# Reporting Cyber Risk to Boards

Board Edition

Authors
Freddy Dezeure
George Webster
Lokke Moerel

Reviewers
Alan Kessler
Jamie Hutchinson

Date: 14 March 2022
Version: Final

## Purpose

This paper presents an overview of the recommended approach for Boards when dealing with cyber risk, and of good starting points for Board cyber metrics. It is a complementary paper to one addressed to Chief Information Security Officers (CISOs) on how to best control, measure, and report cyber risks to their Boards and should be read in conjunction with that paper.

## Most Boards are not cyber-aware

Boards have a statutory duty to have proper risk oversight. Cyber risk constitutes by now a critical, potentially material, business risk. However, most Boards are ill-equipped to deal with cyber risks. They consider cyber as too technical, they merely approve resources and delegate the risk.

For traditional business risks, there is an established practice of how to report evidence and an accepted distribution of responsibility/delegation. Regarding cyber risks, there is no current established practice. CISOs struggle to measure the effectiveness of their cybersecurity program and provide reasonable assurance that the residual cyber risk stays below the company risk appetite. Many CISOs do not speak "Board language" and are not invited to report.

In exceptional cases where cyber risk reporting to the Board is taking place, there is a wide variety of methods, tools, and processes in use. Often reporting is about progress in implementation of cyber security measures (measuring *efforts*, often reporting all green), instead of reporting on *risk reduction*.

## It's all about risk

Our cyber environment requires us to make choices in terms of what to protect and how. Perfect security is an illusion and resources are scarce. Assessments and decisions regarding priorities are facilitated and objectivized by using risk assessment. For cyber, we use a model in which risk is composed of three factors **Threat**, **Vulnerability** and **Impact**.

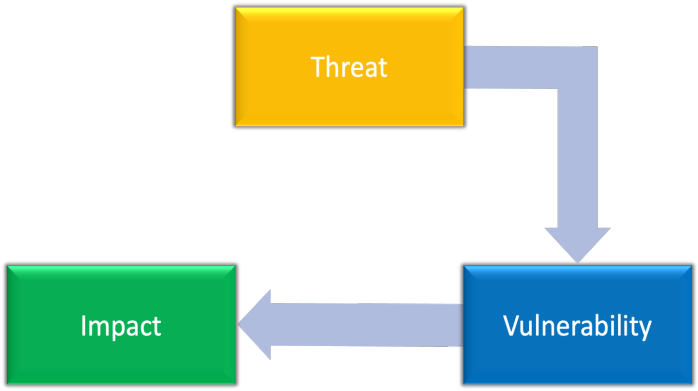



*Figure 1 Risk as a combination of threat, vulnerability and impact*

**Threat** is mostly external to our organization and is closely linked to adversaries which could harm our organization. Identifying our **key adversaries** and their motives is important for prioritization of our mitigation measures. We can observe current threats and try to predict future threats.

The second factor is **Vulnerability**, and this is the one on which we can have the most leverage by designing and implementing controls and mitigation measures. Identifying **key controls**, considering our key assets, and the motivation and methods of our key adversaries is important for prioritization.

In terms of **Impact**, we can think of intellectual property theft, leakage of private data, interruption of service, personal harm, and brand damage. Impact is closely linked to assets. Identifying our **key assets** is important for prioritization.

## Recommended approach for Boards when dealing with cyber risk

### 1. Become cyber-aware and obtain reasonable assurance

Request regular reporting and not only in case of an incident. Foster earnest reporting and not only "all clear". Insist on internal alignment and clear communication channels, with the CISO playing a central role, assuring a professional and independent view on the cyber risk[1].

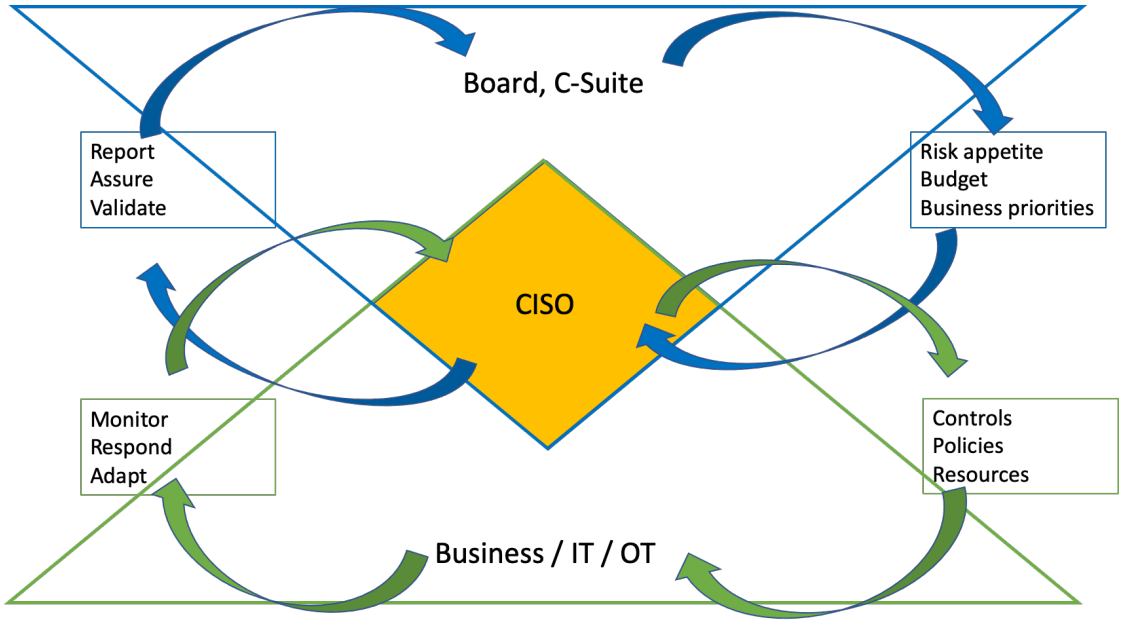



*Figure 2 Information flows and CISO coordination role.*

Reporting cyber risk should serve the purpose of (re)assuring the Board that it is within the risk appetite today and tomorrow:

- Are we good enough?
- Are the resources allocated to cyber appropriate and effective?
- How do we compare with our peers and our sector?

Metrics reported could be combined with context on significant incidents inside and outside the enterprise, on threats and regulatory developments. The CISO should signal any developments that substantially change the situation for better or for worse and propose relevant actions and resources as a consequence.

A sample report to illustrate a possible reporting structure with example figures is attached in the Annex.

[1] Information flows, inspired by NIST Cyber Security Framework https://www.nist.gov/cyberframework

## 2. Ask the right situational questions

Questions for Boards to ask their CISO are very much related to the risk factors.

- Do we have an inventory of key assets?
- What kind of adversaries are targeting us and why?
- Which are our key controls and what is their status?
- Where are the gaps and how do we plan to close them?
- Do we have an incident response / business continuity / resilience plan?
- How much is at risk?
- How do we compare with our peers?

## 3. Control your risks

Cyber security frameworks are a tool to manage cybersecurity risks in a coherent manner and to implement a corporate cyber security strategy. Widely used frameworks are ISO/IEC 27001[2] and NIST's Cyber Security Framework.[3] It does not matter much which framework an organization chooses because there are mappings between them. For Boards it is important though to ensure that there is full internal alignment (between CISO, IT/OT, and risk management) on which framework is used by the organization.

Frameworks typically feature hundreds of controls which are impossible to report at Board level. Key controls therefore need to be identified. A good place to start is the guidance issued by the various national cybersecurity authorities. There is a large degree of overlap between these different sets of baseline guidance and they do provide an excellent, succinct, and practical starting point. Below are the some of the key controls which are invariably included:

- K1: Maintain an up-to-date inventory on all (key) assets and dependencies;
- K2: Produce reliable, valid, safe, and secure backups of key assets;
- K3: Enforce multi-factor authentication wherever possible;
- K4: Limit users' access permissions to what is strictly necessary;
- K5: Identify and perform timely patching of important vulnerabilities;
- K6: Collect and analyze logs of all (key) assets;
- K7: Segment the network to protect key assets;
- K8: Harden internet facing systems;
- K9: Implement an incident response and recovery process;
- K10: Raise user awareness (including Board members).

The mitigation of every control could be measured and reported by a "Coverage Score", combining deployment, operation, and effectiveness of a control.

[2] https://www.iso.org/isoiec-27001-information-security.html
[3] https://www.nist.gov/cyberframework

# Annex: Sample report

## Development of the threat landscape

| Who? | Group / Malware? | Why? | Trend |
|---|---|---|---|
| Adversary 1 | APTX | Adversary known to steal intellectual property in high tech industry. | → |
| Adversary 2 | APTY | State sponsored actor known targeting critical infrastructure | ↗ |
| Adversary 3 | FINX | Ransomware actor increasingly prevalent and sophisticated | ↗ |

## Notable incidents and threat developments

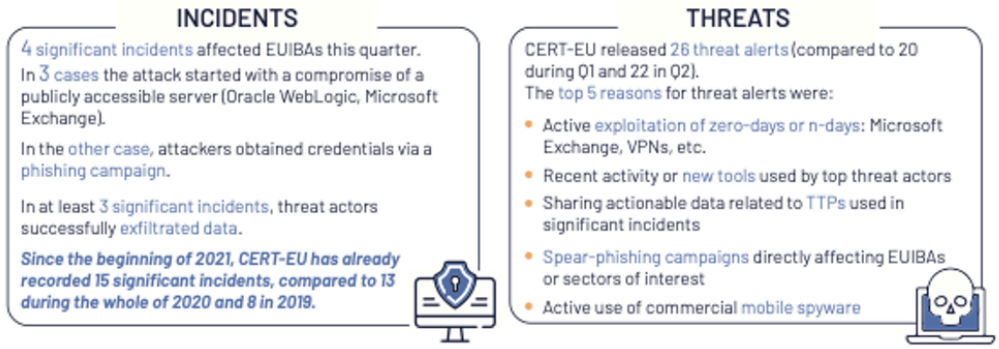
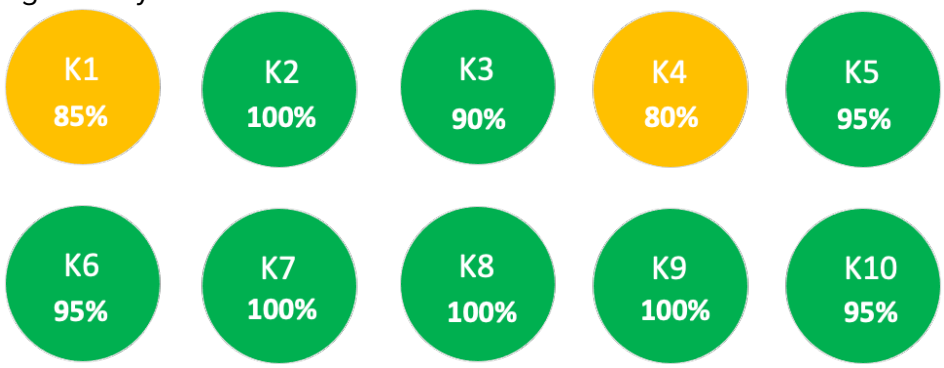
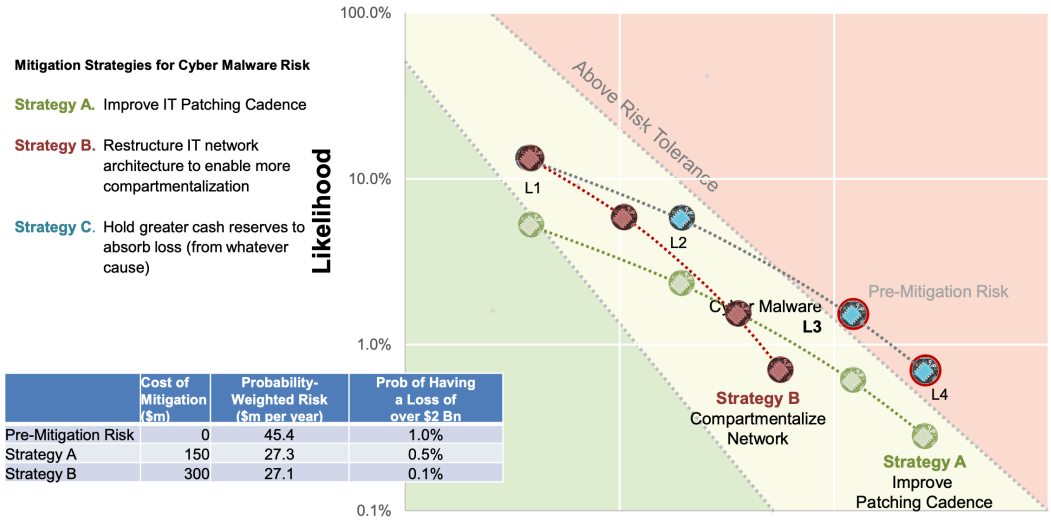



*Figure 3 Credit CERT-EU*

## Coverage of key controls




## Impact of additional measures on mitigation of the cyber risk




| | Cost of Mitigation ($m) | Probability-Weighted Risk ($m per year) | Prob of Having a Loss of over $2 Bn |
|---|---|---|---|
| Pre-Mitigation Risk | 0 | 45.4 | 1.0% |
| Strategy A | 150 | 27.3 | 0.5% |
| Strategy B | 300 | 27.1 | 0.1% |

*Figure 4 Credit Center for Risk Studies, University of Cambridge*