Cyber Security: The changing landscape

September 2016

kpmg.com/channelislands
Agenda

- Introduction
- Cyber
- General Data Protection Regulation
- Questions
Introduction

- Protect your personal, client and business information
- Strategic matters
- Technical versus cultural
- KPMG has global expertise
Mika Laaksonen
Our cyber security journey - global

6

Made Cyber Security one of our six global multi-disciplinary Strategic Growth Initiatives (SGIs)

Accelerated Cyber Security revenue growth

Overtaken our direct competitors in many key markets…

…and moved Cyber Security to the heart of KPMG

$1000m FY20

$614m FY14

$153m FY11

Completed five acquisitions in a year

Increased our range of clients

3,810 Clients globally

Deepened and broadened our range of services

Earmarked $165m for investment in organic growth over five years

40%

Growth target

© 2016 KPMG Channel Islands Limited, a Jersey company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential
How prepared are we?

<table>
<thead>
<tr>
<th>How prepared is your company for a cyber event?</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully prepared</td>
<td>25%</td>
</tr>
<tr>
<td>Somewhat prepared</td>
<td>69%</td>
</tr>
<tr>
<td>Not where we need to be</td>
<td>3%</td>
</tr>
<tr>
<td>Unsure</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: 2016 Global CEO Outlook, KPMG International

**Are we prepared?** Seventy-two percent of CEOs say they are not fully prepared for a cyber event, significantly higher than in 2015 (50 percent).

**Can you be fully prepared?** In interviews, CEOs frequently said: “We are as prepared as we can be” or “You can never be fully prepared.”

**How to prepare?** By practicing the ability to respond to cyber events. Companies need an ability to be agile and deal with the unexpected.
Attacks

Targeted attacks are becoming more common…

In a study of 1,200 companies, security research firm FireEye identified:

- 24% of these companies experienced events that matched the patterns of a targeted attack
- 97% of these companies were breached.

We did a similar study in Finland, Sweden and Denmark – The results are similar.
The risks - where’s the upside?

Cyber security is correlated with performance. More CEOs from top-performing companies believe that they are fully prepared for a cyber event.

As the volume of data grows exponentially, so do the opportunities to use it. Typically, when services are free, businesses make money from the data, and the consumer becomes, in effect, a product.

KPMG CEO Survey 2016. Growing companies are more prepared

KPMG CEO Survey 2016. Security prompts innovation
Threats - http://cyber.kpmg.com/#

- Data breach
- Malware
- APT
- Hacktivism
- Mobile security
Regulatory Focus Areas and Industry Activities

**Regulatory Focus Areas**
- Evaluation of Cybersecurity Inherent Risk
- Enterprise Risk Management and Oversight
- Threat Intelligence and Collaboration
- Data Classification and Risk-Based Controls
- External Dependency and Vendor Risk Management
- Cyber Incident Management and Resilience (BCP/DR)
- Information Sharing
- Social Engineering and Insider Threats
- Data Loss Prevention (DLP)

**Industry Activities**
- Cybersecurity Assessments and Benchmarking
- Refresh Information Governance Model
- Enhance Data & Information Protection
- Improve Security Monitoring and Incident Management
- Participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Develop and Revise Policy & Standards
- Maintain an Effective End-User Awareness Program
- Improve Third-Party Vendor Security Assessment Program
The General Data Protection Regulation ("GDPR")

- Applicable to all organisations that process personal data of EU nationals, including organisations outside EU
- Approved in April 2016
- Two year transition period → binding 25 May 2018
- Significant increase in sanctions (up to €20m / 4% of global turnover)

Security measures apply both to personal data and other critical data.
Welcome to the Channel Islands
Perfect storm

Why is this important?

4.3 million phishing attempts / hour
1.8 million malware attacks / hour
74% UK SME companies report breaches
20% of all attacks target SMEs
The cost of an attack often exceeds £300k

Source: EU, McAfee, UK Gov

And regulations…

Good security practices are needed to protect the information
You will be accountable!
Questions we ask related to GDPR/cyber

- Personal data?
- What are “logical” personal data registers?
- Who should own the data?
- What policies are needed?
- What are the responsibilities?
- Is training needed?

- What contracts should be amended?
- What is your policy on data retention?
- What logging and audit trail are needed?
- How do you meet the right of access/right to be forgotten/data portability?
- What are your detection and forensic capabilities?
- User management?
Implications in the Channel Islands

Banks

Investment Advisers

Investment Managers

Boards

Web, mobile services, social, email etc.

IT Vendors

Trust / Fund Service Providers

Beneficiaries

Settlers

Regulators

Investors

Registries
Key questions to be addressed

**Business processes**
- What are the business processes processing personal data?
- What type of data is that?
- Who are the participants in the process?
- What are the IT systems involved?

**Product/service information**
- What personal data is stored in association to products/services?
- IT systems and participants?

**Information flows**
- What are the information flows between services?

**Outsourced services**
- What processes or services are outsourced?
- To whom and where?

**Access to information**
- Who has access to the information?
- What is the purpose?
Know where you are

Sanctions
Know where you are (cont’d)

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>MATURITY LEVEL 1 ADHOC</th>
<th>MATURITY LEVEL 2 INITIAL</th>
<th>MATURITY LEVEL 3 CONTROLLED</th>
<th>MATURITY LEVEL 4 MONITORED</th>
<th>MATURITY LEVEL 5 OPTIMISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOVERNANCE AND OPERATING MODEL</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVENTORY/ DATA MAPPING</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REGULATORY CHANGE</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RISK AND CONTROL</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFORMATION LIFECYCLE MANAGEMENT</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLICIES</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROCESSES, PROCEDURES, TECHNOLOGY</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECURITY FOR PRIVACY</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>THIRD PARTY MANAGEMENT</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRAINING AND AWARENESS</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MONITORING</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INCIDENT MANAGEMENT</td>
<td>CURRENT STATE</td>
<td>CURRENT MATURITY GAP</td>
<td>DESIRED STATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Efficiency
Jersey stats

Guernsey stats unavailable at this time

- **JFSC**: 4,000 attacks per day (spikes up to 12,000)
- **States of Jersey**: estimated at 10% of the JFSC’s threat level
- **Jersey Police**: receives significant cyber crime reports, with huge increase year on year and they estimate that this is significantly under reported
- Relatively **low awareness** covering cybersecurity (95% of breaches involved human error in 2014)
- **NO** local centralised emergency operation
Threats to the Channel Islands

Locally, we have seen a sharp increase in:

- Whaling
- Distributed denial of service
- Insider threat

- Ransomware
- Data loss
Topical in the Channel Islands

- Awareness
- Information sharing
- GDPR
- ISO 27001 (information security management standard)
- SIEM (security information and event management)
Thank you