Reporting

Ricardo Reimao
CYBER SECURITY CONSULTANT

Report – the final product

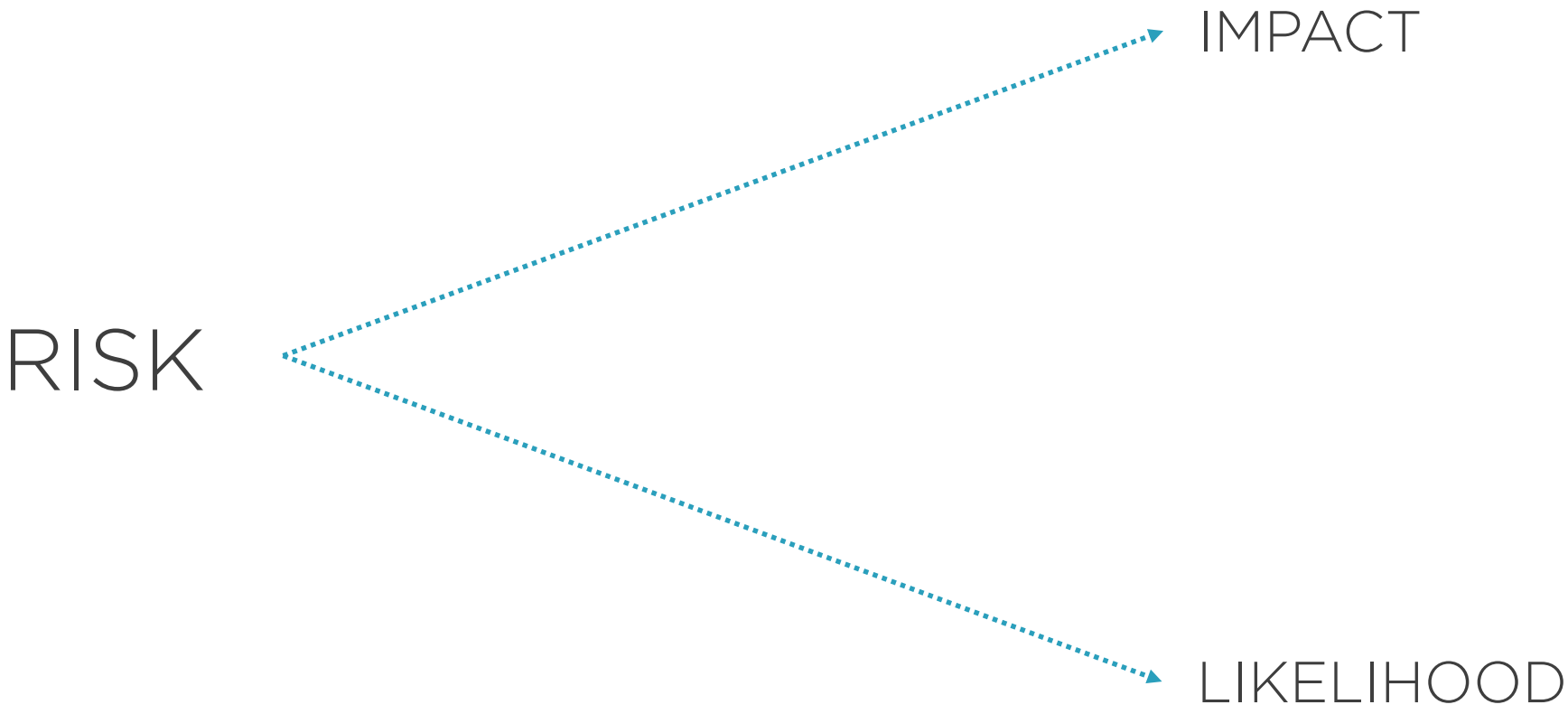
Overview

Understanding risk

Proposing recommendations

What to include in your report

Risk


IMPACT
RISK
LIKELIHOOD

IMPACT

The consequences if attack is successful

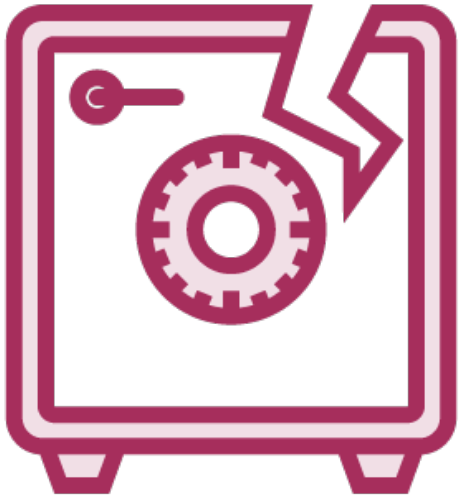
- Which networks can be accessed?
- What is the nature of the attack?
- Which servers would be exposed?
- What kind of data is being transmitted?
- How many users would be impacted?
- What level of access an attacker would have?
- How critical is the environment for the business?

LIKELIHOOD

How likely could someone exploit the vulnerability?

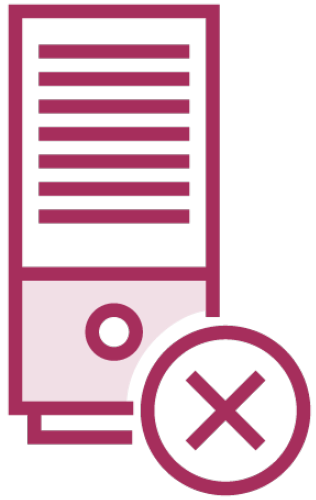
- What is the nature of the attack?
- How long would an attacker take?
- What is the required skill level?
- Where was the network found?
- What is the nature of the company?

Risk



Confidentiality

Integrity



Availability

Recommendations and Reporting

What to Include in a Report

Cover page	Legal information	Executive summary
Technical findings	Recommendations	Appendix

Cover Page

- Project name
- Company logo
- Client logo
- Confidentiality note

Legal Information

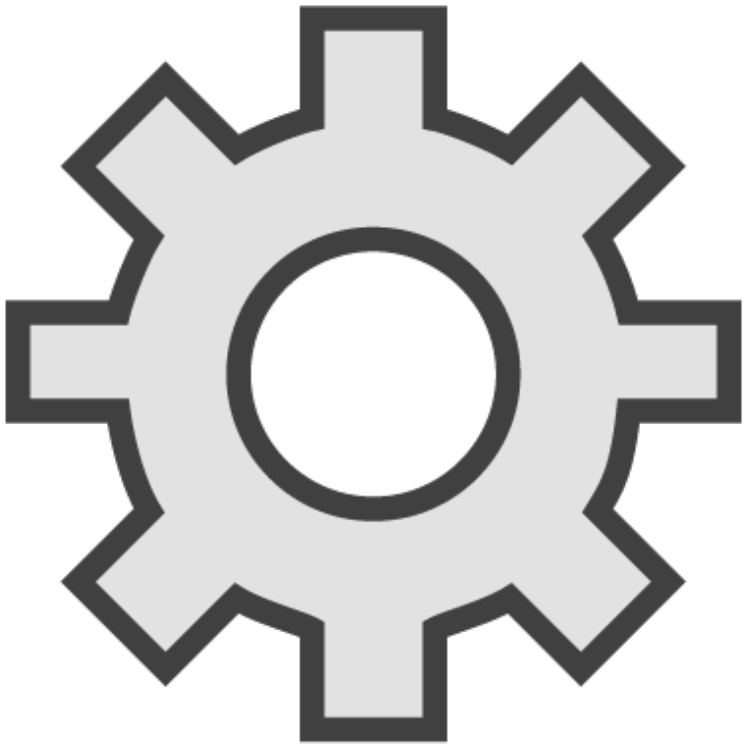
Non-liability statement

Document classification: confidential

Executive Summary

- Brief description of the project
- Scope of the tests
- When the tests were performed
- Summary of findings in a non-tech language
- Risks to confidentiality, integrity, and availability

Technical Findings



Sectioned by vulnerability

- Description of the finding
- Impact
- Likelihood
- Risk
- Recommendation

Weak Wireless Encryption - WEP

Description:
The WEP protocol is considered insecure due to the fact the encryption key can be easily retrieved through analytical attacks. This protocol was discontinued in 2003.
If exploited, this vulnerability could expose internal servers, including the HR and Payroll servers.

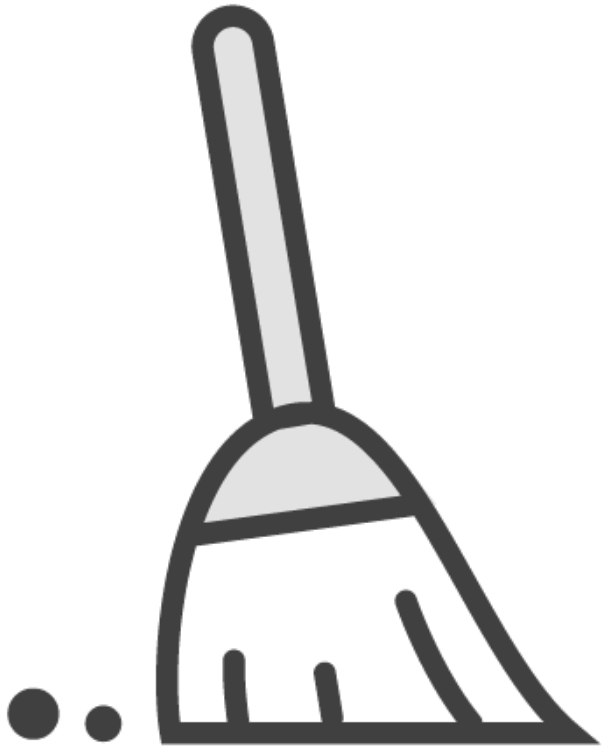
Vulnerable Networks:
GBM Cameras WiFi

Affects:
Confidentiality, Integrity, Availability

Recommendation:
It is recommended to upgrade the wireless protocol to WPA2 with a strong encryption key

Impact: HIGH | Likelihood: HIGH | Risk: HIGH

Proposing Recommendations



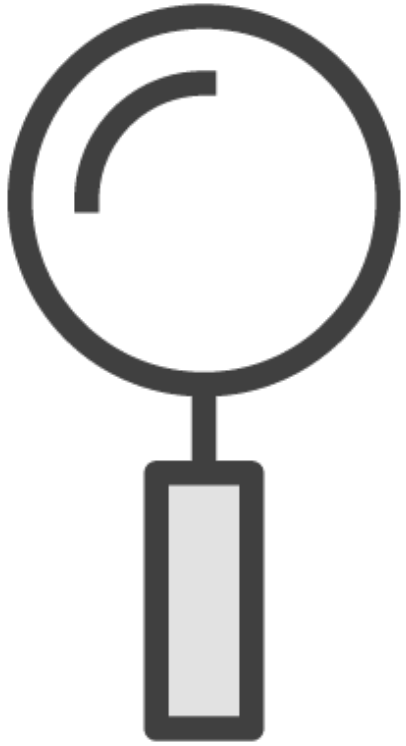
Understand the technical issues

Understand the client environment

Research best practices

Propose improvements

Appendix



Proof of findings

- Screenshots
- Data found (obfuscated)
- Additional information

What NOT to Include in a Report

Sensitive data

- Passwords
- Confidential documents
- Network traffic dumps

Summary

No single answer for reporting

Importance of executive summary

Detailed technical finding

Recommendations based on client environment

What to not include in a report