a reception area or CCTV could be used if that is possible.
17	Accidents or unauthorized entry	The same door which is used for loading sheds is used to enter the building	Remote	Critical	Serious	The risk is not high because the same door has been used until now and no accidents have happened. However, in terms of health and safety and privacy, it is much better if the	Separate door to be used, but this might not be possible as the unit is in a small industrial estate.

						delivery door is separated from the entrance door.	

Patch Management Using RACI Chart

"RACI is an acronym that stands for **responsible, accountable, consulted and informed**. A RACI chart is a matrix of all the activities or decision making authorities undertaken in an organisation set against all the people or roles."[3]

R	Responsible
A	Accountable
C	Consulted
I	Informed
For eg AR, CI	More than 1 role

Project Activity	CEO	HR	IT Dept	Sales Director	Manufacturing Director	Finance Director	Delivery and Site Director
Train employees on cyber security, implement cyber culture			AR			CI	C
GDPR should be followed	AR		CI				
Systems are running antivirus, antimalware which is up to date			AR				
Appropriate firewall is put in place			AR				
Policies on / ban use of removable media such as USB sticks			AR				
Appropriate backup strategy should be put in place			AR				
Company laptops are set up with acceptable standards of cyber security for use (including installation of VPN)			AR				
Health and safety in the workplace, especially when making the garden sheds	A				R		CI

Conclusion

Using the risk matrix, risk register and RACI chart, the business can decide on important changes that must be made to the cyber security regulations and culture of the company to mitigate the risk of cyber security incidents.

[3] https://www.iosh.co.uk/~/media/Documents/Networks/Branch/Humber/Branch%20Presentations/how-to-do-raci-charting-and-analysis.pdf?la=en

Portfolio 4

ATT&CK helps you know how effective your defences are, if the data you are collecting is useful, and it helps to answer other questions you may have as well although it is not 100%. It is a knowledge base of adversary behaviour, based on real-world observation, it's free, open and globally accessible. It provides a community language for people to use, and it is also community driven.

ATT&CK lives in the TTP section at the top of the pyramid. The view we see in it is called the matrix. Tactics are the column names, the adversary's high-level technical goals, such as initial access. Down the columns, we have techniques or how the goals are achieved. Behind each of the techniques, we have the procedure examples. Each technique gives a description of what the activity is, why the adversary may be doing it and various levels of technical detail of how that technique could actually be done. We are also provided with metadata, starting with the technique ID. ATT&CK is a communication mechanism. For example, spear phishing attachment is also called T1193. The other pieces of metadata we see are platforms, data sources and there are others as well.

After this we have mitigations which are different ways that you can prevent the technique from taking place in the first place or turning into malicious activity. Then we have detections and procedure examples (specific examples of how attackers have done these). The procedure examples are referenced. There are group pages as well, which describe a specific threat group.

The ATT&CK use cases are detection, threat intelligence, assessment and engineering and adversary emulation.

The video was useful in helping me understand MITRE ATT&CK and things were explained very clearly.