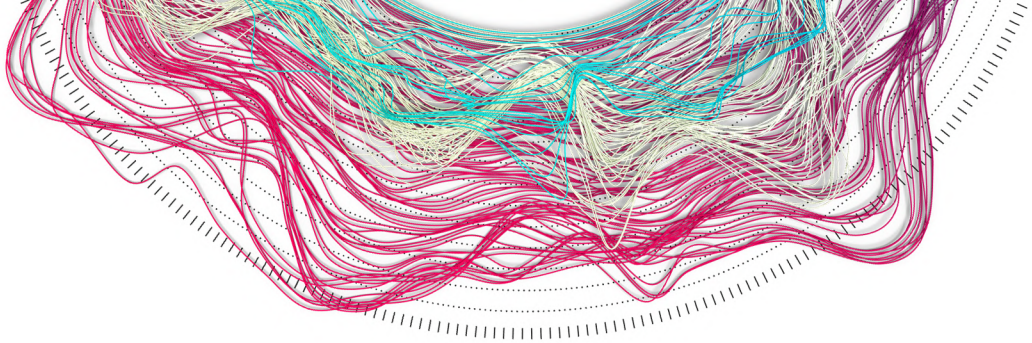
CYBER SECURITY 2024
A GUIDE FOR BOARD MEMBERS



1. CYBER SECURITY: STRATEGIC IMPACT

As reported by Forbes, the #1 pain point for board members and senior executives in 2023 is cyber security: ransomware, bad actors and other threats top their lists of concerns, thanks in part to a proliferation of high-profile hacks over the last decade.

Gartner states that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021. Does your organization have a well-defined attack response strategy before this occurs?

All organizations must implement cyber security measures to protect company and customer data. The Board of Directors and the Executive Management is responsible for ensuring that a viable cyber security infrastructure is in place.

Since the Board of Directors is responsible for ensuring compliance with the applicable laws in business operations, or at least for supervising such compliance in the event of delegation, a violation of data protection law may constitute a breach of duty on the part of the Board of Directors.

Global Data Protection Index, DELL:

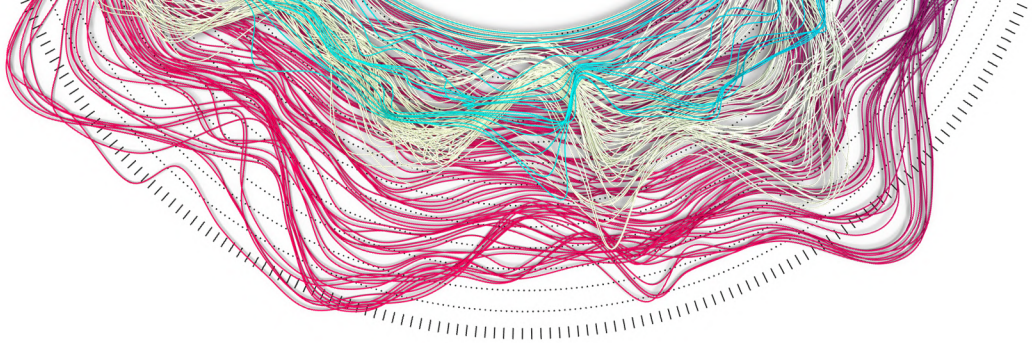
67% of companies see increases in ransomware and malware as significant concerns

91% recognize the importance of cyber resilience at a senior leadership level

> **Truth is, attackers can compromise any organization as it's impossible to stay 100% secure. Thus, it's about how fast you can detect and react to a cyber attack.**
>
> Dr. sc. David Gugelmann
> Co-CEO, Exeon Analytics

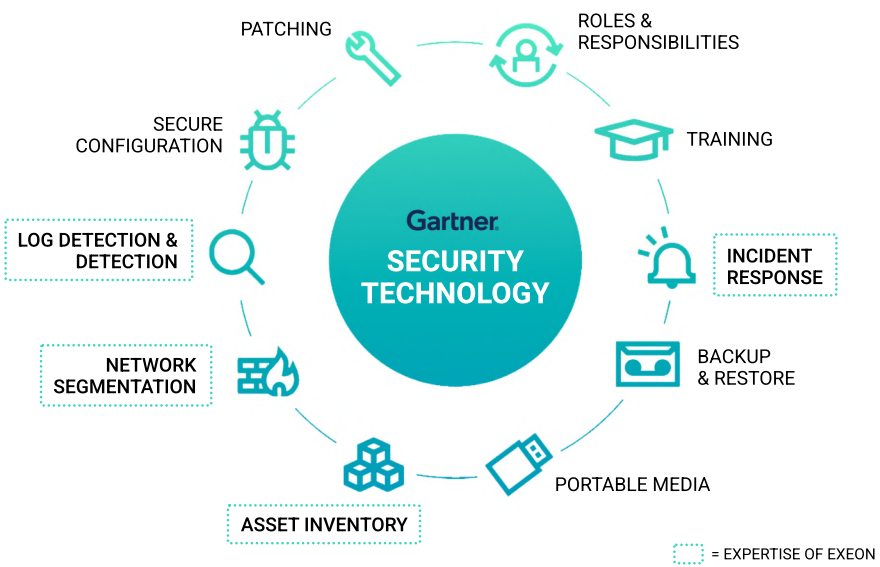
exeon
Smart Cyber Security.

CYBER SECURITY 2024
A GUIDE FOR BOARD MEMBERS



2. OVERVIEW: CYBER SECURITY MEASURES

Gartner recommends that organizations adopt a framework of 10 security controls to improve security posture.



As Board Members are personally liable for cyber security measures, it is elementary to ask and act on specific questions in each of these categories.

IMPLEMENT AND TEST INCIDENT RESPONSE

Do we have a clear incidence management process in place for the four phases of preparation; detection and analysis; containment, eradication and recovery; and post-incident activity?

HAVE AN UP-TO-DATE ASSET INVENTORY

Do we have a continuously updated inventory of all IT equipment and software? Is the inventory taken into account for the analysis of cyber threats?

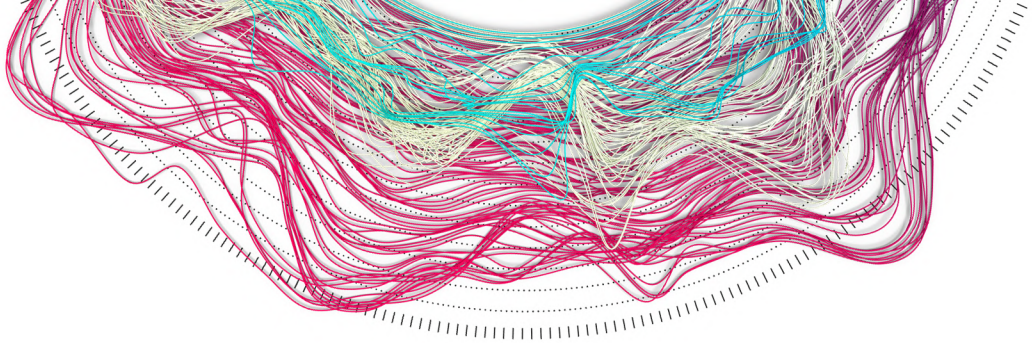
PROPER NETWORK SEGREGATION

Is our network properly segmented and do we continuously monitor the traffic flow to make sure that no unintended communication is taking place?

COLLECT LOGS AND IMPLEMENT REAL-TIME DETECTION

Do we have an automated log collection, analysis and anomaly detection solution in place?

CYBER SECURITY 2024
A GUIDE FOR BOARD MEMBERS



3. NETWORK SECURITY MONITORING

There are many preventative security measures, but what if a hacker has already penetrated the network? Network Security Monitoring allows corporations to understand exactly what is happening in the network, detect anomalies early on and efficiently respond to potential cyber threats.

Cost of a data breach 2022, IBM:

4.35 million
Average total cost of a data breach

24 days
Hacker's time undetected in network

1. Understand your network's data flows
2. Early detection of cyber attacks
3. Efficient handling of security incidents

To avoid downtime, negative reputation and ransomware payments, a network security solution is critical.

NDR solutions support rapid investigation, internal visibility, intelligent response, and improved threat detection across on-premises, cloud and hybrid environments. Detecting attacks at the network layer works extremely well because it is virtually impossible for threat actors to hide their activities.

exeon
Smart Cyber Security.

4. A QUALITY SOLUTION, SWISS-MADE

ExeonTrace visualizes network traffic, detects anomalies and suggests responses completely automatically.

Founded in 2016 and based on over 10 years of award-winning academic research at ETH Zurich, ExeonTrace is used by large organizations in finance, government, logistics and transportation, energy and manufacturing.

A leading Swiss Network Detection and Response platform protecting on-prem and cloud networks through advanced Machine Learning algorithms.

Those who trust ExeonTrace:

PostFinance · SWISS · PLANZER · swisscom · NTT DATA · ORACLE · softwareONE

Gartner Peer Insights™
★★★★★
Near perfection at 4.8/5 stars: contact us for a free consultation today.

contact@exeon.com
+41 44 500 77 21

swiss made software

Exeon headquarters:
Grubenstrasse 12
8045 Zürich