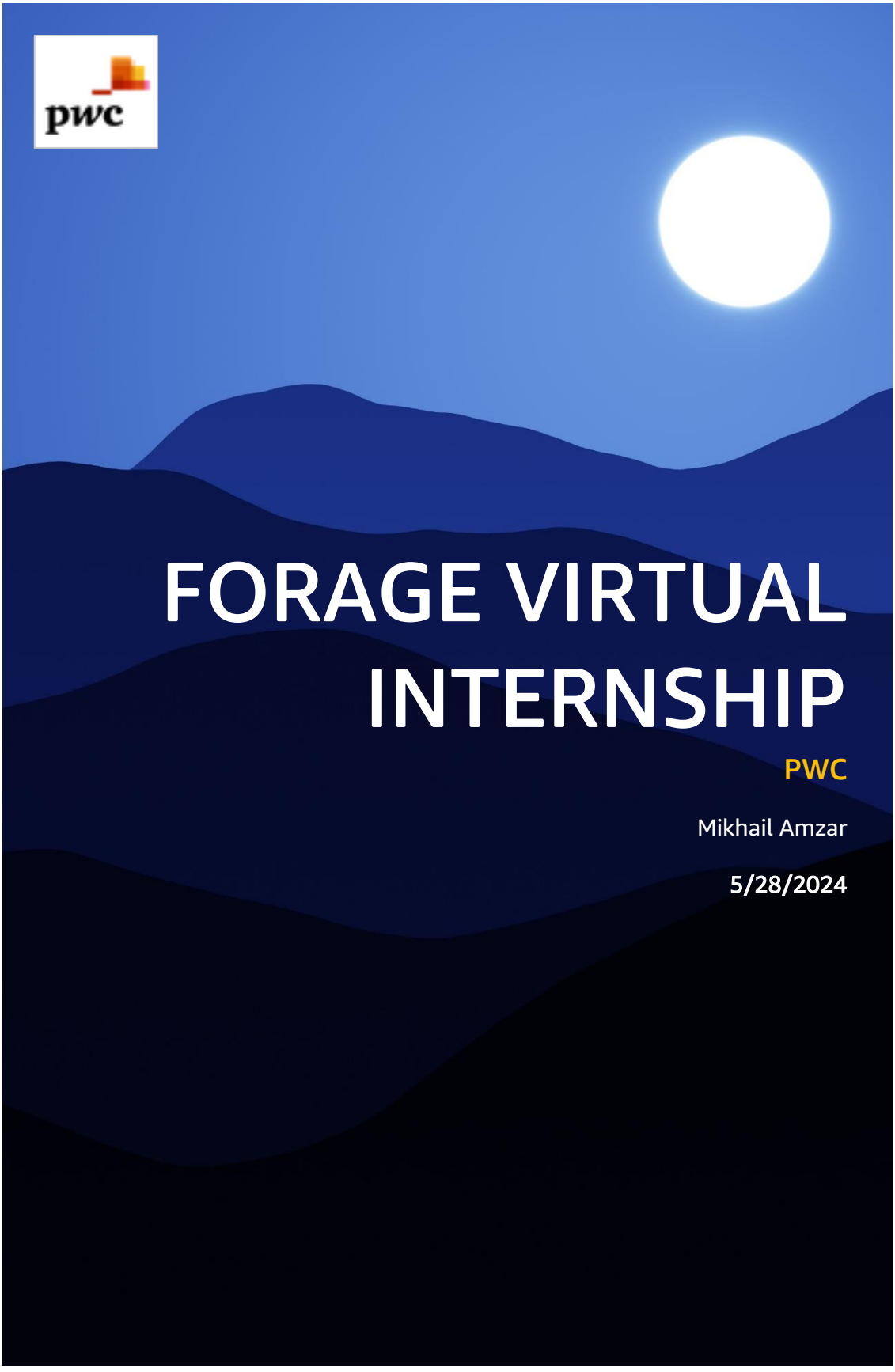


FORAGE VIRTUAL INTERNSHIP

PWC

Mikhail Amzar

5/28/2024

Virtual Internship with PwC .

CONTENTS

TASK 1

OVERVIEW

What you'll learn

- Integrated defense in cybersecurity
- How to recognize information security dangers and biases.
- How to differentiate due care and due diligence in risk management.

What you'll do

- Explain integrated defense to Boldi AG.
- Assess Boldi AG's security practices.
- Describe basic risk limitation options (Deter, Detect, Prevent, Avoid).
- Offer cybersecurity attack response recommendations.

CONTEXT

Client Background: Boldi AG

Boldi AG is a family-owned business in Switzerland with around 90 employees. They are a premium component supplier for the chemical industry, they have 4 people in IT and hire external IT consultants now and then.

Last night the news had a story about a competitor who was hit by a severe ransomware attack. Wake-up call for Boldi AG: their last information risk analysis was conducted in 2014. Management has decided to ask top consultancies to pitch their cybersecurity services.

The team needs your help to prepare a convincing pitch presentation. But first, Stefan, your team leader on this assignment, sets up a call together with you and the Boldi AG management to get more information. They mention they have heard of the concept of layered, integrated defense but would like to know more about how it works.

You're happy to jump in and explain together with Stefan that integrated defense is a universal concept that applies to deliberate attacks and non-intentional threats such as acts of nature. A layered approach to Boldi AG's information security would involve classification from the innermost layer of vital assets, core functions, processes, data, and information to the public-facing boundary points. These interlocking layered strategies, tactical procedures and operational details would reduce the potential impact of information risks.

Then, referring to the recent attack on Boldi AG's competitor, you warn management that there are three dangers/biases that they need to be aware of:

- **Ignoring "blind spots" in their defenses,**
- **Blindly trusting in their systems, processes, and people, plus**
- **Not checking up to see if these are actually working correctly.**

Boldi AG thanks you, and the call ends.

Voicemail from Boldi AG Manager:

"Hi, after considering the dangers you flagged, we've identified a potential blind spot. We have been storing our back-up systems images and database back-ups at an offsite facility that is not monitored 24/7. This means that we cannot exclude with 100% certainty that unauthorized persons could enter that facility. Feel free to call me if you have any questions. Thanks."

What should you respond with?

Remind the management of some security best practices that pertains to what they shared:

- physically protect information systems
- control access by all users.
- control disclosure and disposal of information.
- train all staff regularly.

Refer and adhere to a risk management framework if necessary to get the guidance.

POWERPOINT PRESENTATION (PART 1)

We need to consider the information provided in the voicemail. Please differentiate first **due care** from **due diligence** for information risk management. Afterwards, use your new knowledge to analyze what Boldi AG did wrong. Was it due care, due diligence, or both?

Our Cybersecurity team will include your findings in the final pitch presentation with your detailed explanation.

My answer:

Due Care
Due care is having reasonable processes, policies, and procedures in place to protect all IT assets. Risk management, including assessments and mitigating controls, are all part of due care. Due care is the establishment and continual improvement of your cybersecurity processes, with an emphasis on risk mitigation and control monitoring. The broad scope of this term means it catches **most** of your cybersecurity practices.
Exm: • Proper Standards, Policies, Procedures (NIST CSF or ISO 27001) • Cybersecurity Awareness Training • Continuous Controls Monitoring and Refinement

Due Diligence
Due diligence focuses on identifying and mitigating cybersecurity risks invited by any third party you do business with. It requires understanding your vendors' security posture and what might happen if an incident occurs.
Exm: First step in due diligence? Identify all third parties and fourth parties involved in your operations. • Partners, Contractors, SaaS providers, Vendors, Clients, etc. • Who you're working with and who they're working with. Third party Risk Management. • Understand the third party's cybersecurity posture, policies, programs. Having a Security Service Level Agreements (SLAs) to specify obligations and compliance.

In the case of Boldi AG, they are showing a lack of due care. Although they are concerned with keeping backups of their system and database, they do not have proper security posture in place for those critical IT assets.

- The facility is not monitored 24/7.
- Need to have strict and proper physical and digital access control mechanisms in various layers of the facility to guard from unauthorized access.
- Need to keep logs of every entity/person that access the facility or any critical areas.
- Need to deploy physical security measures to deter intruders and provide monitoring capabilities like fences, security cameras, and guards.

POWERPOINT PRESENTATION (PART 2)

Based on the key principles of defense, what basic options does Boldi AG have for limiting or containing damage from risk?

Hint: the abbreviation of the options is **Deter, Detect, Prevent, Avoid**. Please briefly explain each one.

A:

	Description
Deter	Deter potential attackers with credible defensive capabilities.
Detect	Detect attacks as they begin and monitor them as they progress.
Prevent	Consists of actions a program can take to stop or reduce the risks associated with the threats before they even get off the ground.
Avoid	Avoid the attack by effective deterrence, negotiation or by other means

1. **Develop and exercise incident response** and crisis plan that clearly outline how a response should be managed and coordinated. These should be challenged to ensure they are effective in a catastrophic ransomware scenario, where common security and IT tools may be unavailable and recovery efforts may have to be sustained for weeks or months.
2. **Understand where critical data is,** what the implications would be on that data if systems were unavailable, the regulatory requirements attached to this, and what would need to be recovered to create a 'minimum viable company'.
3. **Ensure that offline backups have been created and validated** for all critical systems and data, including Active Directory, with a well-defined and tested restore procedure.
4. **Build or retain the technical expertise to investigate and respond to the attack** (e.g. investigating the extent of compromise, identifying attacker access, and eradicating the attacker from the environment).

Example of how a professional would do this task:

Integrated Information Defense I

Due care

You take *due care* of those responsibilities, and your investors' expectations and investments, when you set up the business, its business logic and processes, and all of its facilities, equipment, people, and supplies so that it can operate. The burden of due care requires you not only to use common sense, but also to use best practices that are widely known in the marketplace or the domain of your business. Since these represent the lessons learned through the successes or failures of others, you are being careful when you consider these; you are perhaps acting recklessly when you ignore them.

Due diligence

As a business leader, owner, or stakeholder, you exercise *due diligence* by inspecting, auditing, monitoring, and otherwise ensuring that the business processes, people, and systems are working correctly and effectively. This means you must check that those processes and people are doing what they were set up to do and that they are performing these tasks correctly. More than that, you must also verify that they are achieving their share of the business's goals and objectives in efficient and effective ways - in the best ways possible.

Source: Mike Wills, Systems Security Certified Practitioner Official Study Guide
© 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc.

Virtual Case Experience Cybersecurity
PwC

3

Integrated Information Defense II

What did Boldi AG wrong? Was it due care, due diligence or both?
This is a case where due care and due diligence were both failed.

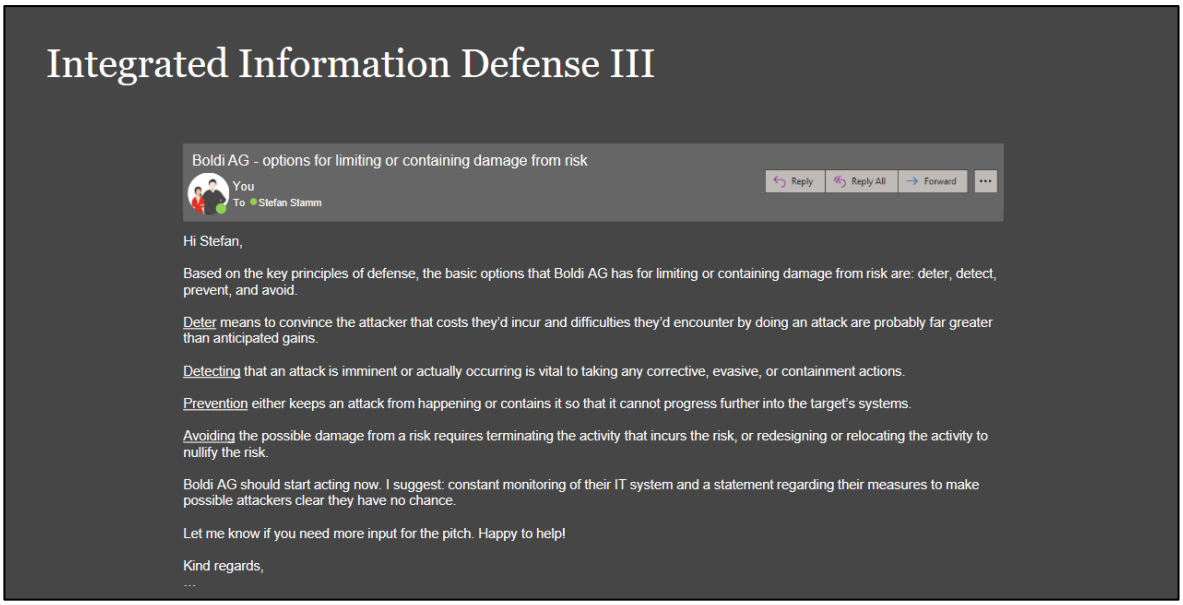
Due care requires
- identifying information risks to high-priority goals, objectives, processes, or assets;
- implementing controls, countermeasures, or strategies to limit their possible impacts;
- and operating those controls (and the systems themselves) in prudent and responsible ways.

Here, the information risks were obviously not identified.

Due diligence requires
- ongoing monitoring of these controls as well as periodic verification that they still work correctly and that new vulnerabilities or threats,
- changes in business needs, or changes in the underlying systems have not broken some of these risk control measures.

Here, there were no controls and no periodic verification of them.

Part 2:


Integrated Information Defense III
Boldi AG - options for limiting or containing damage from risk
You
To Stefan Stamm
Reply
Reply All
Forward
Hi Stefan,
Based on the key principles of defense, the basic options that Boldi AG has for limiting or containing damage from risk are: deter, detect, prevent, and avoid.
Deter means to convince the attacker that costs they'd incur and difficulties they'd encounter by doing an attack are probably far greater than anticipated gains.
Detecting that an attack is imminent or actually occurring is vital to taking any corrective, evasive, or containment actions.
Prevention either keeps an attack from happening or contains it so that it cannot progress further into the target's systems.
Avoiding the possible damage from a risk requires terminating the activity that incurs the risk, or redesigning or relocating the activity to nullify the risk.
Boldi AG should start acting now. I suggest: constant monitoring of their IT system and a statement regarding their measures to make possible attackers clear they have no chance.
Let me know if you need more input for the pitch. Happy to help!
Kind regards,
...

TASK 2

OVERVIEW

What you'll learn

- How Boldi AG manages risk.
- How to recognize information security concerns.
- How to differentiate between types of risk assessments.

What you'll do

- Plan interviews with Boldi AG staff to learn about their risk management.
- Identify security issues in Boldi AG's file management.
- Explain quantitative and qualitative risk assessments and their suitability for information security.

CONTEXT

Task background

Our Cybersecurity team gave an excellent presentation. We won the pitch! Now the action starts: Stefan needs to present a risk assessment of Boldi AG to its management, explaining it in detail step by step. But a risk assessment requires lots of work up front.

You are working with Stefan on location at Boldi to learn as much as possible about the company. First, it is critical to establish a common understanding of information risk at Boldi AG. This means learning about the company and its culture.

- What is their risk tolerance?
- How willing are they to accept risk?
- How do they handle changes in processes and systems?

A risk management framework can provide top-down guidance and establish the attitude and mindset to build consensus about risk. It is also important to understand how Boldi AG controls changes in business processes and systems, particularly Information Technology Systems.

Your Task

Create and submit a PowerPoint slide deck for Stefan answering **step 2** and **3**. For the **first step**, use the memo function of your phone and upload a voicemail to complete your task.

1. To learn more about Boldi AG and its culture, you first need to determine who you should talk to at Boldi AG and what the content of these interviews should be. How does your agenda differ based on the audience, e.g. management vs.

engineers? Stefan is currently in a meeting, leave him a voicemail (no longer than 1.5 minutes).

2. Now you are prepared to conduct an information risk impact assessment. In the meantime, you discover that Boldi AG files on paper and the company's cloud-based information systems are inconsistent in format and hard to use for analysis. Plus, there are no controls over who in the company can access these files.

   Does any of this present an information security concern? Please explain your answer in the slide deck. Think of this through the prism of confidentiality, integrity, and availability (CIA) and add slides to your started presentation.

3. After you know enough about Boldi AG, decide what type of risk assessment would be best, a quantitative risk assessment or a qualitative risk assessment. Then explain the difference between quantitative and qualitative assessments. What do you rely on to be able to perform a quantitative assessment? Which method could be more adapted for information security risk assessments?

Quantitative assessment

Quantitative assessments use simple techniques (like counting possible occurrences or estimating how often they might occur) along with estimates of the typical cost of each loss.

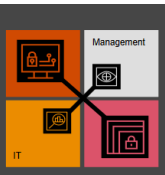
Terms or information that is related to Quantitative Assessment:

SLE	Usually measured in monetary terms, **single loss expectancy (SLE)** is the total cost you can reasonably expect should the risk event occur. Typically expressed in monetary terms, it includes immediate and delayed costs, direct and indirect costs, costs of repairs, and restoration (for hardware, software, facilities, data, people). In some circumstances, it also includes lost opportunity costs, or lost revenues due to customers needing or choosing to go elsewhere.
ARO	**Annual rate of occurrence (ARO)** is an estimate of how often during a single year a particular risk could reasonably be expected to occur. An ARO of 0.5, for example, says that this risk is expected to occur no more often than once every two years.
ALE	**Annual loss expectancy (ALE)** is the total expected losses for a given year and is determined by multiplying the SLE by the ARO.

Safeguard value	This is the estimated cost to implement and operate the chosen risk mitigation control. You cannot know this until Boldi AG's management has chosen a risk control or countermeasure and an implementation plan for it.
How Boldi AG deals with time when its systems, processes, and people are not available to do business (downtime):	
MAO	The **maximum acceptable outage (MAO)** is the maximum time that a business process or task cannot be performed without causing intolerable disruption or damage to the business. It is the time limit to restore all mission-essential systems and services to avoid impact to Boldi AG's mission.
MTTR	The **mean time to repair (MTTR),** or mean time to restore, reflects the average experience in doing whatever it takes to get the failed system, component, or process repaired or replaced.
How long to repair and restore is too long?	
RTO	The **recovery time objective (RTO)** is the amount of time in which system functionality or ability to perform the business process must be back in operation. They are established for each system that supports Boldi AG and its mission. Boldi AG's management may set more aggressive needs for recovery, and if so, they may be spending more than is necessary to achieve these shorter time objectives. All RTOs must be shorter than the MAO that they support; otherwise, the MAO cannot be achieved.
RPO	The **recovery point objective (RPO)** measures the data loss that is tolerable to Boldi AG, typically expressed in terms of how much data needs to be loaded from backup systems in order to bring the operational system back up to where it needs to be. They can be expressed as numbers of transactions or in units of time. Either way, the RPO represents work that has to be accomplished again and is paced by what sort of backup and restore capabilities are in place.

Example answer:

Risk assessment I



What main stakeholders at Boldi AG should we talk to and what should the agenda of these interviews be?

There must be two different approaches in place, one for the management and one for the IT business.

Management and business leaders (top-down approach)

Talk to Boldi AG's management and business leaders (top-down approach). The purpose is to analyse the activity sectors of the company and which disruptive events are feared. Based on those fears, the idea is to analyse which applications are concerned. Here is how the agenda could look like:

1. Understand the main areas of activity of the company and the processes in those activity sectors (for example: logistics, production, procurement, etc.)
2. Have each leader of a main area of activity spontaneously speak up about their 1 to 3 principal security fears
3. Identify the main applications concerned by those fears
4. Proceed with step 2 of the risk assessment

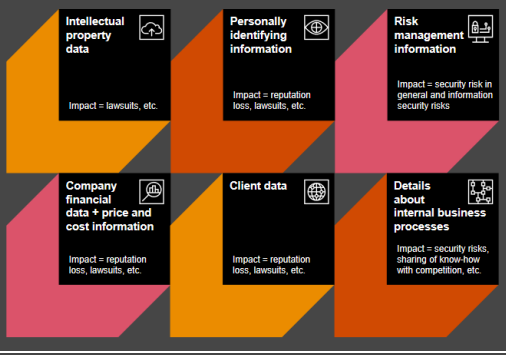
IT department (bottom-up approach)

Talk to Boldi AG's IT department (bottom-up approach). The idea is to analyse the applications and the risks that they are exposed to and to then analyse how those risks would impact the processes of the company's main areas of activity. Here is how the agenda could look like:

1. Identify critical applications for each main area of activity of the company
2. Review documentation of applications
3. Analyse gap between current state of applications and industry standards
4. Filter out the least likely scenarios (focus necessary also for financial reasons as it is not possible to cover all risk)
5. Review applications and most likely scenarios with the IT department

Risk assessment II

What kind of information Boldi AG typically stands to lose with which impact?



Information risk for Boldi AG?

Yes, because the data could represent significant vulnerabilities of company systems, and its inadvertent or deliberate disclosure could be very damaging to the company; because the lack of controls on access and use suggests that data integrity is lacking or cannot be assessed and because conflicting formats and content might make much of the data unusable for analysis and decision making without a lot of effort, impacting whether that data can support decision making in a timely manner. These are the expression of confidentiality, integrity, and availability for these data sets.

C – no controls on access

I – no controls on access

A – inconsistent in format

Risk assessment III

Quantitative Assessments

Quantitative assessments attempt to arithmetically compute values for the probability of occurrence and the single loss expectancy. These assessments typically need significant insight into costs, revenues, usage rates, and many other factors that can help estimate lost opportunities, for example. Quantitative assessments rely on a sufficiently large pool of reliable data.

Qualitative Assessments

Qualitative assessments, by contrast, depend on experienced people to judge the level or extensiveness of a potential impact, as well as its frequency of occurrence. Not all clients have a sufficient amount of reliable data for a quantitative assessment, which is the reason why qualitative assessment might be the better approach for information security risk assessments. It all depends on the client in the end.

Both are valuable and provide important insight; quite often, management and leadership will not have sufficient data to support a quantitative assessment, or enough knowledge and wisdom in an area of operations to make a qualitative judgment.

TASK 3

OVERVIEW

What you'll learn

- Insights into cybersecurity concepts.
- About vulnerability assessment, scanning, and mitigation.
- The significance of an up-to-date Information Systems Security Baseline.

What you'll do

- Research cybersecurity terms.
- Create a graphic explaining key concepts.
- Add notes for the Head of IT Infrastructure.

CONTEXT

Our task essentially:

After **analyzing** the impact of possible risks at Boldi AG, it's time to determine how we can lower the likelihood of these risks through specific cybersecurity measures. We need to prevent these risks from occurring by decreasing each IT system's threat surface and thus decreasing the total threat surface of Boldi AG.

Stefan has met with the Head of IT Infrastructure at Boldi AG to discuss the measures required to follow up on the risk assessment. He acknowledged the need for a detailed **vulnerability review** as this has not been performed for several years. However, he is not convinced that maintaining an up-to-date Information Systems Security Baseline is worth the effort since the system can be scanned with a vulnerability scan anytime. We need to convince him, and you'll help Stefan to create some graphics to do so.

Submit a PowerPoint slide deck to complete this task.
First, you need to learn more about

- **Vulnerability Assessment**
- **Mitigation Planning**
- **Vulnerability Scanning**
- **Hardware and Systems Security**
- **Information Systems Security Baseline**

and why an up-to-date Information System Security Baseline is crucial.
Use your new knowledge to create a graphic using the terms, so we can present it to the Head of IT Infrastructure.
Write notes below your graphic, explaining in your own words the relationship between the terms.

My answer:

Vulnerability Assessment
Vulnerability Assessment is the process of identifying vulnerabilities and determining their severities in an information system in order to decide the remediation or mitigation effort that is needed.
https://www.imperva.com/learn/application-security/vulnerability-assessment/

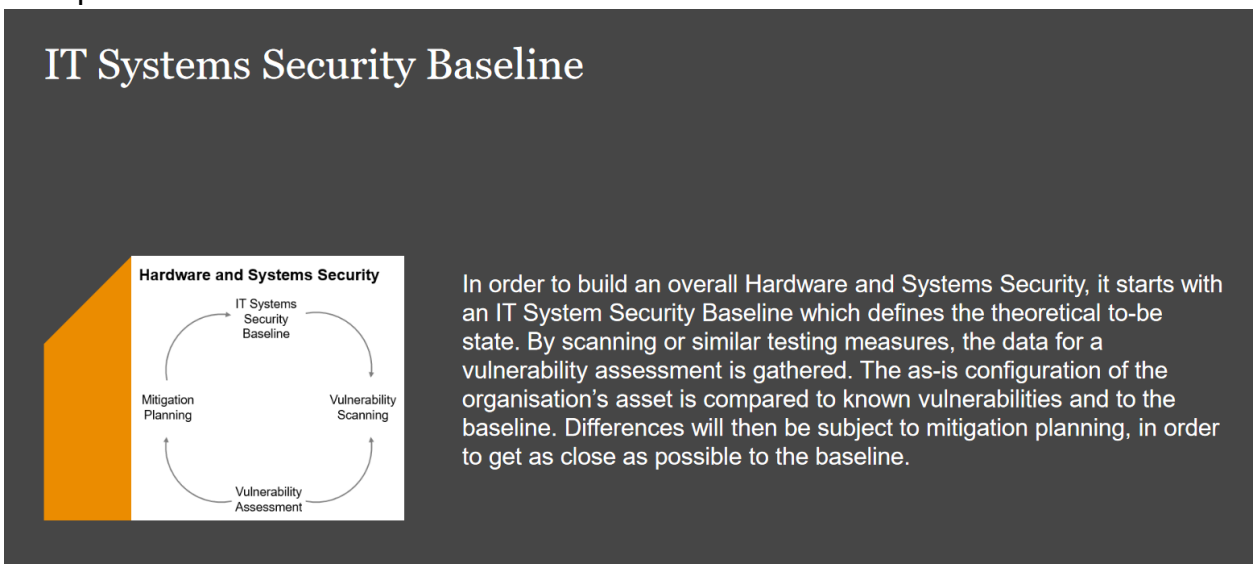
Mitigation Planning
Mitigation Planning is determining mitigation efforts that is needed to address risk and vulnerability, and the steps on how to implement and manage the security controls that will be deployed.

Vulnerability Scanning
Vulnerability Scanning is the process of identifying security weaknesses and flaws in systems and softwares.
https://www.splunk.com/en_us/blog/learn/vulnerability-management.html

Hardware and System Security
Hardware and system security refers to the security that secures machines and computer devices, and systems and software from threats.
https://www.wheelhouse.com/resources/what-is-hardware-and-software-security-a11018

Information Systems Security Baseline
The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.
https://csrc.nist.gov/glossary/term/baseline_security

Example answer:



TASK 4

OVERVIEW

What you'll learn

- The significance of network segmentation for security.
- About firewall configuration for network segmentation.

What you'll do

- Create notes on the role of network segmentation in security.
- Explain firewall configuration using whitelisting and blacklisting concepts for specific firewalls (A, B, C, D).

CONTEXT

The Head of IT Infrastructure of Boldi AG does see the need for network segmentation but cannot follow why a segmented network cannot prevent you from every possible issue. In order to give him and his people a broad understanding of the topic, Stefan organizes a workshop and need your help.

Your task

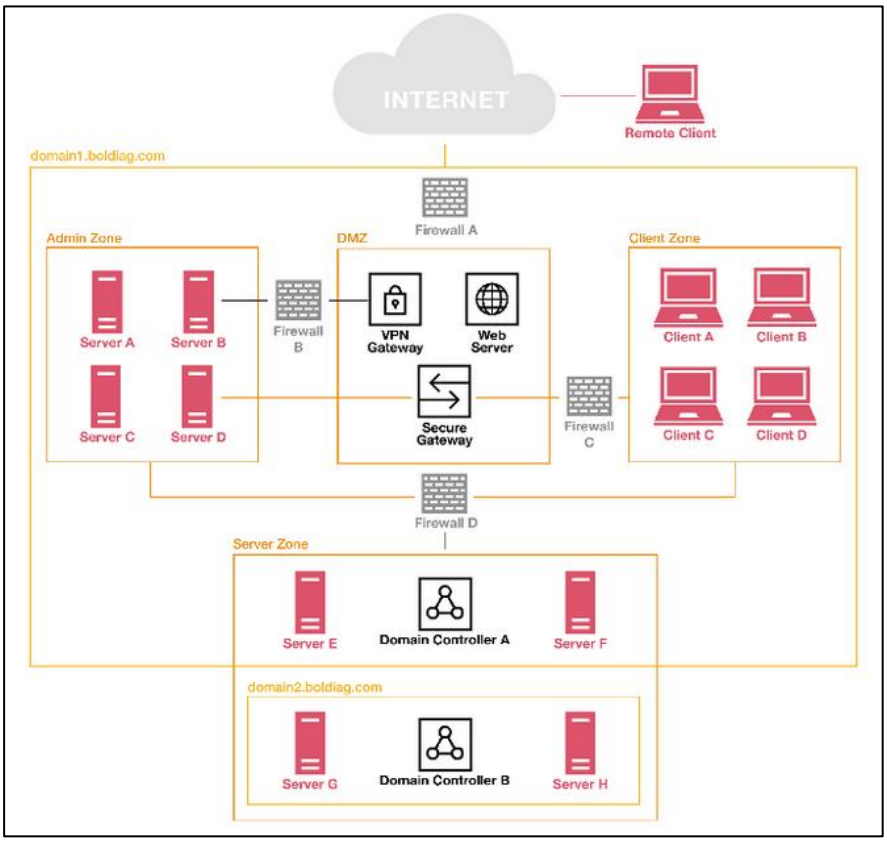
Submit a Microsoft Word document with both parts in it to finalise your work.

Part 1

For Stefans preparation, write in Microsoft Word format detailed notes explaining how segmentation contributes to network security and to the security of the whole organisation. Your notes will help Stefan creating the workshop.

Part 2

The Head of IT Infrastructure of Boldi AG provided Stefan with the following network segmentation:



Domain: A namespace which logically divides an organization's network objects that share the same directory.

Admin Zone: Special purpose server zone, e.g. central logging, Security Information and Event Management (SIEM)

Server Zone: General purpose server zone, e.g. application servers, database servers

Client Zone: General purpose client zone, e.g. user laptops

Regarding network segmentation and trust architectures, the base configuration and maintenance of firewalls is of great importance. There are two approaches to configuring firewalls: whitelisting the good or blacklisting the bad.

Add to your notes how firewalls A, B, C and D at Boldi AG need to be configured using the concepts of whitelisting and blacklisting and why.

My answer:

1. What is the definition of network segmentation?

Network segmentation is the *process* of dividing a large network into smaller networks to improve organization, performance, and security of the network. Limiting access to sensitive data and resources.

2. Benefits of network segmentation, in relation to Boldi AG's operation.

Better network performance for internal operations.

By doing segmentation, you reduce the amount of network congestions overall and network traffic in specific networks. This will allow for better performance in each network segments and ease users and devices to operate in their respected network.

Containing cyber attacks and limit their damage.

Segmentation prevents cyber-attacks from spreading to other networks by containing them. This protects other networks from the damage.

Protect vulnerable devices and critical points.

Segmentation can secure important devices (servers, databases) used for critical operations from access from unauthorized users. These devices can sometimes have no way of protecting themselves, some may be legacy hardware or running legacy software which lack the needed security protections.

Complying with regulations and reduce compliance scope.

Network segmentation is a regulatory requirement in many regulations, as such performing it make sures your organization follows the industry best practice and laws. It also reduces the scope of your systems, components, and data that will be subjected to *regulatory requirements* and *audit processes*.

3. Configuration of firewalls using whitelisting and blacklisting

Difference between whitelisting and blacklisting

Whitelisting	**Blacklisting**
In a whitelist configuration, the network administrator defines the list of approved entities that are **authorized** to access a system, network, or data. The entities could be: • Users • Websites • Email domains • Systems • Apps • Ip addresses	In a blacklist configuration, the network administrator defines a list of entities that are **not authorized** to access a system, network, or data because they are considered or known to be a threat/malicious. The entities could be: • Users • Websites • Email domains • Systems • Apps • Ip addresses

Firewall A: Blacklisting

This firewall is deployed to protect incoming traffic to the out facing server in the DMZ such as the web server from the external internet. Blacklisting allows any users from any source that legitimately want to see the webserver while still blocking known malicious threats, IP address and domain.

Firewall B: Whitelisting

Admin Zone houses special purpose servers that oversee the clients with logging and security monitoring functions. Access to this zone should be secured to protect against any threats from the DMZ. Whitelisting will allow for only trusted and approved clients trying to connect via the VPN gateway while blocking anything else that is not on the list.

Firewall C: Whitelisting

Only approve authorized applications or users from the Client zone to have access to Admin Zone. Deny any devices that are not authorized or have privileged access to Admin Zone servers to reduce risk of intrusion from compromised clients.

Firewall D: Blacklisting

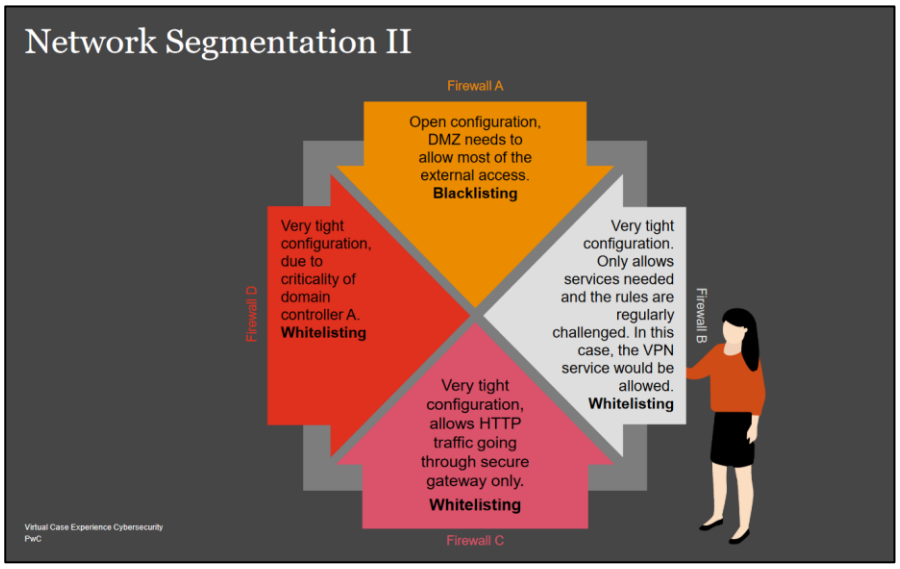
Server Zone will get accessed frequently as it's used by employees and get monitored by Admin Zone. Blacklisting allows access for any entities as long as it's not listed in the blacklist. This will ease operations for internal departments using the servers in that zone.

Pro answer:

Network Segmentation I

The **network segmentation** not only logically groups cohesive systems into one zone but also creates secure passages between them. Every internal firewall works as check point, where a packet is challenged for its legitimacy which makes lateral movement much harder. The current trend is going more and more into a micro-segmentation of networks where the zones are broken down as far as it makes sense. It is also called a Zero Trust Architecture, because at every internal firewall the traffic is verified and not blindly trusted just because it's internal.

However, the firewalls allow for the configured protocols to pass through to the next zone. If for example the Domain Controller A was compromised, the attacker could use whitelisted, standard protocols to compromise more servers with very few indicators.



CONCLUSION

PwC Switzerland Cybersecurity Job Simulation on Forage - June 2024

- Completed a job simulation involving cybersecurity for PwC Digital Intelligence, gaining experience in understanding and explaining the concept of integrated defense.
- Developed expertise in integrated defense strategies and their application in real-world scenarios.
- Conducted risk assessments and formulated security recommendations for a client.
- Demonstrated proficiency in cybersecurity terminology, network segmentation, and firewall configuration.

“Why are you interested in this role?”

I recently participated in PwC's job simulation on the Forage platform, and it was incredibly useful to understand what it might be like to participate on a cybersecurity team at PwC. I worked on a project aiming to enhance cybersecurity measures. I practiced conducting risk assessments and recommending security strategy options in a real-world context. Doing this program confirmed that I really enjoy working on cybersecurity and mitigating risks, and I'm excited to apply these skills to PwC's cybersecurity team.