Cybersecurity, a crucial stake to ensure business continuity

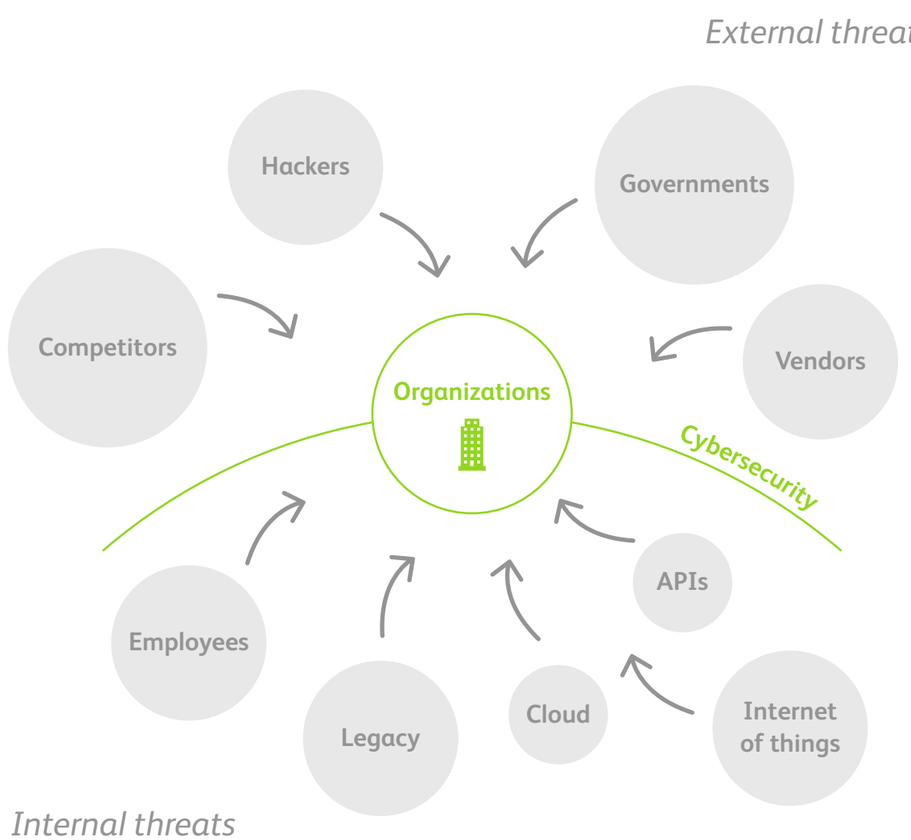
Organizations must integrate in their global IT security approach the development of new threats coming from the massive digitalization.

Already impacted by cyberattacks (small extract)*, organizations have built defenses...

Organization	Sector	Cyber damages
Yahoo!	Technology	• Cyber attack in 2014 affecting 500 million user accounts
Marriott Hotel	International Hotel Group	• Cyber attack started in 2014 and spotted in 2018 affecting up to 500 million guests
Equifax	Credit company	• Cyber attack in July 2017 affecting personal data of 143 million of customers
Alterix	Marketing analytics company	• Cyber attack that publicly exposed data (248 fields) for about 123 million U.S. households
Korean Credit Bureau (KCB)	Financial institution	• Cyber attack in 2014 where data from 100 million credit cards had been stolen

**Examples extracted from press articles*

... that should be reinforced to face existing and new threats of the digitalization



BearingPoint®

A sustainable security implementation based on an integrated overall process

BearingPoint security approach.

1. Strategy & Governance

- Define the organization's appetite for risk by involving all stakeholders
- Document and communicate clearly and unambiguously IT security policies

2. Architecture

- Create a "state of the art" architecture to support business goals
- Support all stakeholders in order to find cost optimized and sustainable solutions

3. Integration

- Align architecture with operations' teams and existing processes
- Integrate processes and tools based on the existing systems

4. Implementation

- Reinforce the security by implementing solutions on existing processes and tools
- Ensure the integration of specific conditions for platform

5. Operation

- Integrate the security within operational functions of the organization
- Initiate and amplify a true security culture within the organization

6. Control

- Set up appropriate monitoring and reporting for both the operation teams and the top management based on reliable information

7. Remediation

- Involve all stakeholders to find cost optimized remediation solutions
- Implement sustainable and flexible solutions.

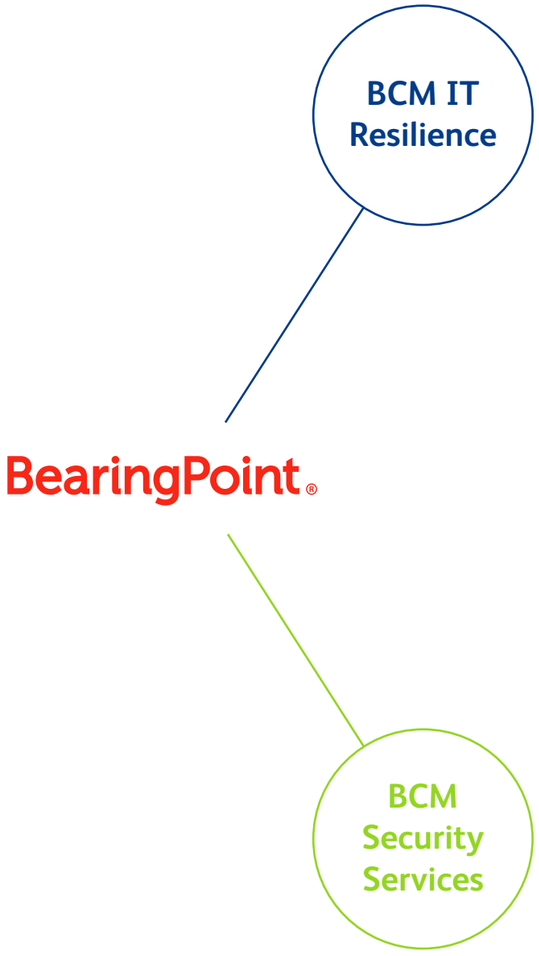
8. Risk & Compliance

- Inform the management if anything cannot be remedied or can only be remediated with delay
- Realize a residual risk assessment

BearingPoint®

A wide and complete range of services to reinforce the IT security of organizations

BearingPoint security services portfolio.



Security & BCM Governance	• Develop a security strategy in line with your business requirements, setup the governance around security, evaluate the Risk and its management • Develop a business contingency plan aligned with the business requirements and implement a crisis management including the required regular training and review
Security & BCM assessment	• Determine threats' vectors to identify gaps and opportunities based on the top management's appetite for the risk • Perform an assessment through a clear methodology to evaluate the existing maturity of the architectures' security, data protection and business continuity mechanisms
Application, cloud & IoT security	• Integrate the IoT (Internet of Things) notion in the global security architecture and develop an IoT security culture and create IoT security requirements • Enhance the security by integrating application, cloud and IoT with the legacy systems
Infrastructure security	• Design and build a tailored security system responding to each business particularity thanks to the support of a large cybersecurity experts • Implement the "security infrastructure of tomorrow" to protect business against rising number of sophisticated cyber attacks
Advanced threat inspection	• Identify risks and vulnerabilities of digital assets to implement solutions for enhancing the IT security of the organization • Leverage on an experienced inspection team having performed various testing plans on applications, security and cloud infrastructure, embedded systems, etc.
FOSS* security	• Ensure within an agile environment where open source software is often used that rules and policies are correctly implemented to reduce a significant risk for the organization

**FOSS : Free and Open Source Software*

BearingPoint