Never a dull moment

Media Conference «Clarity on Cyber Security»

—

24 May 2016

KPMG

Introduction

Why this study?

Methodology of the survey

- **Online survey with 43 questions**

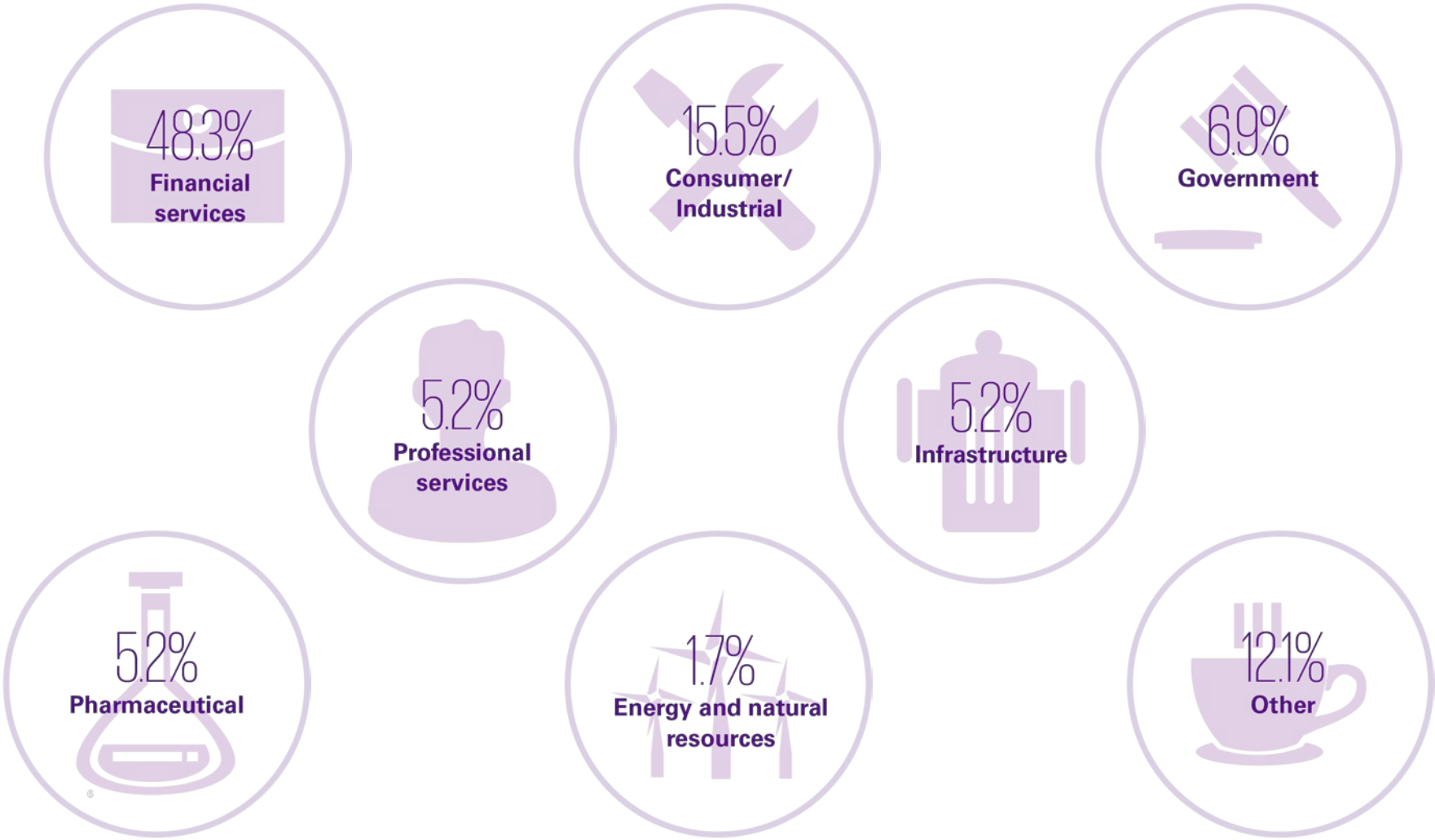
- **60 participants from C-Level**
  - 35 working for large enterprises (> 5,000 FTEs)
  - 25 from small and mid-size companies

- **Personal interviews were conducted with four Swiss business representatives of large companies.**

- **Evaluation of the results was carried out by a KPMG cyber security team of experts.**

- **The content of the study results is enriched with the experience of the KPMG consulting practice.**

Distribution by sector



Study results – never a dull moment

While classic cyber security challenges have not yet been mastered, ...

... new ones are emerging on the horizon.

KPMG

Evolution of cyber risk in Switzerland

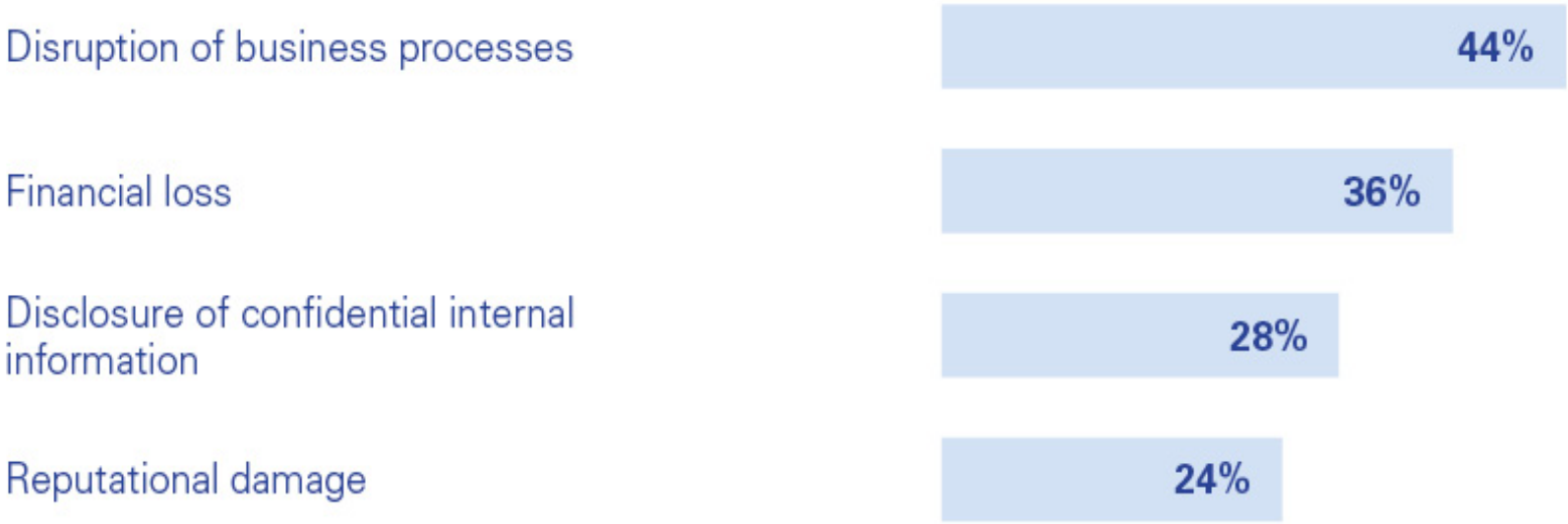
More than ever, Cyber Security is a prerequisite for business success

Cyber attacks are business as usual

54%

experienced a cyber attack in the past 12 months (2015: 52%)

What were the consequences of Cyber Attacks?



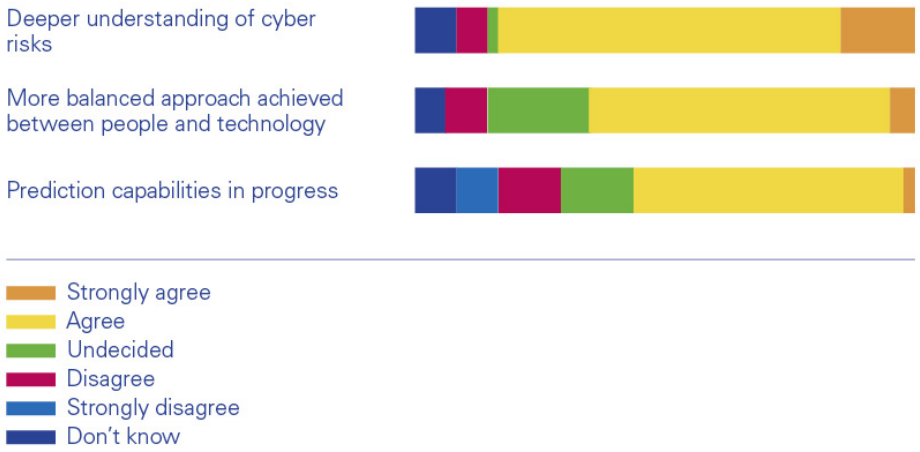
The nature of cyber security is better understood at the Executive Board

84% indicate that their organization reached a deeper understanding in the past 12 months

75% agree that Executive Board perceives Cyber Security as an operational risk (2015: 69%)

Only 19% believe employees are sufficiently aware of the cyber risk (2015: 36%)

Can you confirm improvement from a Cyber Security point of view within the last 12 months on the following topics?



Despite significant investments Swiss companies are not adequatly prepared

Respondents having a **security incident response plan** have **doubled** (48% vs 21%)

Three times as many respondents conduct **Cyber Security exercises** (48% vs 14%)

The number of respondents investing in a **better monitoring** architecture to detect Cyber threats has **significantly increased** (60% vs 38%)

The **majority** of respondents have integrated Cyber Security in **third-party contracts** (63% vs 36%)

Third parties not under control

93% of FS institutions require right to audit, and 65% of Non-FS institutions require right to audit in third-party contracts.

33% **of FS** institutions report that understanding, visibility and control of Cyber Security has worsened when outsourcing to third parties, while only

8% **of Non-FS** institutions report this

Only 19% believe that leveraging the cloud can reduce security efforts on infrastructure protection

In the light of outsourcing and tighter interconnection with business partners - when building business ecosystems - mastering the third party challenge is critical

KPMG

Emerging challenges

Know thy enemy

An understanding of the motivation, intent, strategy, tactics and the tools of the attackers is critical in order to anticipate threats and effectively prepare for, prevent, detect and respond to attacks.

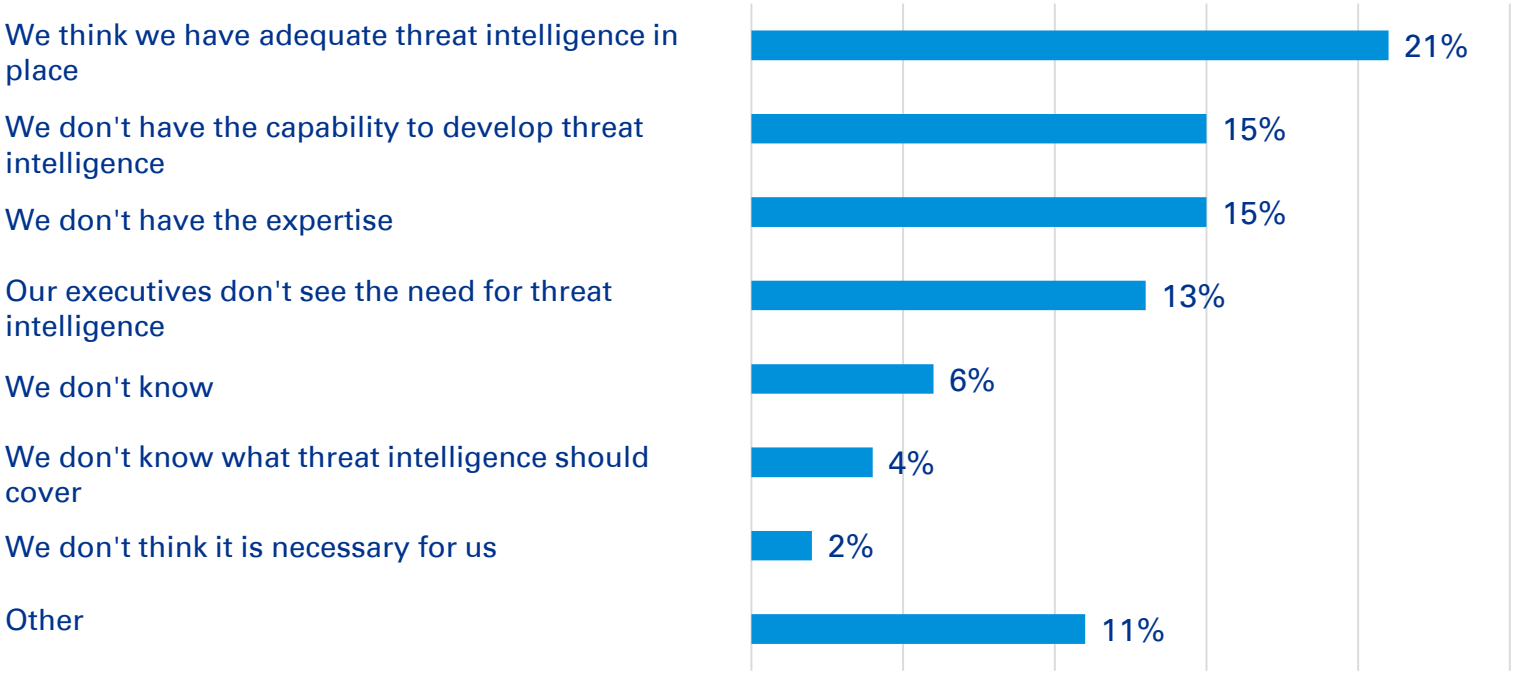
Further challenges ahead - the insider

80% of

respondents do not have a proper insider threat management program.

Finding the needle in the haystack

Only 21% think they have adequate threat intelligence in place



Build networks, break down silos

It takes a network to defeat a network

Are competitors trustworthy?

66% of the respondents collaborate with other organizations

The goals of collaboration are:

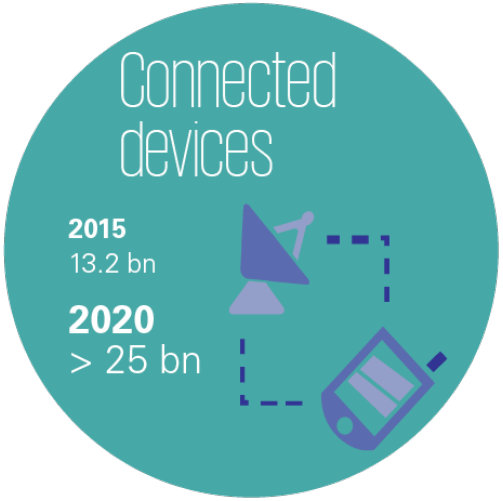
88% to share threat intelligence, 83% to share lessons learned and 78% to discuss preventive measures

32% feel **company policies** (e.g. business secrets) constrain the ability to collaborate, in addition **cultural issues (21%)** and the **lack of exchange platforms (21%)** are mentioned as the obstacles for collaboration

4th industrial revolution raises the stakes

Cyber Security directly affects the resilience of our organizations, our economy and our individual health and safety.

Cyber becomes physical



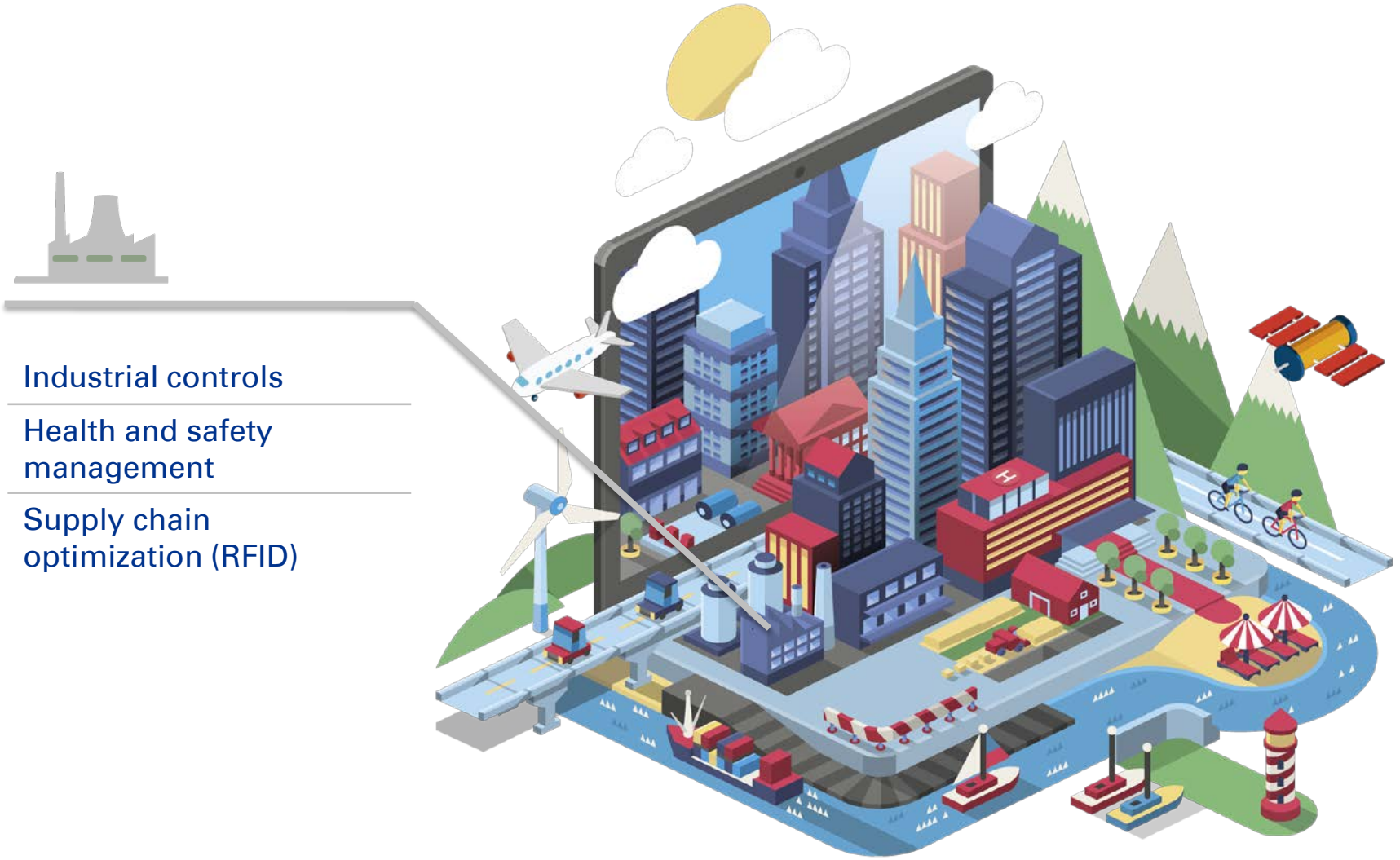
Home and City

- Smart Meters – efficient use of energy
- Building automation
- Smart management of city infrastructure
- Surveillance
- Water supply
- Sewage disposal

Transportation

- Connected Vehicles
- Self-Driving Cars
- Smart Infrastructure
- Public transportation
- Aviation
- Sea faring

Manufacturing and Operations



- Industrial controls
- Health and safety management
- Supply chain optimization (RFID)

Consumer and retail businesses

Improved customer experience

In-store localization

Health

- Expanded access to healthcare
- Well-being – the quantified self
- Emergency Notification

Sustainability

Feed the planet – improved crop yield

Sustainable environment – reduced water consumption

Internet of Things challenges

66% are concerned that Internet of Things implies that traditional controls are no longer effective

57% fear that exotic devices get connected to their networks

53% didn't try to have an overview of Internet of Things devices

Companies should take into account that the security, safety and reliability of their (physical) products will depend on managing Cyber Security properly.

Two speeds

Outrider
A number of Swiss organizations manage to at least keep up with the speed of the evolving threat landscape, the most advanced succeed in reducing the risk and leverage cyber to enable new business and operating models (for instance digitalization).

Late starter
Others struggle to keep up with the rapidly evolving threat landscape. They won't be able to evolve their business into Industry 4.0.

Summary

Know thy enemy -

Understand the motivation, intent, strategy, tactics and the tools of the attacker

Build networks, break down silos –

it takes a network to defeat a network

The 4th industrial revolution raises the stakes –

Cyber Security becomes physical

Two speeds –

Leverage Cyber Security to enable new business and operating models or miss Industry 4.0

Never a dull moment

Media Conference «Clarity on Cyber Security»

—

24 May 2016

Medienanfragen

Media Relations
+41 58 249 53 51
media@kpmg.ch

kpmg.ch/socialmedia

kpmg.com/app

Download on the App Store