KPMG

Cyber Security and the Auditor

ABIAL Professional Practice Update
June 01, 2016

Agenda

KPMG

State of Cyber Security

Fundamentals

State of Cyber Security

The Challenge

Cloud technology, big-data, mobile working and social applications have made companies more productive and agile.

However, the wholesale adoption of these technologies also brings cyber security risk.

The assets that make your company run, if breached, could bring the whole company down.

State of Cyber Security

Quantifying the threat

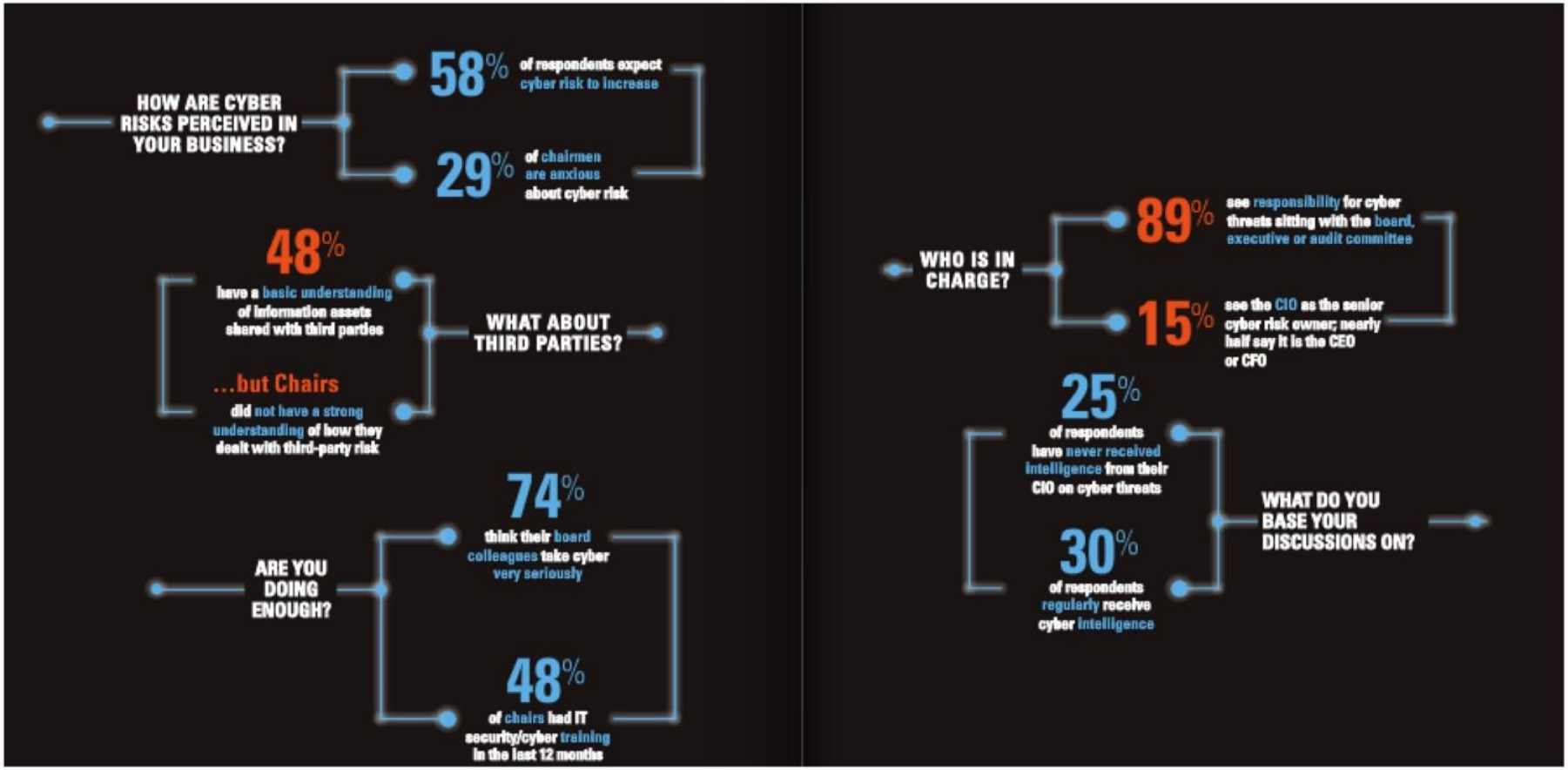
Last year, Luxembourg computer incident response centre (CIRCL) received 83,610 reports of cyber attacks in the Grand Duchy. The figure rose 18 times compared with the 4,500 incidents reported in 2011.

http://www.wort.lu/en/business/luxembourg-computer-incident-response-centre-luxembourg-s-cyber-security-landscape-is-a-warzone-551d12630c88b46a8ce56a89

In December 2013, Target acknowledged a data breach centered on its Point-of-Sale systems within its U.S. retail stores. A few weeks later, Target announced that the breach had expanded to include additional compromised systems, leading to the theft of additional customer information. In total, personal information in the form of names, mailing addresses, phone numbers, and e-mail addresses for up to 70 million people was stolen.[6,7]

KPMG's 2015 FTSE 350 Cyber Governance Health Check:

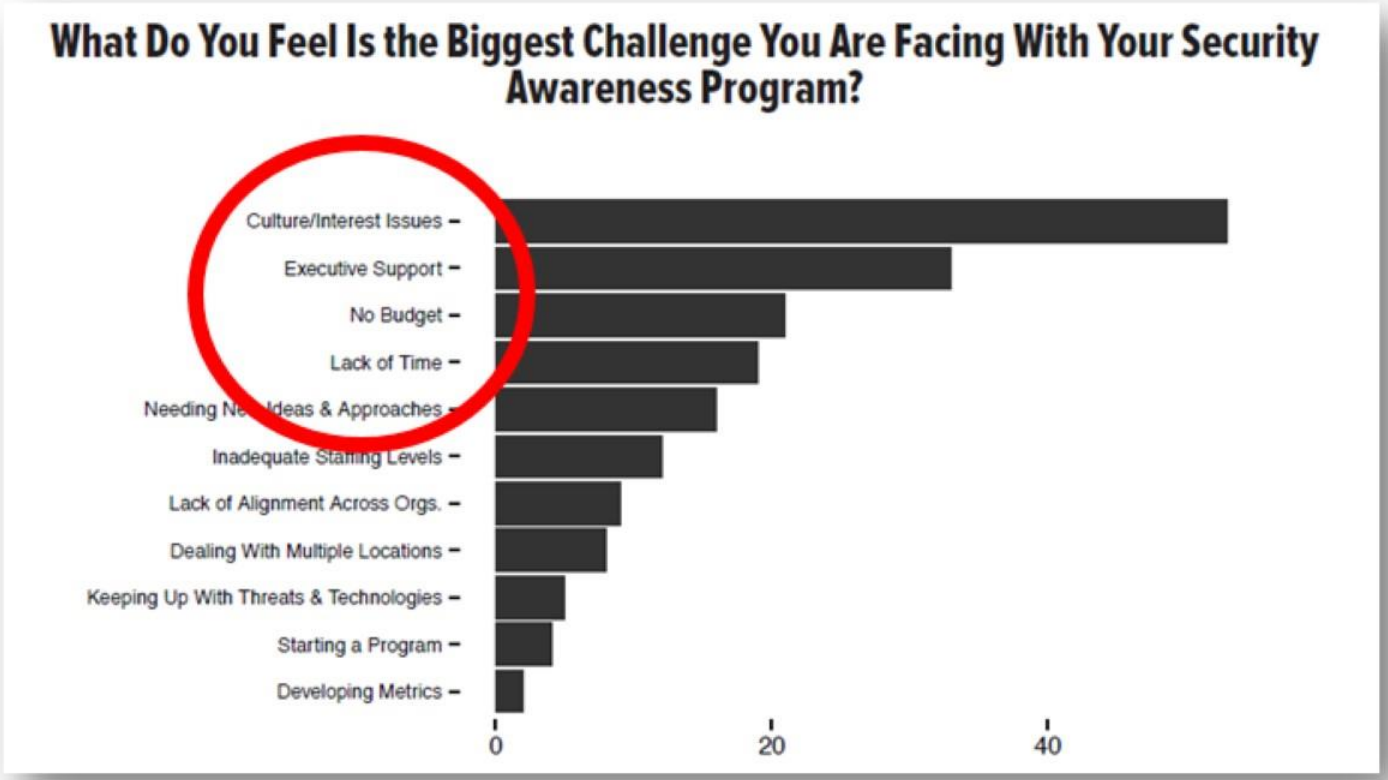
State of Cyber Security



Source: KPMG 2015 FTSE 350 Cyber Governance Health Check - "An insight into the issues of today and tomorrow"

State of Cyber Security

What ISOs say...



Source: SANS 2015 Security Awareness Survey

KPMG

Threat Landscape

What are we dealing with?

Threat Landscape

What are we dealing with?

A panorama of cybercriminal activity and circumstances which facilitate criminal behaviour

- Social Engineering, **Spear Fishing** [CEO Fraud]
- System Design Flaws, Misconfiguration [Zero-Day Exploits]
- Attacks on mobile devices [Postbank case]
- **Advanced Persistent Threats (APT)**
- Financial cut-backs, Lack of awareness and support
- PoS attacks [Target case, other retailers in the US]

... and many more!

Threat Landscape

Spear phishing: A more targeted and sophisticated form of phishing.

Unlike standard phishing schemes that use mass e-mails, spear phishing schemes target individuals that fit a certain profile.

For example, they may only target high-ranking employees of a specific company or governmental agency, or users of a specific site.

Further more, the request for information may appear to come from a colleague working at the same company.

The goal of these scam artists is to lure recipients into divulging sensitive information about themselves and/or their organization. Sophisticated attackers do extensive research on their targets prior to sending out e-mails, so they not only look realistic, but the information requests seem plausible and do not raise suspicion. This added element of social engineering and relevance makes a spear phishing message particularly effective and dangerous.

Threat Landscape

APT1 is an enterprise scale and *presumably* military-funded data theft and espionage operation, which has been active since 2006.

APT1 has targeted about 150 organizations and corporations worldwide (incl. Luxembourg). The volume of information *believed* to be stolen comprises hundreds of TERABYTES.

Individual targets were subject to constant data theft for as long as 4 years and 10 month.

Largest data volume reportedly stolen from a SINGLE entity was 6.5TB over a 10 month period.

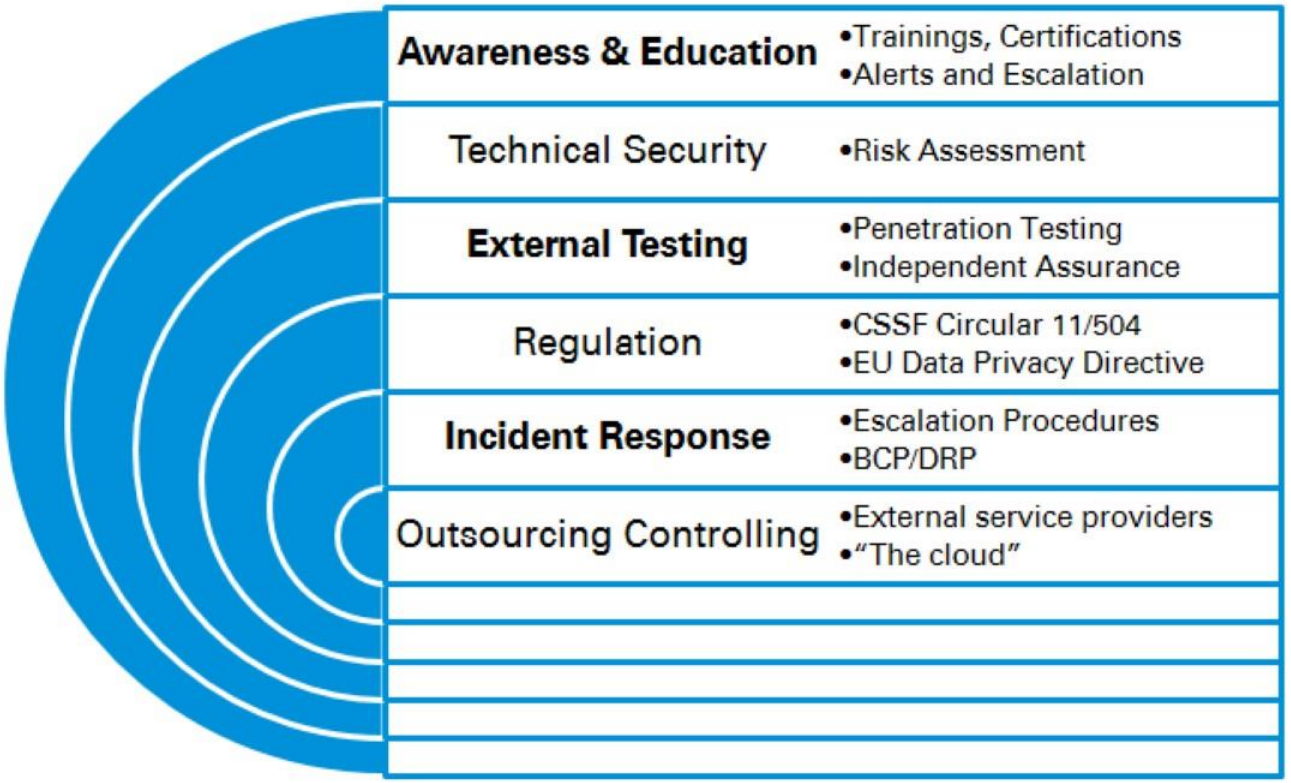
KPMG

The Auditor's Perspective

What should we focus on?

The Auditor's Perspective

What should we focus on?



The Auditor's Perspective

Awareness & Education

Pass

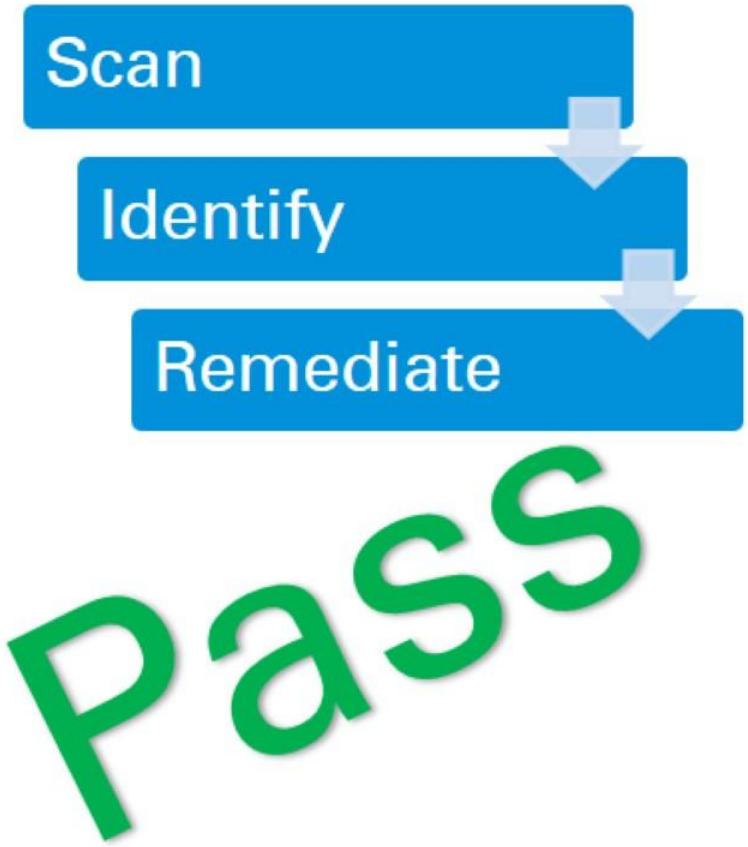
It is critical to provide ongoing training and education for all employees, including C-level executives, in order to increase cyber awareness.

Organizations need to

- clearly define roles and responsibilities,
- promote greater collaboration, and improve communication to, and beyond, the team.

The Auditor's Perspective

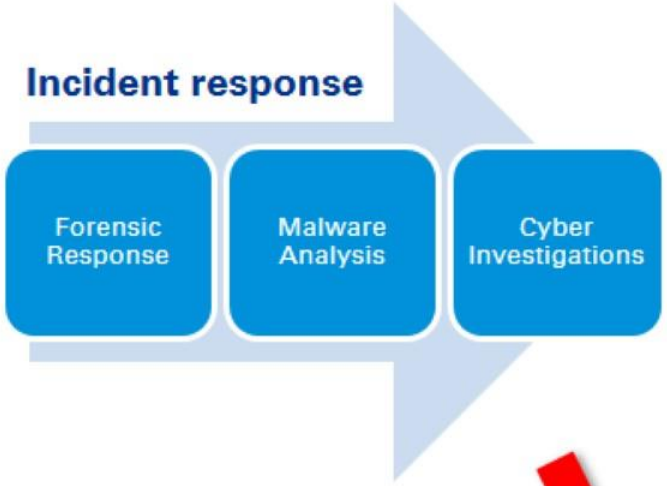
External vulnerability testing



Using the **specialist knowledge** of independent experts supports an organization's cyber security strategy by providing **details on vulnerabilities.**

Early detection of weak points significantly reduces the **risk of exploitation.**

The Auditor's Perspective



Fail

Organizations create comprehensive incident response plans but:

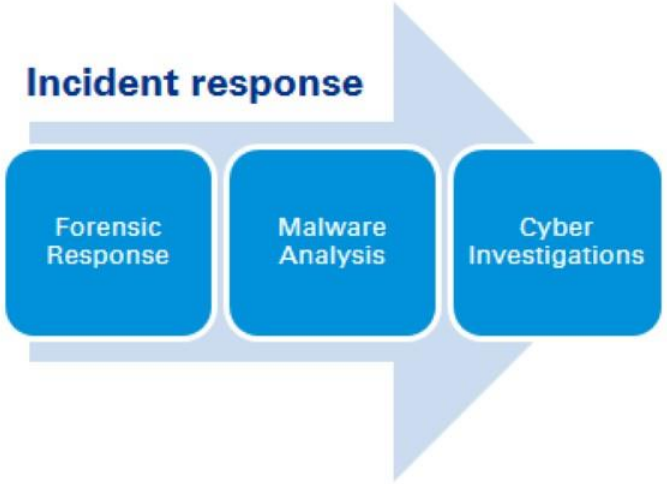
- **sometimes do not test them until a real event occurs**
- view creating an incident response plan as a **one-time event as opposed to an ongoing process.**

Off-the-shelf plans are often

outdated and ineffective

against evolving threats and changing technology.

The Auditor's Perspective



Organizations should establish policies, processes, and procedures that are **tailored** to their culture, environment, response personnel, and most importantly, business objectives.

Documentation should be **concise**, and should **evolve constantly to remain current** with both external trends as well as shifts in business objectives.

Pass

KPMG

Summary

Summary

- **Awareness programs** are an essential part of any robust Cyber Security strategy
- Tailored and well-tested **Incident Response** plans ensure swift recovery from cyber attacks
- External **vulnerability scanning** will increase the overall security level

KPMG's Cyber Security brochure:

KPMG

Thank you!

Thomas Koch (GCFA, CISA)
Senior Manager, Information Risk Management

KPMG Luxembourg, Société coopérative
39, Avenue John F. Kennedy
L-1855 Luxembourg

Phone: +352 22 51 51 7920
Mobile: +352 621 87 7920
Fax: +352 22 51 71
E-mail: thomas.koch@kpmg.lu

kpmg.lu

kpmg.lu/app