

PwC Switzerland Cybersecurity Program

Table of Contents

PwC Switzerland Cybersecurity Program.....	1
Table of Contents.....	1
Program Overview.....	1
Task 1: Integrated Information Defense.....	3
Scenario.....	3
Service Proposal Presentation for Boldi AG.....	5
Boldi AG: Risk Management and Defense Strategy Presentation.....	6
Task 2: Cybersecurity Risk Assessment.....	10
Scenario.....	10
Boldi AG Risk Assessment.....	11
Information Risk Impact Assessment Presentation.....	12
Recommended Risk Assessment Presentation.....	16
Task 3: IT System Security Baseline.....	18
Scenario.....	18
Information Systems Security Baseline Presentation.....	19
Task 4: Network Segmentation.....	23
Scenario.....	23
Boldi AG Network Segmentation Report.....	24
Personal Reflection.....	26
Certificate of Completion.....	27

Program Overview:

Welcome to the PwC Switzerland Cybersecurity Program! We are so excited to have you here!

Are you confident about navigating the cyber landscape safely? Prepared to proactively combat cyberattacks and threats? Wondering how we help build trust in the digital transformation by combining people, technology and business?

Our Job Simulation in Cybersecurity will give you the chance to live our approach: All Eyes on Trust. Help us to build and protect our clients business so they can have the confidence to take the initiative, transform and thrive in an uncertain but highly rewarding environment. And gain insights on how we help our clients work around the risks and proactively combat cyberattacks and threats.

Skills you will learn and practice: Network Security, Firewall Configuration, System Security, Risk Management Frameworks, Principles of Defense, Cause Analysis, Risk Impact Analysis, Presentation

Task One: Integrated Information Defense

It's an urgent pitch presentation. You're on the team.

What you'll learn

- About 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.

Task Two: Cybersecurity Risk Assessment

We won the pitch! Time to get to work.

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.

Task Three: IT System Security Baseline

Prepare a diagram, with explanations.

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.

Task Four: Network Segmentation

Prepare for a workshop on the topic.

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)

Task 1: Integrated Information Defense

Review the scenario below. Then complete the program and activities.

We've been asked to pitch our Cybersecurity services. It's urgent!
Please finish the task in the time given (1 hour).

1. Explain the key principles of defense
2. Help our team prepare the presentation

Here is the background information on your task:

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.

You're about to meet with our Cybersecurity team to set up workflows for preparing the pitch, when you see that a manager at Boldi AG has left you a voicemail message: [voicemail transcript below]

"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 unauthorised persons could enter that facility. Feel free to call me if you have any questions. Thanks."

A bit surprised, you and Stefan call back to remind Boldi AG management of the absolute minimum of information security best practices:

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

To wrap up the call, you explain that in a broader sense information security must be actively managed. A risk management framework can provide top-down guidance to organizations in setting the necessary organizational attitude and mindset.

Here is your task:

Submit a PowerPoint set including both parts below to complete your task.

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 analyse 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.

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.

Before you answer in an email to Stefan (please use one PowerPoint slide of your deck), think about how Boldi AG can react to an attack like the one experienced by their competitor.

Resources for the task:

1. PwC Cybersecurity: Responding to the growing threat of human-operated ransomware attacks
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Responding-to-growing-human-operated-ransomware.pdf>
2. PwC Cybersecurity: Key Principles of Defense
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Key%20Principles%20of%20Defense.pdf>

Service Proposal Presentation for Boldi AG

For this presentation, I worked on developing a comprehensive cybersecurity consulting proposal for Boldi AG. My goal was to address their urgent need for improved security measures by analyzing their current vulnerabilities and recommending both immediate actions and long-term strategies. The first task involved creating a pitch presentation that highlighted the importance of due care and due diligence, identified critical gaps in their security, and proposed solutions based on key principles of defense—Deter, Detect, Prevent, and Avoid. This work set the foundation for helping Boldi AG strengthen their cybersecurity posture and protect their valuable assets.

I also drafted an email response for Stefan, addressing his concerns about Boldi AG's security blind spot. In the email, I provided targeted recommendations that include immediate actions and long-term strategies to mitigate the identified risks and enhance Boldi AG's overall cybersecurity posture.

Subject: Follow-Up on Boldi AG's Security Concerns

Hi Stefan,

Thank you for your voicemail regarding Boldi AG's identified security blind spot at their offsite backup facility. After considering the situation, I've outlined the following recommendations:

1. **Enhance Monitoring (Detect):** Implement 24/7 monitoring at the offsite facility to ensure any unauthorized access is detected and addressed promptly.
2. **Update Security Protocols (Prevent):** Given that Boldi AG's last information risk analysis was conducted in 2014, I strongly recommend an immediate review and update of their security practices, with a focus on securing all data storage locations.
3. **Risk Management Framework (Deter):** To ensure continuous improvement, we should work with Boldi AG to implement a comprehensive risk management framework that will guide ongoing security efforts.
4. **Regular Audits (Avoid):** Introduce regular security audits to identify and mitigate risks proactively, ensuring that vulnerabilities are addressed before they can be exploited.

These steps will help strengthen Boldi AG's defenses and align with the key principles of defense, ultimately reducing the risk of incidents like ransomware attacks. Let's discuss these recommendations in more detail during our next meeting.

Best regards,
Justin Goncalves
PwC Cybersecurity Analyst

See Slideshow Presentation Below

Boldi AG: Risk Management and Defense Strategy Presentation

Boldi AG: Risk Management and Defense Strategy

Justin Goncalves
PwC Cybersecurity Analyst
8/18/2024

Due Care vs. Due Diligence


- **Due Care:** The implementation of security measures to provide reasonable protection for assets
- **Due Diligence:** Continuous monitoring, evaluating, and improving security measures to address evolving risks.

Why are these important?

Asset Protection: Due care ensures fundamental security measures are in place to safeguard critical assets.

Continuous Security: Due diligence involves regular monitoring and updating to adapt to evolving threats.

Trust and Compliance: Both demonstrate a commitment to protecting sensitive data, building trust, and ensuring regulatory compliance.



Boldi AG's Current Risk Environment

Company Overview:

- Boldi AG is a family-owned business in Switzerland with around 90 employees, serving as a premium component supplier for the chemical industry.
- The IT team consists of 4 in-house members, with occasional support from external IT consultants.

Current Concern:

- Recent events have highlighted the need for a comprehensive review of Boldi AG's cybersecurity measures, especially since the last information risk analysis was conducted in 2014.

Identified Risks:

- An unmonitored offsite backup facility has been identified as a potential blind spot, raising concerns about unauthorized access and data security.



Boldi AG's Security Lapse

Lack of **due care**, or **due diligence**?

Boldi AG's offsite backup facility is not monitored 24/7, exposing critical data to potential unauthorized access.

This oversight reflects a failure in due care, with inadequate protective measures for the backup environment, and a lapse in due diligence, as security practices haven't been updated since 2014. These gaps leave Boldi AG vulnerable to threats that could have been prevented with proper protocols and ongoing vigilance.

Defense Strategies: Limiting and Containing Risk

- **Deter:** Implement visible security measures and strong policies to discourage potential attackers.
- **Detect:** Enhance monitoring tools to identify and respond to threats early.
- **Prevent:** Strengthen access controls, regularly update systems, and secure backup environments to block attacks.
- **Avoid:** Eliminate or reduce exposure to risks by discontinuing insecure practices and securing all data storage locations.



Strengthening Boldi AG's Security Posture

Immediate Actions:

- **Enhance Monitoring:** Implement 24/7 monitoring for all backup facilities.
- **Update Protocols:** Review and update security practices immediately.

Long-term Strategy:

- **Risk Management Framework:** Establish a comprehensive framework for ongoing security.
- **Regular Audits:** Conduct continuous security audits to ensure compliance and improvement.

Expected Outcomes:

Implementing these recommendations will significantly enhance Boldi AG's security posture by addressing the key principles of defense. Enhanced monitoring (**Detect**) and updated protocols (**Prevent**) will reduce the likelihood of successful attacks, while a comprehensive risk management framework (**Deter**) and regular audits (**Avoid**) will ensure long-term protection against potential risks, including ransomware. This approach will help safeguard critical assets, maintain compliance, and build stakeholder trust.



Key Takeaways and Next Steps

Key Takeaways:

- **Urgency:** Addressing Boldi AG's cybersecurity gaps is critical to protecting their assets and operations.
- **Recommendations:** Immediate actions include enhanced monitoring and updated security protocols, while long-term strategies focus on risk management and regular audits.
- **Defense Principles:** The proposed measures align with key principles of defense—Deter, Detect, Prevent, and Avoid—to reduce potential risks, including ransomware.

Next Steps:

- **Schedule Follow-Up:** Propose a meeting to discuss the implementation of the recommended actions.
- **Offer Support:** Reiterate your availability for further consultation or to address any additional questions.
- **Implementation Plan:** Begin planning the timeline for rolling out the immediate and long-term cybersecurity strategies.

Task 2: Cybersecurity Risk Assessment

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.

Here is 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 an 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?

Here are some resources to help you:

Use the linked PDF's for helpful guidance on completing your task.

1. PwC Cybersecurity: Qualitative Assessments
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Qualitative%20Assessments.pdf>
2. PwC Cybersecurity: Quantitative Assessments
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Quantitative%20Assessments.pdf>
3. PwC Cybersecurity: Root Cause Analysis
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Root%20Cause%20Analysis.pdf>

Boldi AG Risk Assessment

1. Voicemail for Stefan

In the voicemail, I provided Stefan with an overview of my plan to conduct interviews at Boldi AG, focusing on gathering insights from both management and engineering teams. The goal was to understand their risk tolerance and information security culture to better inform our risk assessment.

“Hi Stefan,

I wanted to update you on the next steps I’m taking to better understand Boldi AG’s risk tolerance and information security culture. I’ll be conducting interviews with both the management and engineering teams to get a well-rounded perspective.

For management, I’ll focus on their overall risk tolerance, how they approach changes in processes and systems, and their strategy for setting the tone in risk management. This will help us gauge how willing they are to accept risk and what their priorities are in terms of information security.

On the engineering side, I’ll be looking into how these changes are implemented, their views on the effectiveness of current security practices, and any technical challenges they face with the existing systems. This will give us insights into any gaps between policy and practice.

I’ll begin scheduling these interviews shortly and will keep you updated with any key findings. Looking forward to discussing our next steps.

Thanks, Stefan.”

[End of Voicemail]

2. Information Risk Impact Assessment

For the slideshow presentation, I conducted a comprehensive information risk impact assessment for Boldi AG, with a focus on evaluating their current data management practices through the lens of the CIA framework—Confidentiality, Integrity, and Availability. By thoroughly examining the existing inconsistencies between paper files and cloud-based systems, as well as the lack of access controls, I identified several critical security risks that could compromise the organization's sensitive information, data accuracy, and operational efficiency.

In response to these findings, I developed a set of targeted, actionable recommendations aimed at mitigating these risks and strengthening Boldi AG's overall security posture. The presentation is designed to provide Boldi AG's management with clear insights into the potential vulnerabilities and offer strategic solutions to ensure long-term data protection, system reliability, and compliance with best practices. This approach not only addresses immediate concerns but also sets the foundation for a more robust and resilient information security framework moving forward.

See Slideshow Presentation Below

Information Risk Impact Assessment Presentation



Boldi AG

Information Risk Impact Assessment

Justin Goncalves
PwC Cybersecurity Analyst
8/18/2024



Objectives



- Identify Information Security Risks
- Evaluate Risks using the C.I.A. Framework
- Recommend Security Enhancements

Identified Security Concerns

Inconsistency Between Paper Files and Cloud-Based Systems:

- Boldi AG's information management is fragmented, with paper files and cloud-based systems storing similar data in different formats. This lack of standardization complicates data retrieval and analysis, potentially leading to errors and inefficiencies in operations.

Lack of Access Controls:

- The absence of strict access controls over both paper and digital records means that any employee or external consultant could access sensitive information without proper authorization. This creates a significant risk of unauthorized access, data breaches, and potential data loss.

Confidentiality Risks

Risk: The lack of access controls over Boldi AG's paper and digital records significantly increases the risk of unauthorized access to sensitive information. This includes proprietary data, client information, and intellectual property, which could be exposed to internal and external threats.

Impact: Unauthorized access to confidential information could lead to severe consequences, including loss of competitive advantage, reputational damage, legal liabilities, and potential regulatory penalties. Protecting the confidentiality of this data is critical to maintaining trust and compliance with industry standards.



Data Integrity Risks

1

Inconsistent Data Management:

Boldi AG's reliance on varying formats across paper and cloud-based systems results in data fragmentation, increasing the risk of errors during data entry, processing, or migration between systems.

2

Increased Error Potential:

The lack of standardized procedures heightens the chance of unintentional data corruption or alteration, which can lead to inaccurate or misleading information within critical systems.

3

Vulnerability to Manipulation:

Without robust controls, there's a greater risk that data could be intentionally altered by malicious actors, undermining the integrity of essential information and leading to faulty decision-making.

4

Need for Integrity Safeguards:

To protect data integrity, Boldi AG must implement standardized data management practices, regular audits, and version control mechanisms. These safeguards are essential to ensuring data accuracy, reliability, and security across all platforms.

Availability Risks

1. Inconsistent Access

The lack of standardized data formats leads to delays in accessing critical information during urgent situations.

2. Risk of Downtime

Without proper access controls, unauthorized users could disrupt systems or cause data loss, leading to operational downtime.

3. Challenges in Data Retrieval

Fragmented storage methods complicate quick data retrieval, hindering timely decision-making and operations.

Security Recommendations

These recommendations aim to strengthen Boldi AG's security by addressing critical vulnerabilities. Implementing these measures will enhance data protection, ensure system reliability, and reduce the risk of unauthorized access. Regular audits and staff training will help maintain these improvements over time.

- 01 | Implement Strict Access Controls
- 02 | Standardize Data Management Practices
- 03 | Enhance Backup and Recovery Systems
- 04 | Conduct Regular Security Audits
- 05 | Provide Ongoing Security Training for Staff



Summary

Boldi AG faces significant risks across three critical areas: **confidentiality**, **integrity**, and **availability**. The absence of access controls heightens the risk of unauthorized access to sensitive information. Inconsistent data formats and procedures increase the likelihood of data corruption or alteration. Additionally, fragmented storage and inconsistent access could delay the retrieval of crucial data. Addressing these risks is essential to maintaining the security and reliability of Boldi AG's operations.

3. Recommended Risk Assessment Method for Boldi AG

For the final part of this task, I had to select the most appropriate risk assessment method for Boldi AG. After evaluating the company's current situation, including the lack of detailed data and the urgency to address security concerns, I recommended a qualitative risk assessment as the best approach. This method allows for a quicker and more adaptable evaluation of risks, enabling Boldi AG to prioritize threats based on expert judgment and take prompt action. To make this decision clear and easy for Stefan, I created a concise slide that directly compares quantitative and qualitative risk assessments, highlighting their differences and explaining why the qualitative approach is more suitable for Boldi AG's needs. This was followed by a recommendation slide that clearly outlines the reasoning behind this choice, ensuring that Stefan can effectively communicate the rationale to the management team.

See Slideshow Presentation Below

Comparing Risk Assessment Methods

Quantitative Risk Assessment:

- **Definition:** Assigns numerical values to risks, using metrics such as cost, probability, and impact to quantify potential losses.
- **Advantages:** Provides precise, data-driven insights that facilitate cost-benefit analysis and informed decision-making.
- **Limitations:** Requires accurate and comprehensive data, can be complex, and may not capture all risk factors.

Qualitative Risk Assessment:

- **Definition:** Evaluates risks based on subjective criteria, categorizing risks into levels such as high, medium, or low.
- **Advantages:** Easier to conduct, does not require precise data, and allows for flexibility in assessing risks based on expert judgment.
- **Limitations:** More subjective, potentially less precise, and may lead to inconsistent assessments.

Recommended Risk Assessment Method

Given Boldi AG's size, the current lack of detailed data, and the immediate need to address security concerns, a **qualitative risk assessment** is the most suitable approach. This method allows for a quicker, more flexible evaluation of risks, relying on expert judgment to categorize and prioritize threats based on their potential impact.

Why?

- Adaptability
- Speed
- Prioritization

Task 3: IT System Security Baseline

After analysing 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.

Here is your task:

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.

Here are some resources to help you:

Use the linked PDF's for helpful guidance on completing your task.

1. PwC Cybersecurity: Qualitative Assessments
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Vulnerability-manageme nt.pdf>

Do you already know about the the terms used above? Start some research if not to find out more. Afterwards, level up by listening to a portion (or all!) of our podcast linked below, as well as read our blog posts to gain more insights about systems security.

Information Systems Security Baseline Presentation

For this task, I focused on creating a comprehensive slideshow that emphasizes the importance of maintaining an up-to-date Information Systems Security Baseline (ISSB) at Boldi AG. I began by introducing the critical cybersecurity concepts, such as Vulnerability Assessment, Vulnerability Scanning, Mitigation Planning, and Hardware and Systems Security, and explained how each of these elements supports the ISSB. Through a detailed graphic and concise explanations, I illustrated the interconnectedness of these components and highlighted why the ISSB serves as the foundation for effective risk management.

In the final slides, I emphasized the necessity of continuous improvement in security practices. By regularly updating the ISSB and integrating proactive measures, Boldi AG can ensure that their IT infrastructure remains resilient against evolving threats. The presentation was designed to not only educate the Head of IT Infrastructure on the importance of the ISSB but also to drive action towards implementing and maintaining these crucial security measures.

See Slideshow Presentation Below

Enhancing Boldi AG's Cybersecurity Posture

The Importance of an Up-to-Date Information Systems Security Baseline

Justin Goncalves

PwC Cybersecurity Analyst
8/18/2024

Objectives

- Review Key Cybersecurity Concepts
- Emphasize the Importance of ISSB
- Drive Continuous Improvement in Security Practices

Introduction to ISSB

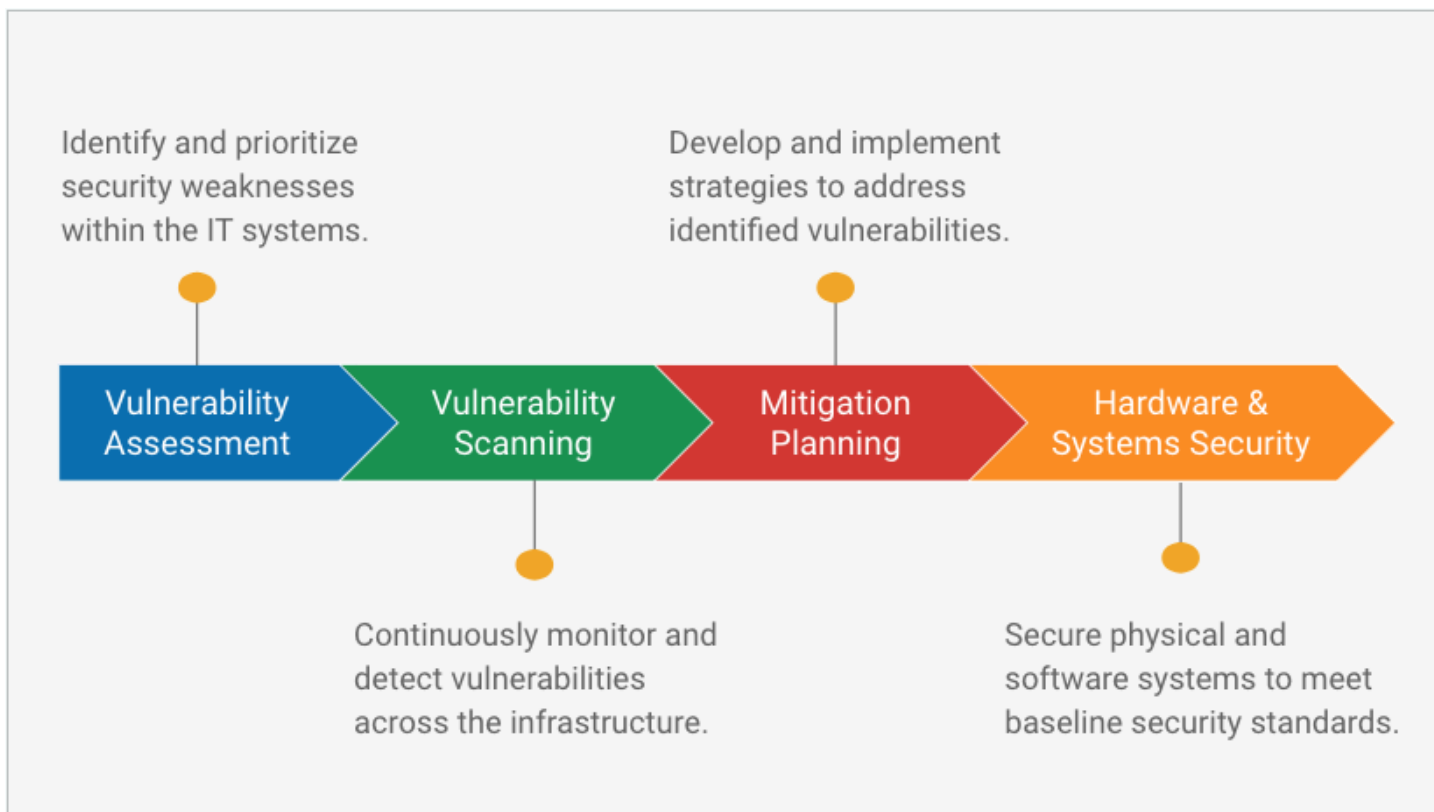
Defining ISSB:

- An **Information Systems Security Baseline** (ISSB) is a set of minimum security standards that all IT systems within an organization must meet. It serves as the foundation for consistent and effective cybersecurity practices across the entire infrastructure.

Purpose of ISSB:

- The ISSB ensures that every system, regardless of its function or location, adheres to a uniform level of security. This baseline is crucial for minimizing vulnerabilities and reducing the overall threat surface.

Next we'll review some key concepts that can be considered to be components that are a part of maintaining an Information Systems Security Baseline.



How are these concepts connected?

Vulnerability Assessment identifies weaknesses, **Vulnerability Scanning** continuously monitors for these risks, **Mitigation Planning** develops strategies to address them, and **Hardware and Systems Security** implements protections. Together, these elements ensure that the ISSB is comprehensive, up-to-date, and effective in minimizing vulnerabilities.

Why is the ISSB Important?

The **ISSB** is essential because it sets the minimum security standards that all systems must meet, providing a consistent framework for managing risks. By keeping the **ISSB** current, Boldi AG can systematically identify, address, and monitor vulnerabilities, ensuring a resilient and secure IT environment.

Continuous Improvement

Maintaining an up-to-date **Information Systems Security Baseline (ISSB)** is not just about meeting current security standards; it's about continuously adapting to new threats and evolving technology. This approach ensures that Boldi AG's IT systems remain resilient against emerging risks.

- **Ongoing Assessments**
 - Regularly conduct vulnerability assessments and scans to keep the ISSB aligned with the latest security requirements.
- **Adapting to New Threats**
 - Update the ISSB and associated security measures as new vulnerabilities are discovered and technology evolves.
- **Embedding Improvement**
 - Integrate continuous improvement into the security culture at Boldi AG, ensuring that all IT practices are regularly reviewed and enhanced.

Task 4: Network Segmentation

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 organises a workshop and need your help.

Here is 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 a network segmentation diagram: (See Resource Number 1)

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.

Here are some resources to help you:

Use the linked PDF's for helpful guidance on completing your task.

1. PwC Cybersecurity: Network Segmentation Flow Boldi AG
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Network%20Segmentation%20Flow.pdf>
2. PwC Cybersecurity: Network Segmentation
<https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Network%20Segmentation.pdf>
3. PwC Cybersecurity: Zero Trust Architecture White Paper
https://cdn.theforage.com/vinternships/companyassets/4sLyCPgmsy8DA6Dh3/Zero%20Trust_White%20Paper.pdf

Boldi AG Network Segmentation Report

Justin Goncalves
PwC Cybersecurity Analyst
8/18/2024

Boldi AG: Enhanced Security through Network Segmentation

Part 1: How Segmentation Contributes to Network Security

Network segmentation is a vital strategy in strengthening the overall security posture of Boldi AG's IT infrastructure. By dividing the network into distinct segments, Boldi AG can effectively control and limit the flow of traffic between different areas of the network, thereby reducing the attack surface and mitigating the risk of unauthorized access.

1. **Limiting the Spread of Attacks:**

Segmenting the network ensures that even if an attacker gains access to one part of the organization's network, they cannot easily move laterally to other critical areas. For example, if a device in the Client Zone is compromised, segmentation prevents the attacker from accessing sensitive servers in the Admin or Server Zones without encountering additional security barriers.

2. **Enhanced Access Control:**

Network segmentation allows for precise access control policies tailored to specific segments. This granularity ensures that users and devices only have access to the resources they need, minimizing the risk of insider threats and unauthorized access.

3. **Improved Monitoring and Detection:**

Segmentation facilitates targeted monitoring of network traffic within specific segments, making it easier to detect and respond to suspicious activities. By focusing on individual segments, security teams can quickly identify anomalies and take swift action to mitigate potential threats.

4. **Protection of Sensitive Data:**

By isolating sensitive data within secure segments, network segmentation adds an extra layer of protection. This ensures that critical data, such as financial information or intellectual property, remains secure even if another segment is compromised.

5. **Compliance with Regulations:**

Many industry standards and regulations mandate the implementation of network segmentation to safeguard sensitive information. By segmenting its network, Boldi AG can meet these compliance requirements, ensuring that sensitive data is securely stored and processed in isolated segments.

Part 2: Configuring Firewalls Using Whitelisting and Blacklisting

Before discussing how the firewalls should be configured, it's essential to understand the two primary approaches to firewall configuration: *whitelisting* and *blacklisting*.

Whitelisting refers to a security approach where only pre-approved, trusted traffic is allowed through the firewall. Any traffic not explicitly approved is blocked by default. This approach is much more restrictive and is typically used in environments where security is paramount, as it ensures that only known, safe connections are allowed.

Blacklisting, on the other hand, is a method where all traffic is allowed by default except for those that are

explicitly blocked. This approach is less restrictive and allows for more flexibility, but it requires careful management and monitoring to ensure that malicious traffic is not inadvertently allowed through.

Effectively configuring firewalls within Boldi AG's network requires a clear understanding of the differences between whitelisting and blacklisting. The decision to use either approach depends on the specific security requirements of each network segment and the type of traffic that flows through them. Firewalls are essential for enforcing network segmentation and safeguarding the network by regulating traffic between these segments. At Boldi AG, the four key firewalls (A, B, C, and D) should be strategically configured using whitelisting and blacklisting principles to ensure strong, comprehensive security.

1. Firewall A (Between Internet and DMZ):

- a. Configuration Approach: Blacklisting
- b. Reasoning: Firewall A manages the traffic between the internet and the DMZ (Demilitarized Zone), a segment of the network that allows limited external access. Given the need for flexibility in accessing public-facing services like a web server, this firewall should primarily use a blacklisting approach. This means that while most external traffic is allowed, any known malicious traffic is blocked. This setup ensures that necessary services are accessible while still providing a basic level of protection against external threats.

2. Firewall B (Between Admin Zone and DMZ):

- a. Configuration Approach: Whitelisting
- b. Reasoning: Firewall B is responsible for protecting the Admin Zone, which contains critical systems that require high security. A whitelisting approach is most appropriate here, meaning that only specific, pre-approved services are allowed to pass through. For example, this might include secure VPN access for remote work. By only permitting explicitly authorized traffic, this firewall minimizes the risk of unauthorized access to sensitive areas of the network.

3. Firewall C (Between Client Zone and DMZ):

- a. Configuration Approach: Whitelisting
- b. Reasoning: Firewall C controls the interaction between the Client Zone, where general workstations are located, and the DMZ. To protect this segment, the firewall should be configured to allow only specific types of secure traffic, such as HTTP traffic passing through a secure gateway. This whitelisting approach ensures that only authorized, safe communications are permitted, reducing the risk of security breaches from less secure areas of the network.

4. Firewall D (Between DMZ and Server Zone):

- a. Configuration Approach: Whitelisting
- b. Reasoning: Firewall D safeguards the Server Zone, which houses the organization's most critical infrastructure, including Domain Controller A. Due to the importance of these systems, this firewall must be configured with a very strict whitelist, allowing only essential, pre-approved traffic. This configuration provides robust protection for the most sensitive parts of the network, ensuring that only trusted and necessary traffic is permitted.

Network segmentation and the strategic configuration of firewalls are essential for maintaining a secure network architecture at Boldi AG. By applying the concepts of whitelisting and blacklisting appropriately, the organization can significantly reduce the risk of unauthorized access, protect sensitive data, and enforce consistent security policies across all network segments.

Personal Reflection

Participating in the PwC Cybersecurity Program has been an invaluable experience, offering practical insights and hands-on experience that closely simulate the responsibilities of a cybersecurity analyst at a prestigious firm like PwC. Throughout the program, I engaged in a variety of tasks that deepened my understanding of key cybersecurity concepts and enhanced my ability to apply these concepts in real-world scenarios.

Each of the four tasks—ranging from conducting a comprehensive risk assessment for Boldi AG to developing network segmentation strategies and firewall configurations—challenged me to think critically and strategically. I gained practical experience with essential skills such as risk analysis, vulnerability management, network security design, and effective communication. These exercises not only reinforced the importance of clear communication, especially when presenting complex security information to stakeholders, but also allowed me to develop and refine technical skills that are critical for a cybersecurity analyst.

Moreover, this program has given me a clearer understanding of the type of work I want to pursue as an aspiring cybersecurity analyst. The tasks mirrored the real-world challenges faced by cybersecurity professionals and provided me with a better idea of how I can apply my skills to protect and secure an organization's IT infrastructure. The practical experience gained through this program has equipped me with the tools and confidence to excel in future roles, ensuring that I can contribute effectively to any organization's security posture.

Overall, the PwC Cybersecurity Program has been a significant step in my professional journey, offering me the opportunity to apply theoretical knowledge in a practical setting and preparing me for a successful career in the ever-evolving field of cybersecurity.

Certificate of Completion



Justin Goncalves

Cybersecurity Job Simulation

Certificate of Completion

August 20th, 2024

Over the period of August 2024, Justin Goncalves has completed practical tasks in:

- Integrated Information Defense Risk Assessment
- IT System Security Baseline Network Segmentation



Natalie Vogel |
Elisabeth Ziller
HC Marketing &
Recruitment Leaders

Tom Brunskill
CEO, Co-Founder of
Forage

Enrollment Verification Code `pjmM9HGbsBqCwYmg` | User Verification Code `rCsmcfq94jpnW64` | Issued by Forage