HUGO BOSS

HUGO BOSS

HUGO BOSS

CYBERSECURITY STRATEGY

MAY 2025

HUGO BOSS

WORLDCLASS INFORMATION SECURITY

NO MATTER HOW MUCH WE INVEST – A LARGE SECURITY INCIDENT IS ALWAYS POSSIBLE AND WE NEED TO BE PREPARED

$1,2 Billion

Ransomware payments exceeded in 2024
Repair costs not inculded

124%

Increase in cyberattacks compared to last year

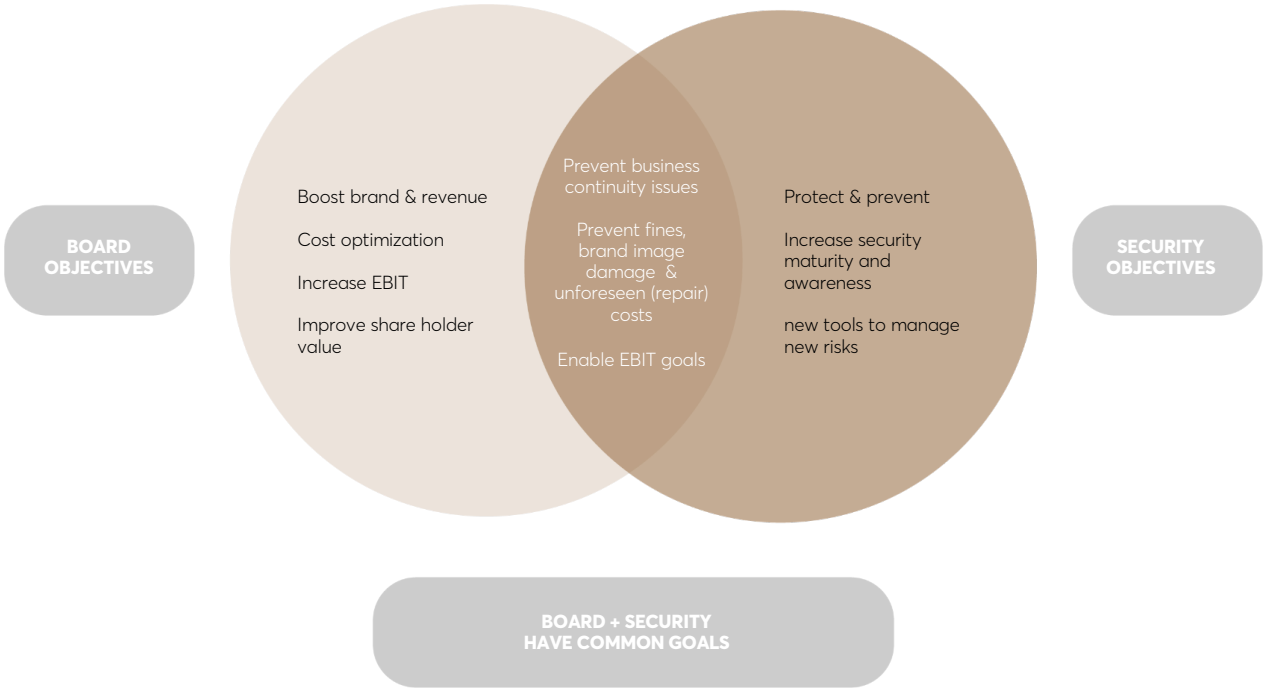
1. Ensuring **resilience** against major attacks
2. Detect threats and attackers **as early as possible**
3. Cybersecurity education for **workforce awareness**
4. Build an **agile security program** to react fast to changing threat landscape

HOT TOPICS
- **Security Operations Centre (SOC)**
- **SIEM and SOAR automation**
- **Threat Intelligence**
- **Security Service Edge**
- **DevSecOps**

EXECUTIVE SUMMARY

HUGO BOSS

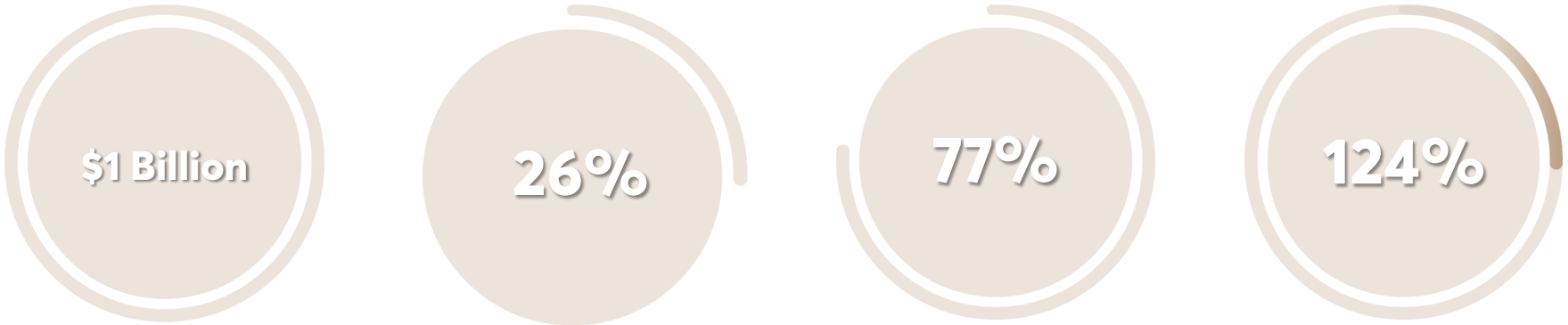
EXECUTIVE ALIGNMENT
HOW BOARD AND CYBERSECURITY MUST WORK TOGETHER



HUGO BOSS prioritizes cybersecurity initiatives using a methodology that considers the impact and likelihood of **risks**, aligning with **business goals** and **regulatory requirements**. This approach ensures strategic investment in resources to maintain and enhance their cybersecurity posture.

HUGO BOSS

THE TOP RISK TO DEAL WITH
RANSOMWARE THREAT LANDSCAPE



Ransomware payments exceeds in 2023
Repair costs not included

Of organization got hit four or more times in 2023

Of cases includes data exfiltration

Increase in Cyberattacks compared to last Y

WE DO EVERYTHING TO PROTECT THE FAMILY

Source: Gartner

HUGO BOSS

WHAT MATTERS TO US – WHAT MUST BE PROTECTED
WE WANT TO KEEP HIGH STANDARDS

NONNEGOTIABLE RISKS

- Devastating cyber attack
- E-com down for more then one week
- Stores offline
- Logistics offline

HIGH / MEDIUM RISKS

- E-Com down for a few days
- Smaller cyber attack on an HB office location
- Data loss / data protection fines
- Izmir production offline

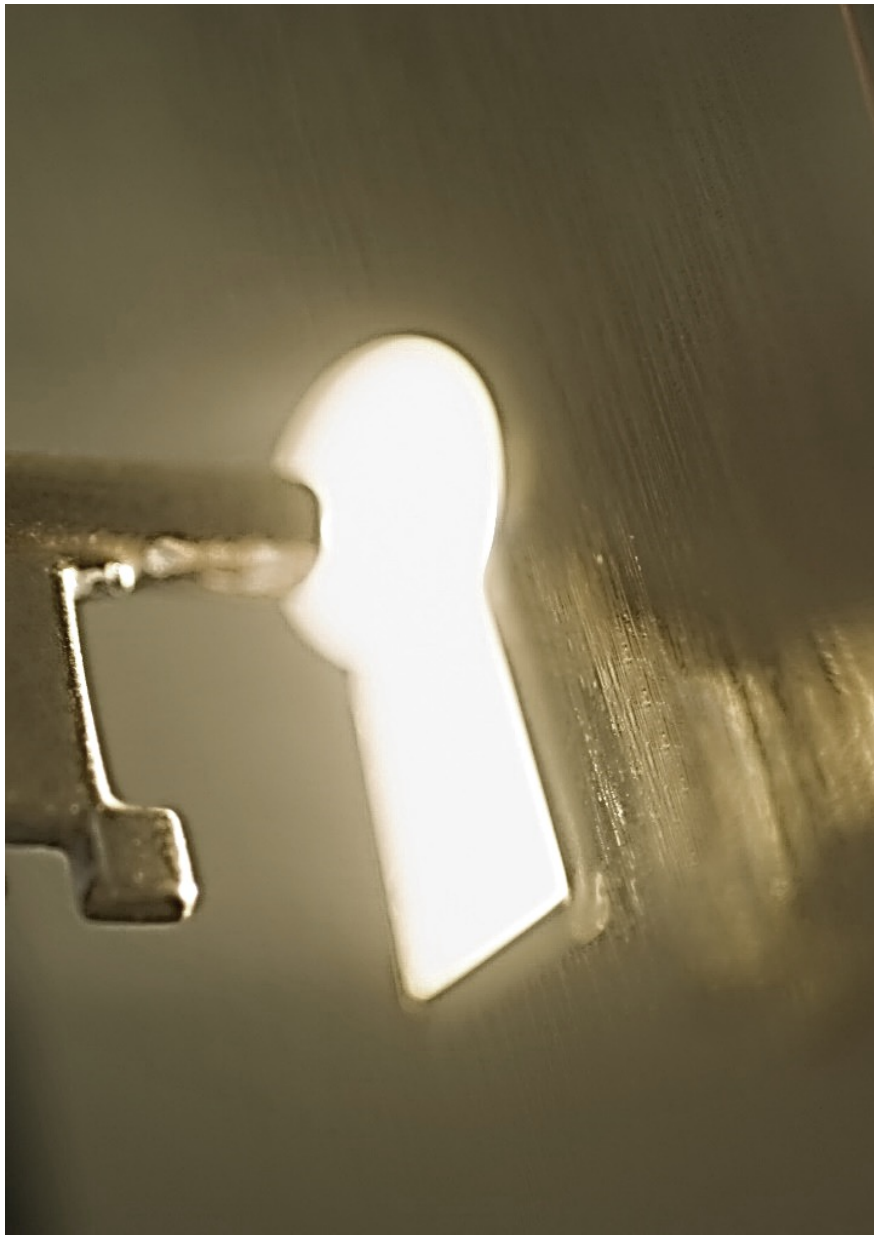
COMPLIANCE RISKS

- ISO certification
- Reputational risks
- Cyber Insurance
- Fines for noncompliance

CYBER SECURITY VISION, MISSION
CORE VALUES

Information technology is an important resource in all business units. Customers but also employees, suppliers, business partners and shareholders trust that their data and information are secure at HUGO BOSS. To justify this trust, the integrity, availability and confidentiality of data and information must be sufficiently ensured.

VISION	**BECOME THE MOST TRUSTED FASHION ENTERPRISE BUSINESS WORLDWIDE**
MISSION	**WE LOVE SECURITY, WE WIN TRUST**
AMBITION	**EMPHASISE TRUST – PROTECT THE BRAND – CREATE RELIABLE SYSTEMS**



HUGO BOSS

THE GUIDING PRINCIPLES FOR CYBERSECURITY

- PROACTIVE DEFENSE THROUGH CONTINUOUS IMPROVEMENT – CONFIDENTIALITY INTEGRITY AND AVAILABILITY
- COLLABORATION – WITHIN THE COMPANY AND PARTNERS TO ENSURE SECURITY - ONLY AS A TEAM YOU CAN WIN
- AWARENESS AND TRAINING - BUILD THE FOUNDATION
- COMPLIANCE TO REGULATORY REQUIREMENTS ARE KEY
- RISK MANAGEMENT - BUILDS THE BASIS FOR OUR ACTIONS
- CYBER RESILIENCE - KEEPS SYSTEMS AND SERVICES RUNNING BUILDING CONTINUITY PLANS
- INDUSTRY STANDARDS LIKE NIST & ISO27000 FRAMEWORK HELP US TO ACHIEVE OUR GOALS IN THE MOST COST EFFECTIVE WAY

KEY RISKS: IDENTIFYING AND MITIGATING CRITICAL THREATS

Risk Category	Description	Mitigation Strategy
Data Breaches	Unauthorized access to sensitive data	Implement robust encryption and access controls
Ransomware Attacks	Malware that encrypts data for ransom	Regular backups and employee training
Insider Threats	Malicious actions by employees or contractors	Implement zero trust architecture and monitoring
Supply Chain Attacks	Compromises through third-party vendors	Rigorous vendor risk assessment and management
Cloud Security Vulnerabilities	Risks associated with cloud infrastructure	Implement cloud-native security tools and practices

HUGO BOSS

STRATEGIC TRANSFORMATION
HOW SECURITY CAN HELP TO GENERATE VALUE

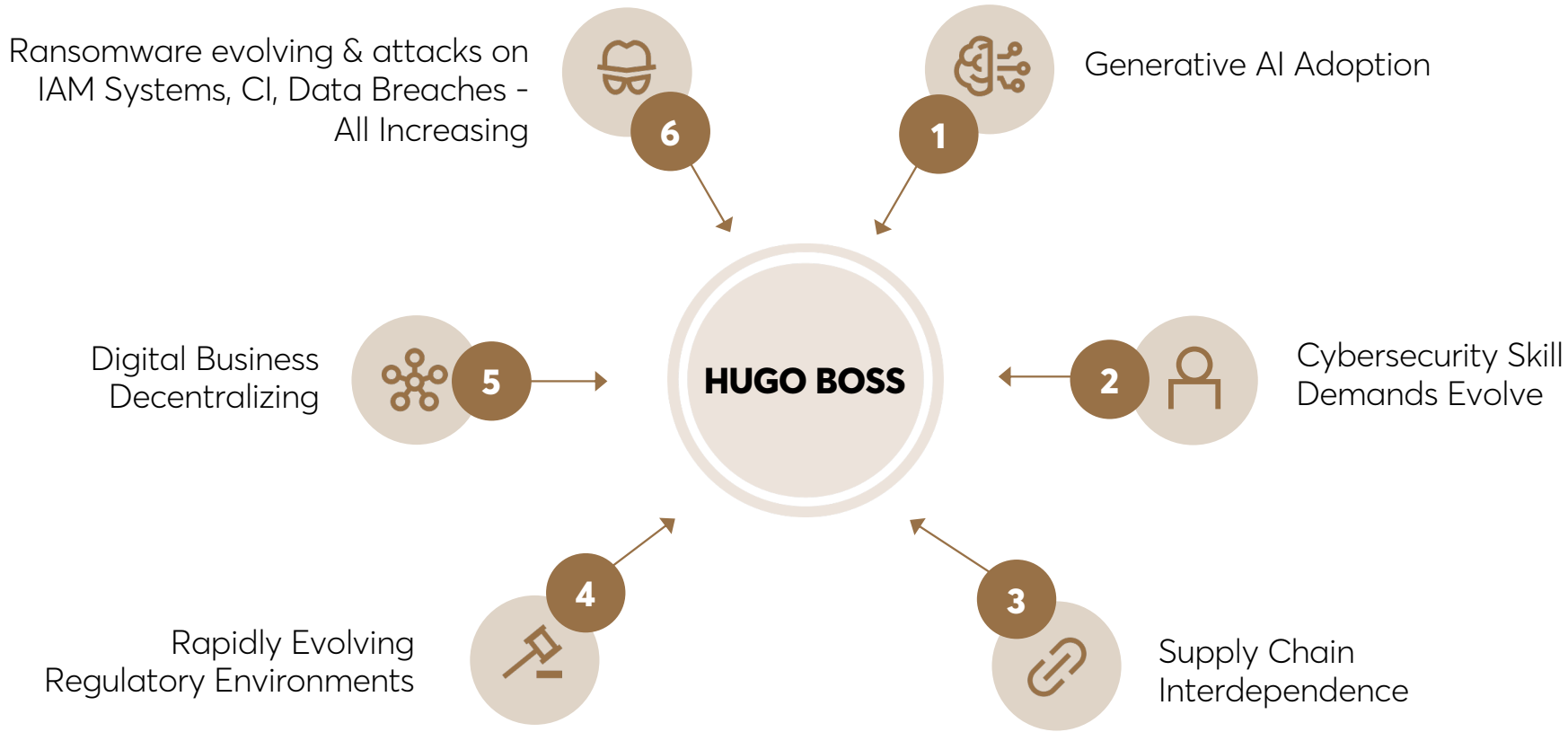
1	2	3	4	5	6	7
Enhanced Customer Trust and Loyalty	Streamlined Operations	New Business Opportunities	Improved Product Development	Enhanced Data Analytics	Vendor and Partner Collaboration	Resilience and Business Continuity
• Innovation: Implementing advanced encryption technologies and secure payment gateways. • Change: Customers feel more secure making purchases, leading to increased trust and loyalty.	• Innovation: Automating security processes such as threat detection and response using AI and machine learning. • Change: Reduces the manual workload on IT staff, allowing them to focus on strategic initiatives.	• Support business to deliver in a fast and secure way applications	• Innovation: Integrating cybersecurity measures into the product development lifecycle. - SAST / DAST / Mobile development. • Change: Ensures that new products and services are secure by design, reducing the risk of future vulnerabilities.	• Innovation: Leveraging secure data analytics platforms to gain insights into customer behaviour and market trends. • Change: Enables data-driven decision-making while ensuring data privacy and security.	• Innovation: Implementing secure collaboration tools for communication and data sharing with vendors and partners. • Change: Enhances collaboration while maintaining the integrity and confidentiality of shared information.	• Innovation: Developing robust disaster recovery and business continuity plans with advanced cybersecurity measures. • Change: Ensures that the organization can quickly recover from cyber incidents, minimizing downtime and financial loss.

HUGO BOSS

ALIGNMENT WITH THE ORGANIZATION'S OVERALL BUSINESS STRATEGY

HUGO BOSS

PERSISTENT FORCES INFLUENCING CYBERSECURITY PROGRAMS



CI = Critical Infrastructure

HUGO BOSS

KEY DEPENDENCIES
THE STAKEHOLDERS

INTERNAL STAKEHOLDERS

1. **Executive Leadership:**
   Provides strategic direction and ensures alignment with business goals.
2. **IT Department:**
   Implements and manages technical security measures.
3. **Legal and Compliance Teams**
   Ensures adherence to legal and regulatory requirements.
4. **HR Department**
   Manages employee-related security measures and training.
5. **Business Unit Leaders**
   Integrate cybersecurity into business operations.
6. **All Employees**
   Act as the first line of defence against cyber threats.

EXTERNAL STAKEHOLDERS

1. **Third-Party Vendors**
   Provide essential services and technologies.
2. **Regulatory Bodies:**
   Set and enforce compliance standards.
3. **Industry Associations:**
   Offer best practices and threat intelligence.
4. **Cybersecurity Consultants**
   Provide expertise and guidance on complex security issues.
5. **Law Enforcement Agencies**
   Assist in responding to and investigating cyber incidents

HUGO BOSS

KEY DEPENDENCIES

1. **Technology Infrastructure**
   - Dependency: Reliable and up-to-date hardware and software systems.
   - Importance: Ensures that security measures can be effectively implemented and maintained.

2. **Skilled Personnel**
   - Dependency: Access to skilled cybersecurity professionals.
   - Importance: Critical for designing, implementing, and managing security measures.

3. **Budget and Resources**
   - Dependency: Adequate financial and resource allocation.
   - Importance: Ensures that cybersecurity initiatives are properly funded and resourced.

4. **Regulatory Compliance**
   - Dependency: Adherence to legal and regulatory requirements.
   - Importance: Avoids legal penalties and ensures the organization meets industry standards:

5. **Vendor and Partner Security**
   - Dependency: Security practices of third-party vendors and partners.
   - Importance: Ensures that external parties do not introduce vulnerabilities into the organization.

6. **Employee Awareness and Training:**
   - Dependency: Comprehensive training program, Awareness … aims for all employees.
   - Importance: Reduces the risk of human error and enhances overall security posture.

HUGO BOSS

IN CASE OF QUESTIONS, REACH OUT TO

STEFAN BALDUS
INFORMATION AND IT COMPLIANCE OFFICER

Information-security@hugoboss.com