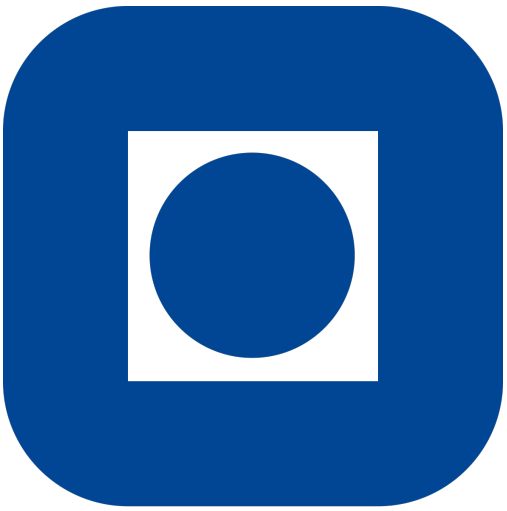
SOHO Case Study

Kristian Havstein, Ole André Hauge, Sigrid Karset



NTNU

September 20, 2020

Contents

List of Figures

List of Tables

Abbreviations

MITM	Man in the middle
WEP	Wired Equivalent Privacy
SLA	Service Level Agreement
OS	Operating System
MFA	Multi factor authentication
SETA	Security education, training and awareness
LAN	Local Area Network
VLAN	Virtual LAN
SLE	Single-loss expectancy
IP	Intellectual property
SOHO	Small Office/Home Office

1 Introduction

The Meier family are frequent and heavy users of information technology, both professionally and personally.

The corona pandemic has given rise to a sudden and oftentimes complete need for "work from home"-arrangements (remote work). This special circumstance removes social, operational and technical countermeasures implemented by the Meier parents work organizations.

In this paper a short risk assessment will be conducted of the Meier's small office/home office (SOHO) network. The assessment will focus on risks that present themselves in the Meier's SOHO solution, as well as risks that are accentuated by the current corona pandemic.

Mr. and Mrs. Meier have had a dinner-table discussion and concluded that they are willing to risk losses up to *9,999 kr* as long as it *unlikely* to happen regularly. This is equivalent to levels one and two in the radar chart, as well as the following likelihood and consequence pairs: *(0,0), (0,1), (1,0), (1,2), (2,1)* and *(2,2)*.

2 Assets

In this section, we identify and list assets for the Meier family. Table 1 gives an overview of these and their value. The table also contains weighted score for the assets, which is based on potential impact on reputation, personal, and professional.

Table 1: Table of Assets

Nr	Name	Usage	Value	Reputation	Personal	Professional	Score
Criterion weight				30	40	30	100
1	Parent PC	government, business / personal finance	8000	0.5	0.9	0.2	57
2	Lilian laptop	Study, economics	5000	0.4	0.8	0	44
3	Jan laptop	Study	5000	0.2	0.8	0	38
4	Dora laptop	Study, games	5000	0.1	0.5	0	23
5	Tablet 1,2	Apps, browsing	2x2000	0.1	0.2	0	11
6	Phone 1,2 - parent	MFA, apps, browsing	2x4000	0.7	0.8	0.6	71
7	Phone 3,4,5	Apps, browsing	3x3000	0.4	0.7	0	40
8	WEP Access point	Network infrastructure	0	0	0.2	0.2	14
9	Business credentials	Business	N/A	0.8	0.4	1	70
10	Internet connectivity	Business, Study, Browsing	N/A	0.1	0.2	0.2	17
11	Business information	Business	N/A	0.8	0.7	1	82
12	Financial information	Private	N/A	0.5	1	0.2	61
13	Private information	Files	N/A	0.7	1	0.1	64

Assets with a higher score are designated as important (valuable) and should be prioritized in the choice of countermeasures. Weighting is primarily determined by; cost of replacing the information, cost to employers, value of intellectual property and loss of productivity caused by lack of availability.

Some assets are hard to accurately estimate a financial value for, and may be irreplaceable. These are marked as "N/A" in table 1.
We see from the table that assets pertaining to the parent's PC, business credentials (authentication), private-, business- and financial information are the most valuable. This should be addressed by chosen

countermeasures, if found to be vulnerable to identified threats in the later chapters.

Note that the low score of the wireless access point in itself, does not mean that this asset should not be considered for countermeasures as other assets are dependent on this network device's security posture.

3 Vulnerabilities

This section will identify vulnerabilities in the Meier's SOHO. The vulnerabilities is presented in a table consisting of the vulnerability description and the associated threat.

Table 2: Table of Vulnerabilities

Vulnerability nr	Description	Threat
1	No redundancy in network equipment	Deviation in quality of service
2	Residential SLA for internet uplink	Deviation in quality of service
3	Missing endpoint access control	Software attack
4	Missing disk encryption	Confidential information leakage
5	Missing backup policy	Technical hardware failure
6	Vulnerable wireless encryption standard	Confidential information leakage
7	No logical separation of device types in network (VLAN)	Confidential information leakage
8	No backup power	Forces of nature
9	Low security awareness	Human error, Compromises to intellectual property, Technological obsolescence
10	No spam filter	Human error
11	Insufficient/absent anti-virus	Malicious Software
12	Lack of backup	Malicious Software

4 Threats

This chapter will identify and portray the threats the Meier family are facing in their threat environment. This will be visualized in the form of a threat table.

The threat table, table 3, contains a list of threats with qualitative scoring for potential damage associated with each. This score is reflected in later consequence estimations.

Table 3: Threat table

Threat nr	Name	Description	Potential damage
1	Compromises to intellectual property	Compromise of business' IP. Copyright infringement associated with torrenting.	5
2	Technological obsolescence	Obsolete networking equipment, operating system	4

3	Social Engineering	Being tricked into giving credentials or installing malware	5
4	Deviations in quality of service	SOHO uplink SLA may have lower standards vs. business SLA	1
5	Confidential information leakage	Compromise of business secrets. Compromise of sensitive private information	5
6	Software attack	Software attacks that can compromise all identified assets	4
7	Technical hardware failure	Failure of hard-drives	3
8	Human error	Accidental installation of malware	4
9	Forces of nature	Lightening strike may damage or destroy equipment. Lack of electricity may inhibit use of equipment.	2

From table 3, we see that the damage potential for identified threats are highest for social engineering, business- and private confidential information leakage, and compromise to business related intellectual property. Note that the damage estimation is in relation to the Meier family.

Costs associated with protection against threats is covered in the chapter for countermeasures and the pre-defined packages for control.

5 Likelihood and Consequence

Before a risk score can be given, a definition of likelihood and impact should be presented. The risk likelihood and consequence is scored from 0-5 as presented in table 4 and 5.

Table 4: Measures of Likelihood

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely the next 12 months	Will never happen
1	Rare	5% likely the next 12 months	May happen once every 10 years
2	Unlikely	25% likely in the next 12 months	May happen once every 5 years
3	Moderate	50% likely in the next 12 months	May happen once every year
4	Likely	75% likely in the next 12 months	May happen multiple times a month
5	Almost Certain	100% likely in the next 12 months	May happen weekly

Table 5: Measures of Consequence

Rank	Description	Example	Productivity Loss (H)	Financial Impact
0	Not Applicable	No impact	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0-4,999kr
2	Minor	Multi-minute interruption, no exposed data	2	5,000-9,999kr

3	Moderate	Multi-hour interruption, minor exposure of data	4	10,000-19,999kr
4	Major	One-day interruption, exposure of data	8	20,000-49,999kr
5	Severe	Multi-day interruption, major exposure of sensitive data	24	>50,000kr

6 Risks

This chapter assesses the relative risk facing the Meier family's information assets, with a focus on risks related to the current corona crisis. The risks are calculated for the assets and used to measure the effect of the suggested countermeasures, as well as showing the residual risk. The next chapter will discuss the residual risk, if it is within the family's risk tolerance and suggest different packages which the Meier family can choose from depending on their budget. Table 6 bellow illustrates the risk situation before the assessment.

Table 6: Risk Matrix Before Countermeasures

		Likelihood				
		1	2	3	4	5
Consequence	1					
	2			7		
	3		8	5,9	1	
	4			3	4	
	5			2,6,10		

6.1 Risk nr. 1

Risk description: Internet connectivity lost
Threat: Deviations in quality of service
Vulnerability: No redundancy in network equipment, residential SLA for internet uplink
Asset: Parent PC, Internet connectivity (10)
Incident: Loss of work productivity due to reduced network uplink quality (availability).
Before countermeasure:
Likelihood: 4 Consequence: 3 Risk: 12
Countermeasure: LTE backup router
After countermeasure:
Likelihood: 2 Consequence: 1 Risk: 2

6.2 Risk nr. 2

Risk description: Unsafe endpoint configuration and usage
Threat: Confidential information leakage, compromises to intellectual property
Vulnerability: Missing endpoint access control, missing endpoint disk encryption
Asset: Parent PC (1), Business Credentials (9), Business information (11), Financial information (12)
Incident: Confidential information and\or intellectual property of employer leaked when un-qualified service personnel are given access to parent PC's for hardware repairs. Youngest child uses same user account as parent, and therefore has access to all files on parent PC. A potential lack of judgement in the childs' use of said PC leads compromise.
Before countermeasure:
Likelihood: 3 Consequence: 5 Risk: 15

Countermeasure: Configuration of local disk encryption, auto-patch, individual user accounts and least privilege principle for user rights,
Professional IT consultation (not unclue Ismir).
After countermeasure:
Likelihood: 1 Consequence: 0 Risk: 0

6.3 Risk nr. 3

Risk description: Single point of failure in parent PC
Threat: technical hardware failure
Vulnerability: Missing backup policy
Asset: Parent PC (1), Business information (11), Financial information (12), Private information (13)
Incident: Hard drive failure on parent PC leads to private and business data loss.
Before countermeasure:
Likelihood: 3 Consequence: 4 Risk: 12
Countermeasure: Backup of data to extra portable hard-drive.
After countermeasure:
Likelihood: 2 Consequence: 2 Risk: 4

6.4 Risk nr. 4

Risk description: Compromised LAN
Threat: Confidential information leakage
Vulnerability: Broken wireless encryption standard, no logical separation of device types in network (VLAN)
Asset: Wireless access point
Incident: Use of an old wireless access point with broken encryption means that network traffic, and access to the network, is effectively in clear text and available for all in-range (network signal), low-skilled adversaries. This makes attacks on devices in the LAN possible. Further, mobile devices are in the same logical network as PC's. This gives a potential attacker a low-security device that can be used as a staging point for attacks on other network connected devices.
Before countermeasure:
Likelihood: 4 Consequence: 4 Risk: 16
Countermeasure: New WPA3 compliant and faster (802.11ac) wireless access point - with guest network separation.
After countermeasure:
Likelihood: 2 Consequence: 4 Risk: 8

6.5 Risk nr. 5

Risk description: Loss off availability due to power outage
Threat: Forces of nature
Vulnerability: No backup power
Asset: Internet connectivity (10)
Incident: Due to a thunder storm, a lightning strike takes out the power line to the family's neighborhood. Since the family is working at home, they do not have a UPS (Uninterrupted power supply) and therefore will not be able to connect to the internet to conduct work.
Before countermeasure:
Likelihood: 3 Consequence: 3 Risk: 9
Countermeasure: Invest in an UPS.
After countermeasure:

Likelihood: 1 Consequence: 1 Risk: 1

6.6 Risk nr. 6

Risk description: Leakage of work credentials due to phishing
Threat: Human error, Social Engineering
Vulnerability: Low security awareness, no spam filter.
Asset: Work credentials (9)
Incident: Mrs. Meier receives an e-mail titled "Update on the COVID-19 situation" signed by a coworker. The e-mail links to a document in OneDrive. The OneDrive site prompts for a username and password, and when entered, the site gives a failure error code and asks to try again later. Although the e-mail was signed by a coworker of hers, the mail itself was from an unknown address. Mrs Meier fell victim to a phishing attack, and her work credentials are now compromised. Because of the home office situation, more people receive important messages and files through e-mail and the likelihood of getting a fraudulent mail increases.
Before countermeasure:
Likelihood: 3 Consequence: 5 Risk: 15
Countermeasure: Security awareness. Knowing the what risks one is subjected to, would increase the overall awareness of the person. Measures such as awareness training and programs should be conducted. Technical measures such as implementing a spam filter would decrease the chances of being subjected to phishing attacks.
After countermeasure:
Likelihood: 1 Consequence: 5 Risk: 5

6.7 Risk nr. 7

Risk description: Loss off access to laptops and its contents due to malicious code.
Threat: Software attack
Vulnerability: Insufficient/absent antivirus, missing backup
Asset: Lilian laptop, Jan laptop, Dora laptop
Incident: Uncle Ismir Özutöck uploads a torrented video game to the children's laptops. The video game file contains malicious code that encrypts the laptops's files when run. By downloading software such as video games from illegitimate sites, the likelihood of getting faulty and/or malicious software increases.
Before countermeasure:
Likelihood: 3 Consequence: 2 Risk: 6
Countermeasure: Invest in proper antivirus software, Don't download torrented video games, Back up important data.
After countermeasure:
Likelihood: 0 Consequence: 1 Risk: 0

6.8 Risk nr. 8

Risk description: Financial loss due to possession of pirated software
Threat: Compromises to intellectual property
Vulnerability: Low security awareness
Assets: Families laptops, smartphones and tablets.
Incident: Increased awareness made by companies to stop illegal downloading and streaming have led to investigations of common torrent sites. Since uncle Ismir Özutöck downloads torrented software and installs it on the families computers the risk of falling victim to compromises to intellectual property. Because of the home office situation, the kids are more likely to request more games and movies form their uncle.
Before countermeasure:

Likelihood: 2 Consequence: 3 Risk: 6
Countermeasure: Stop illegal use of torrent sites for games and software. Increase awareness of policies and rules.
After countermeasure:
Likelihood: 0 Consequence: 3 Risk: 0

6.9 Risk nr. 9

Risk description: Remote Code Execution Attacks due to outdated operating system
Threat: Technological obsolescence
Vulnerability: Lacking awareness, Outdated OS
Assets: Family's laptops, Financial information (12)
Incident: Microsoft released a patch on January 14, 2020 for a vulnerability in Windows 10. The patch affected features in CryptoAPI which is used for digital signatures. According to the NSA the vulnerability opens for remote code execution attacks. Due to COVID-19 the family is spending more time on their computers and might see the update as an hassle as the alert often comes while the users are working or playing games. Continuously delaying the update can leave the laptop vulnerable to known attacks.
Before countermeasure:
Likelihood: 3 Consequence: 3 Risk: 9
Countermeasure: Update operating system regularly.
After countermeasure:
Likelihood: 1 Consequence: 3 Risk: 3

6.10 Risk nr. 10

Risk description: Loss of files due to a ransomware attack
Threat: Human error, Social Engineering
Vulnerability: Low security awareness, no spam filter, no backup
Assets: Parents PC (1), Business information (11), Financial information (12)
Incident: COVID-19 has given threat agents time to increase their efforts when pretexting, phishing and such, in order to install malware. This rapid increase in activity have not been followed by a proportional effort from the public to learn how to defend themselves. Mr. and Mrs. Meiers spend more time online, working from home, and are not protected by their companies networks or policies to the same extent as when they are at work.
Before countermeasure:
Likelihood: 3 Consequence: 5 Risk: 15
Countermeasure: Increased awareness, backup of important information. Invest in proper antivirus software.
After countermeasure:
Likelihood: 1 Consequence: 1 Risk: 1

Table 7 shows the possible effect if the countermeasures are implemented. As shown, risk nr. 2, 7 and 8 have been entirely mitigated.

Table 7: Risk Matrix After Countermeasures

Consequence \ Likelihood	1	2	3	4	5
1	5,10	1			
2		3			
3	9				
4		4			
5	2,6				

7 Risk Management

There are several strategies for treatment of risk. These are (a) to defend by applying countermeasures eliminating or reducing the recidual risk, (b) transference by shifting risk to other areas, (c) mitigation by reducing the damage to assets if an attacker successfully exploits a vulnerability, (d) acceptance where one, after a formal evaluation, chooses to leave an information asset vulnerable to the current risk, and (e) termination which is to remove the asset form the organization's operating environment.

The chosen countermeasures will be classified according to the previously described types.

8 Countermeasures

The following table gives a organized view of all the countermeasures presented in the Risks section. The table describes what area, likelihood or consequence, the countermeasure targets, as well as an estimated cost of each countermeasure.

Table 8: Table of Countermeasures

Nr	Risk nr	Risk description	Current risk	Countermeasure	Strategy	Cost (NOK)	Consequence after	Likelihood after	Risk after
1	1	Loss of internet connectivity	12	LTE backup router	Reduce consequence	800	1	2	2
2	2	Unsafe endpoint configuration and usage	15	Disk encryption	Reduce consequence	500	5	-	5
3	2	Unsafe endpoint configuration and usage	15	Set up Auto-patch	Reduce likelihood	800	5	2	10
4	2	Unsafe endpoint configuration and usage	15	Individual user accounts	Reduce likelihood	0	5	1	5
5	2	Unsafe endpoint configuration and usage	15	Least privilege principle for user rights	Reduce likelihood	0	5	1	5
6	2	Unsafe endpoint configuration and usage	15	Professional IT consultation	Reduce likelihood	1000	5	1	5
7	3, 7, 10	Single point of failure in parent's PC, Ransomware, Financial loss	12, 6, 15	Backup of data to external HDD	Reduce consequence	300	2, 1, 1	2, 0, 1	4, 0, 1

Table 8 Continued from last page

Nr	Risk nr	Risk description	Current risk	Countermeasure	Strategy	Cost (NOK)	Consequence after	Likelihood after	Risk reduction
8	4	Compromised LAN	16	WPA3 and 802.11ac wireless access point	Reduce likelihood	700	4	3	12
9	4	Compromised LAN	16	Network separation	Reduce likelihood	0	4	2	8
10	5	Loss of availability	9	Uninterruptible Power Supply	Reduce consequence	5 000	1	1	1
11	6, 8, 10	Leakage of work credentials, Loss of files	15, 6, 15	Security awareness training	Reduce likelihood	0*	5, 3, 5	1, 1, 1	5, 3, 5
12	7	Ransomware	6	Anti-virus software	Reduce likelihood	300 * 4	2	2	4
13	7, 8	Ransomware, Financial loss	6, 6	Don't download torrented software	Reduce likelihood	0**	2, 3	0, 0	0, 0
15	9	Remote Code Execution attack	9	Update OS regularly	Reduce likelihood	0	3	1	3

* Free online Security Awareness Training
** Cost of not downloading torrented software is zero, but a consequence of this is having to buy the legitimate software.

Figure 1: Risk Coverage

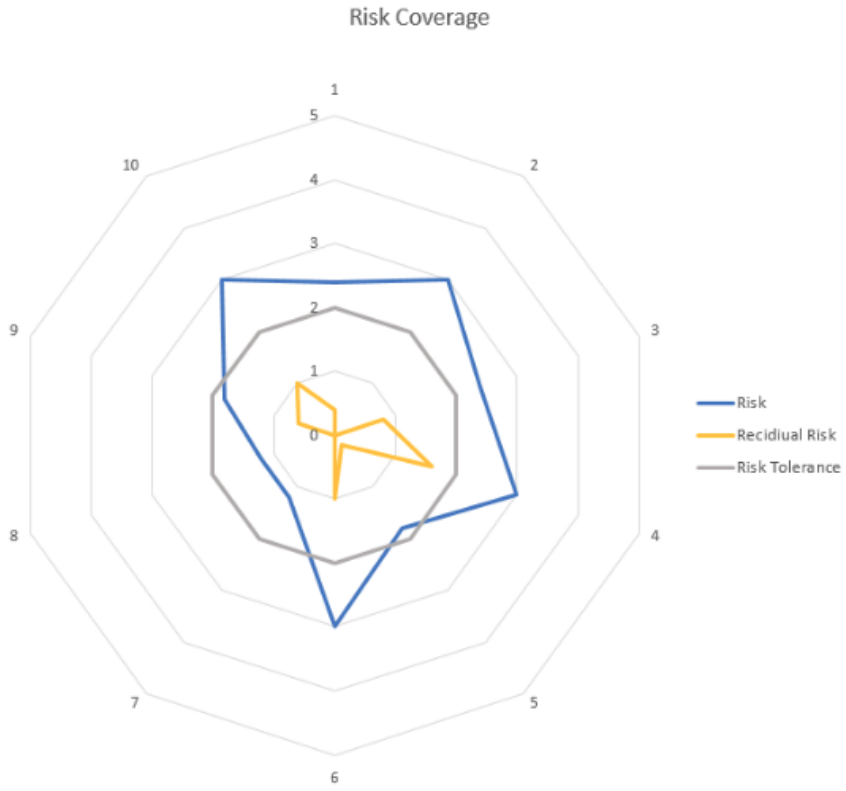


Figure 1 shows the effect of the countermeasures listed in table 8. The residual risk (here highlighted in yellow) is clearly within the risk tolerance of the Meier family, and with the right package of measures the family will be well equipped.

9 Packages of Measures

We have chosen a set of three countermeasure packages. These range from low cost, low human effort to high cost, high effort. Each package tier includes the lower tier packages.

9.1 Package One

Table 9: Package One

Countermeasure Nr	Description	Cost (NOK)
3 (15)	Set up Auto-patch	0
4	Individual user accounts	0
5	Least privilege principle for user rights	0
6	Professional IT consultation	1000
11	Security awareness training	0
13	Don't download torrented software	0
Total cost		1000

9.2 Package Two

Table 10: Package Two

Countermeasure Nr	Description	Cost (NOK)
-	Package one	1000
2	Disk encryption	500
7	Backup of data to external HDD	300
8 (9)	WPA3 and 802.11ac wireless access point (including network separation)	700
12	Anti-virus software	1200
Total cost		3700

9.3 Package Three

Table 11: Package Three

Countermeasure Nr	Description	Cost (NOK)
-	Package two	3700
1	LTE backup router	800
10	Uninterruptible Power Supply	5000
Total cost		9500

Recommendations

Based on the identified assets, threats and vulnerabilities, risk tolerance, and the risk analysis, we recommend package number two. This package has a good balance of cost and risk mitigating countermeasures. It also targets the assets that are high in monetary value, or are deemed irreplaceable.