Ahead of the next curve

Clarity on Cyber Security
30 May 2017

#KPMG_Cyber
Study results

Work on what’s now - think about what’s next
Evolution of cyber risk in Switzerland

No time to waste to discuss cyber hygiene -

cyber attacks are business as usual
Cyber-attacks are increasing

88% of respondents suffered a cyber-attack in the past 12 months (2016: 54%; 2015: 52%)

<table>
<thead>
<tr>
<th>Consequence of Successful Cyber Attack(s) on Your Business (%)</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruption of business processes</td>
<td>44</td>
<td>37</td>
</tr>
<tr>
<td>Reputational damage</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Financial loss</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Disclosure of confidential internal information</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>Disclosure of confidential information about clients or business partners</td>
<td>18</td>
<td>16</td>
</tr>
<tr>
<td>Manipulation of data</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>Unauthorized disclosure of personal data</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>I don't know</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
A deeper understanding of cyber risks

81% confirmed that they have gained a deeper understanding of cyber risks in the past 12 months.

52% have gained better understanding of the attacker’s motivation, strategy, and tools.
Recognized at board, but communication gap persists

- 86% agreed that the Executive Board considers cyber security to be an operational risk.
- 71% are not sure whether cyber security experts speak the language of business.
Two speeds on response capabilities

87% of FS institutions have a cyber response plan.

42% of Non-FS institutions have a cyber response plan.
Cyber security moves beyond irritation

- Security is about trust
- The human factor was, is, and will always be, the weakest link
- We have a design problem – user friendliness is not considered
## Cyber security is about trust

How high do you consider the impact of cyber security breaches on the trust of ... (in percent)

<table>
<thead>
<tr>
<th>Category</th>
<th>Very impacted</th>
<th>Fairly impacted</th>
<th>Moderately impacted</th>
<th>Slightly impacted</th>
<th>Not impacted at all</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>...your customers?</td>
<td>58</td>
<td>21</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>...authorities / regulators?</td>
<td>32</td>
<td>35</td>
<td>12</td>
<td>4</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>...your business partners?</td>
<td>28</td>
<td>42</td>
<td>21</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>...your investors?</td>
<td>21</td>
<td>33</td>
<td>23</td>
<td>4</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>...of the public?</td>
<td>18</td>
<td>30</td>
<td>21</td>
<td>12</td>
<td>11</td>
<td>8</td>
</tr>
<tr>
<td>...your employees?</td>
<td>14</td>
<td>45</td>
<td>30</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>...of other stakeholders?</td>
<td>8</td>
<td>11</td>
<td>8</td>
<td>73</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Very impacted | Fairly impacted | Moderately impacted | Slightly impacted | Not impacted at all | No opinion

© 2017 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.
The “human factor” not considered properly

65% confirm that their organization does not systematically work on cyber security measures that are user-friendly.

48% assess the user friendliness of cyber security measures when implementing new concepts.

11% involve a user interface specialist to achieve user-friendly security design.
Cyber security moves beyond cyberspace

- Physical world integrates with cyberspace
- Major security concerns
- Limited actions to improve security
The Internet of Things is all around us...

There will be 20.8 billion devices connected to the Internet generating over 20 zettabytes of data by 2020. (Source: Gartner)

Healthcare
- Remote patient observation
- Smart medical devices
- Smart prescription management
- Algorithmic diagnostics analysis

Banking & Insurance
- Mobile payment and wallets
- Smart ATMs
- Predictive insurance modeling
- Driving data recorder

Smart City
- Video surveillance
- Predictive policing
- Smart management of city infrastructure
- Renewable energy
- Public safety
- Building automation
- Water and waste water management

Individual Mobility
- GPS
- Car sharing
- Automated driving
- Electric car charging station management

Public Transportation
- Driverless trains
- Connected stations and tracks
- Signalng and connected roadways
- Demand responsive transport (DRT)

Industrial Manufacturing
- Factory automation
- Energy management
- Factory surveillance
- Smart warehousing and routing
- Predictive maintenance

Chemicals & Pharma
- Drug usage tracking
- Chronic disease management
- Smart pills

Private space
- Home automation
- Security improvement
- Smart household appliances

Consumer Goods & Retail
- Connected retail
- In-store localization
- Beacon technology
- Connected clothing

Agriculture
- Automated field testing
- Automated weeding

Transport & Leisure
- GPS and RFID
- Environment monitoring and management
- Responsive and adaptive supply chains
- Reservation, toll, and ticketing systems
- Guidance and control systems

Power & Utilities
- Supervisory control and data acquisition (SCADA)
- Advanced metering infrastructure (AMI)
... but not yet addressed by cyber security

33% have gained better insights into the landscape of relevant IoT devices in the past 12 months.

41% include IoT or OT assets in their cyber security strategy and policy.
Major concerns on how to handle the IoT security challenge

59% state that their main concerns regarding IoT-related risks are exotic devices that are introduced in the organization’s network.

59% state that their main concerns regarding IoT-related risks is the fact that traditional controls are no longer effective.
The basics are not yet under control

Do you have an overview of all Internet of Things (IoT) and operational technology (OT) devices deployed in your company? (in percent)

- 35%: No, we haven’t tried to get an overview
- 31%: No, even though we tried
- 17%: Yes
- 17%: I don’t know
Cyber security moves beyond human versus machine

- Cyber attacks on AI may cripple your organization’s automation and decision making capabilities
- Is AI useful in defense strategies?
- Are we facing a future where machines attack machines?
It’s time to understand the security impact of AI

26% think that the rise of AI leads to new challenges in cyber security now.

43% believe that the rise of AI will lead to new challenges in cyber security within 2–3 years.
... but AI is not yet on the security agenda

12% analyze the security impact of potential AI use cases systematically

4% use AI to protect themselves from cyber threats, but 40% expect that AI is going to be used by attackers in the future.
Summary

Ahead of the next curve
- Work on what’s now – think on what’s next

Major security gaps remain despite progress on cyber security
- No time to waste to implement cyber hygiene – attacks are business as usual
- Focus on business impact to understand, communicate, and mitigate cyber risks

Cyber security moves beyond irritation
- Ensure trust of clients, employees, business partners, authorities
- (Re-)think user friendliness of security to make it effective

Cyber security moves beyond cyberspace
- Prioritize IoT security as it is ubiquitous today already

Cyber security moves beyond human versus machine
- Understand the security impact of AI and put it onto the security agenda
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.

© 2017 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.