Clarity on Cyber Security

Media conference
29 May 2018
Why this study?
Methodology
Methodology of the study

- Online survey consisting of 33 questions

- **60 participants from C-Level (CISOs, CIOs, CTOs)**
  - 26 large companies (> 5,000 FTEs)
  - 34 small and mid-size companies (< 5,000 FTEs)

- **Personal interviews were conducted with five subject matter experts**

- **Evaluation of the data was carried out by a KPMG’s cyber security team of experts**
Distribution of survey participants by sector

- **33%** Financial Services
- **5%** Professional Services
- **25%** Consumer/Industrial Markets
- **3%** Communication/Entertainment
- **13%** Energy and Natural Resources
- **2%** Infrastructure
- **12%** Government
- **7%** Other
In-depth interviews with subject matter experts

**Entering new territory: the opportunities and risks of blockchain and cryptocurrencies**

Oliver Bussmann  
President  
Crypto Valley Association

**The search is on: finding alternative security technologies to deal with the rise of quantum computing**

Renato Renner  
Professor for Theoretical Physics  
ETH Zurich

**Know your target: how cyber due diligence feeds investment decisions**

Christian Unger  
Managing Director and Co-Head Industry Value Creation Partners Group

**Protecting civilians in cyberspace: the Digital Geneva Convention**

Brad Smith  
President and Chief Legal Officer  
Microsoft

**SwissID's quest to provide security, reliability and trust**

Markus Naef  
CEO  
SwissSign
Resilience and trust are prerequisites for sustainable growth in the digital age.
Genuine threats, real damage

From those attacked:

- **42%** incurred **financial losses** (2017: 36%).
  - 75% in financial services vs 25% in non-financial services

- **33%** suffered from **disclosure of confidential internal information** (2017: 29%).

- **42%** experienced **disruption of business processes** (2017: 56%).
  - 25% in financial services vs 50% in non-financial services

- **25%** needed to deal with **reputational damage** (2017: 37%).
Security breaches damage trust

73% believe that customers’ trust in an organization is ‘very’ or ‘fairly’ impacted by cyber security breaches.

58% believe it impacts on investors’ trust in the business.

«Companies are increasingly expected to have a clear strategy towards cyber security and privacy risks. Building it into your due diligence is vital to protecting both investors and customers.»

Christian Unger, Partners Group
Acknowledgment, but limited action

80% of boards consider cyber security to be an operational risk.

36% address the topic in their annual report.
Acknowledgment, but limited action

69% of respondents see digital ID as an important step towards trusted interactions with customers.

35% plan to incorporate digital ID into their products or services.

«As a growing number of activities are carried out online, users need to be confident that the environment is secure and reliable. Digital IDs are an integral part of building this trust.»

Markus Naef, SwissSign
Acknowledgment, but limited action

35% have an **overview of Internet of Things** and operational technology devices deployed in their organizations (2017: 31%).

58% admit that these are **not covered in their current cyber security strategy** and policies (2017: 48%).

Hackers attack Casino’s fish tank thermometer to obtain sensitive data
Acknowledgment, but limited action

53% expect its use of blockchain technology to pose new security risks.

8% have already taken specific steps to manage these risks.

“For blockchains, long-term security is obviously essential, even more than for encryption. No-one wants to use a cryptocurrency that will become worthless in 15 years due to a quantum attack. But exactly this could in principle happen.”

Renato Renner, ETH Zurich

“Blockchain represents great potential but also massive challenges. Huge sums of money could be lost through error or malicious action if we don’t invest enough in security and threat prevention.”

Oliver Bussmann, Crypto Valley Association
Do we learn from past incidents?

After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B

23% include cyber security in their due diligence scope of investments and mergers.

«Compared to other due diligence elements cyber is a relatively new topic. However, the overall understanding of technology and its associated risks is growing rapidly in the investor community. We will see this clearly develop further and become more sophisticated. This will be necessary as the threats and risks will become more difficult to judge.»

Christian Unger, Partners Group
Third party risks are slipping off the radar

44% have no **instruments to enforce their control framework** on suppliers (2017: 32%).

38% have **no contractually agreed, binding terms** related to cyber risks (2017: 29%).

34% **do not require specific cyber security measures** in third party contracts (2017: 30%).

59% of contracts with third parties do not include a **right to audit** (2017: 40%).

Sears and Delta Airlines customers' payment data exposed by third-party vendor breach
Inadequate scenario plans

82% of cyber response plans do not cover attacks against suppliers or business partners.
- 60% in financial services vs
- 93% in non-financial services

Personal data breaches (GDPR: notification within 72 hours)

40% of financial institutions do not have a bespoke response plan.

76% of non-financial service organizations do not have a bespoke response plan.
Product/market fit?

28% of respondents have cyber insurance.

The reason why they don’t have a cyber insurance policy in place

68% say the it doesn’t match their needs.

64% say it is too expensive.

64% say the coverage has too many limitations.
Do we need regulations to get things moving?

Cyber response plans

<table>
<thead>
<tr>
<th>Year</th>
<th>Financial Services</th>
<th>Non-Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>67%</td>
<td>54%</td>
</tr>
<tr>
<td>2017</td>
<td>87%</td>
<td>42%</td>
</tr>
<tr>
<td>2018</td>
<td>100%</td>
<td>48%</td>
</tr>
<tr>
<td>Growth opportunities</td>
<td>Benefits from cyber resilience</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Unleash the value of data</td>
<td>• Build/increase trust</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Governance and (emerging) technology to use AND protect data</td>
<td></td>
</tr>
<tr>
<td>Leverage emerging business models and technologies</td>
<td>• Enhance understanding of upside and downside risks of business models and technologies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• «Toolbox» to get security and privacy right by design when deploying such business models and/or technologies</td>
<td></td>
</tr>
<tr>
<td>From supply chains to networks and ecosystems</td>
<td>• Understand, mitigate and monitor risk exposure caused by third parties (business partner, suppliers)</td>
<td></td>
</tr>
<tr>
<td>Acquisitions and investments</td>
<td>• Due diligence for cyber/privacy risk-adjusted target valuation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Align cyber resilience to protect investment</td>
<td></td>
</tr>
</tbody>
</table>
These should be organizations’ priorities

Act now
- Get the basics right
- Understand your cyber and privacy risks
- Put the human at the center of your cyber security strategy
  - Clients, employees, business partners AND attackers
- Implement cyber resilience consequently and with focus – both private sector and governments

Get ready for the future
- Adopt a forward looking mode
- Understand impact of data, emerging technologies and emerging business and operating models on your cyber and privacy risk exposure
- Encourage a cyber resilience and privacy friendly political, economic and regulatory environment

«We live in an internet-dependent world and cannot rely on governments to fix this problem in isolation. Governments sometimes need to be encouraged to act for the benefit of society as a whole. I think the time has come to do so with regard to cyber weapons.»

Brad Smith, Microsoft
Media requests

Can Arikan
Head of Media Relations
+41 58 249 53 51
+41 79 396 66 46
carikan@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

© 2018 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss legal entity. All rights reserved.