Coloplast's ESG event
22 March 2022

Information security

René Rasmussen
CIO & SVP
Information
Technology

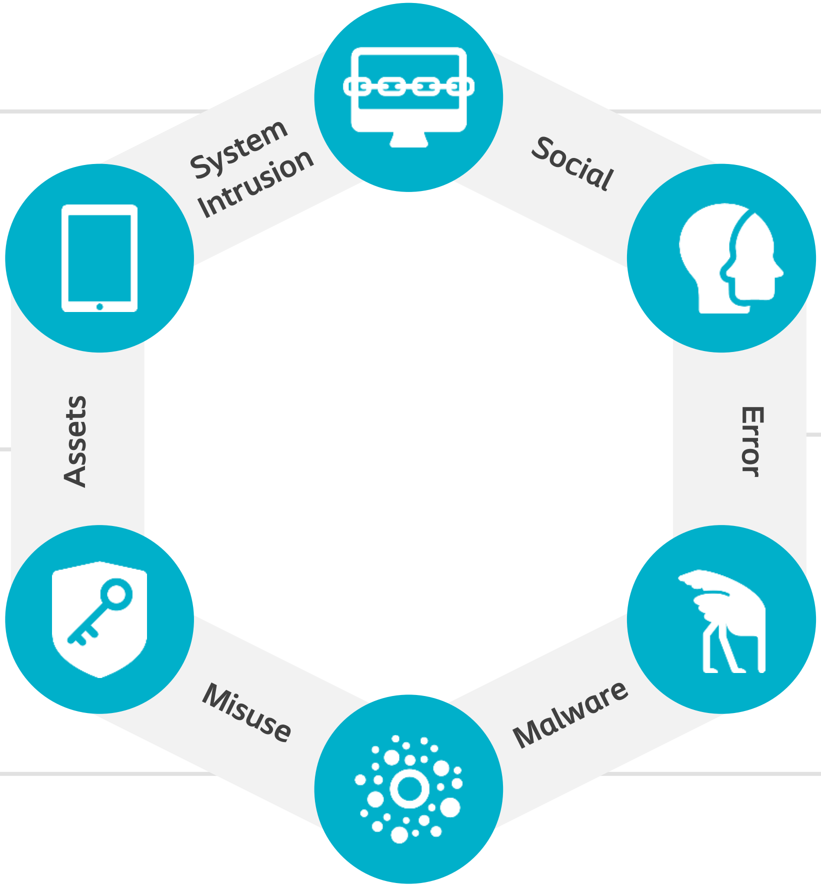
Victor,
Denmark

Making life easier

Ostomy Care | Continence Care | Wound & Skin Care | Interventional Urology | Voice & Respiratory Care

Coloplast

The Information Security threat landscape is constantly evolving



Complex, criminally motivated

- Multiple threat patterns e.g., social attack and malware or social attack and hacking via stolen credentials

Covid changed the way of working

- Expanded 'working' perimeter led to greater dependency on mobile devices

Privilege access abuse

- An insider threat motivated financially or as a grudge

Used for credential stealing

- Threat vector for malware or system intrusion actions
- Phishing via business emails remains the target of choice

Personal / medical data most disclosed

- An unintentional insider threat
- Common error types are database misconfiguration and misdelivery of data

Ransomware—a wide net to maximize profitability

- Criminal actors target ***any*** rather than specific data
- Exfiltration of data becomes a key component

Source: Verizon 2021 Data Breach Investigations Report.

Coloplast is categorized as both healthcare and manufacturing, where a number of key trends have emerged

Industry comparison

✓ Similarities

- Shared threat actor motivation: financial, espionage, and grudge
- Ransomware is a favourite threat pattern used by criminal actors
- Personal identifiable information is the most compromised data type

✗ Differences

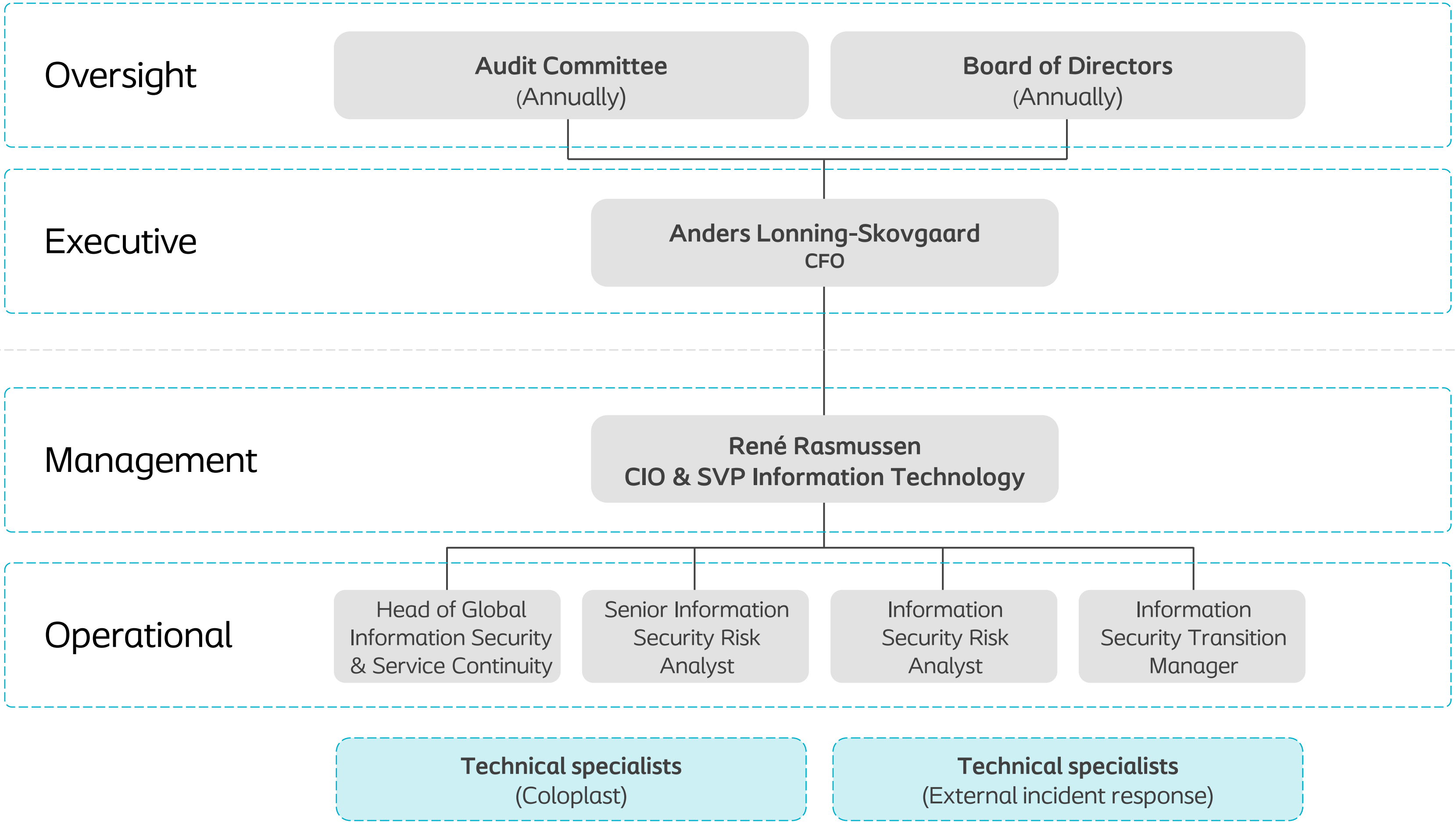
- Basic human error continues to impact the healthcare industry
- Manufacturing breaches are complex and involve multiple threat patterns (social and hacking)

Key takeaways

- Ransomware is by far the greatest potential to cause substantial business disruption
- Unintentional internal threat actions contribute to most data breaches
- Compromise of personal identifiable information exceeds all other data types

Source: Verizon 2021 Data Breach Investigations Report.

At Coloplast the Governance set-up for Information Security has evolved to adapt to the rapidly changing external environment


Oversight
Audit Committee
(Annually)
Board of Directors
(Annually)
Executive
Anders Lonning-Skovgaard
CFO
Management
René Rasmussen
CIO & SVP Information Technology
Operational
Head of Global Information Security & Service Continuity
Senior Information Security Risk Analyst
Information Security Risk Analyst
Information Security Transition Manager
Technical specialists
(Coloplast)
Technical specialists
(External incident response)

Strategy and Governance for Information Security is centred around a risk-based approach

Risk Management

Threats

Objective: Enhance ability to detect, respond & recover

- Physical security perimeter controls
- Technical security controls
- Security Operations Center
- External vulnerability & penetration tests
- IT / OT Network Segregation
- IT Service Continuity

Compliance & Regulations

Objective: Ensure compliance to relevant regulations and laws

- ISO 27001 certification
- ISO 27001 internal audits to certified sites
- Address security requirements in data privacy legislation / national authorities
- Operation of the Information Security Management System

Conduct

Objective: Training and awareness; balanced with the above technical control

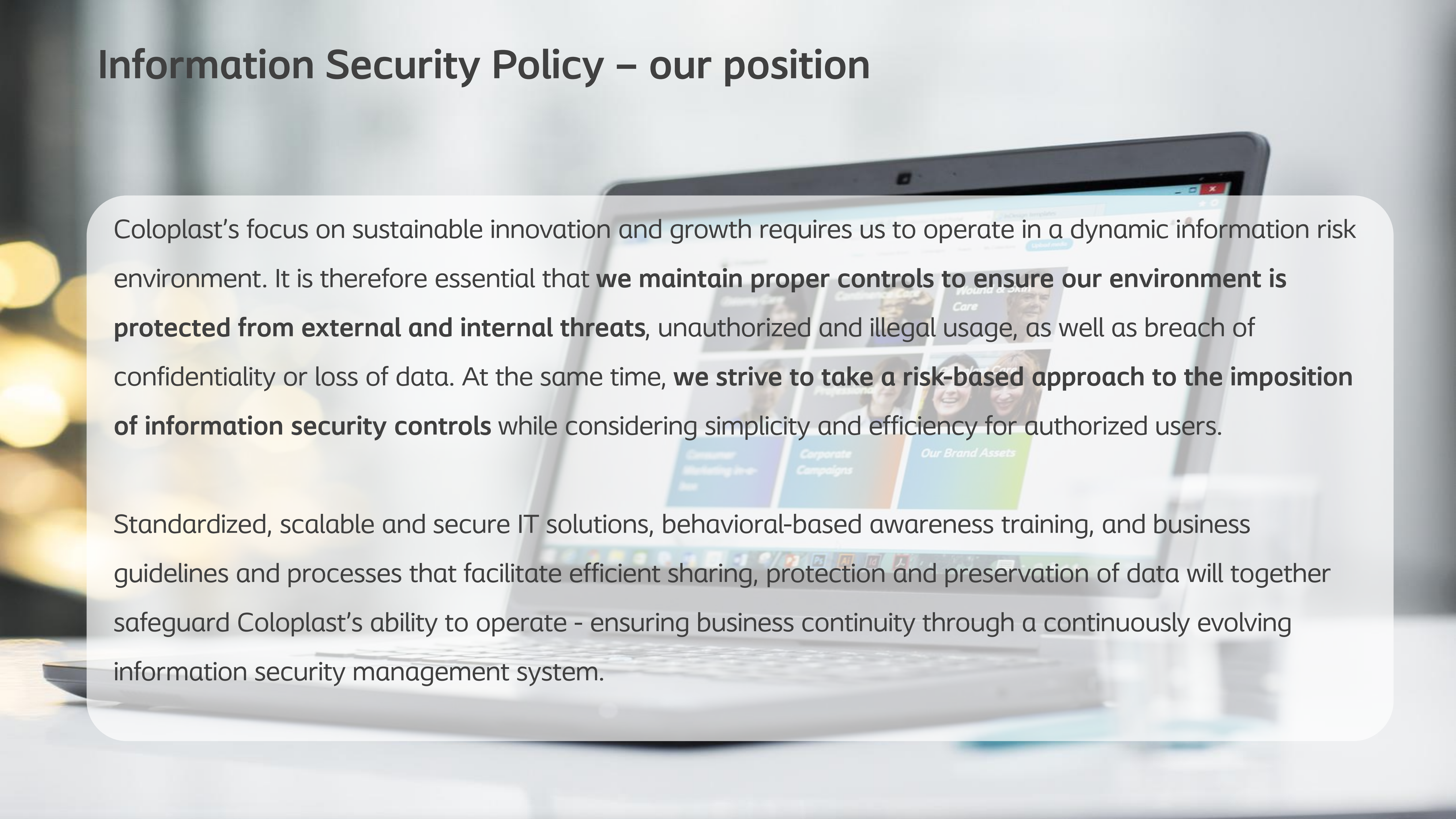
- Global policies and guidelines relating to information security
- Targeted awareness training to all employee categories focusing on user behaviour / habits

Business Interactions & Relations

Objective: Interconnected and interdependent, secure the end2end relationship

- Supplier due diligence (risk profile)
- Externally published Information Security policy
- Annual update to Board of Director & Audit Committee

Information Security Policy – our position



Coloplast’s focus on sustainable innovation and growth requires us to operate in a dynamic information risk environment. It is therefore essential that **we maintain proper controls to ensure our environment is protected from external and internal threats**, unauthorized and illegal usage, as well as breach of confidentiality or loss of data. At the same time, **we strive to take a risk-based approach to the imposition of information security controls** while considering simplicity and efficiency for authorized users.

Standardized, scalable and secure IT solutions, behavioral-based awareness training, and business guidelines and processes that facilitate efficient sharing, protection and preservation of data will together safeguard Coloplast’s ability to operate - ensuring business continuity through a continuously evolving information security management system.