Cyber: A business perspective

BCS - Aberdeen

—

October 2016

George Scott

Director, Cyber Security

T: +44 (0)78 2787 4466

E: George.Scott@KPMG.co.uk

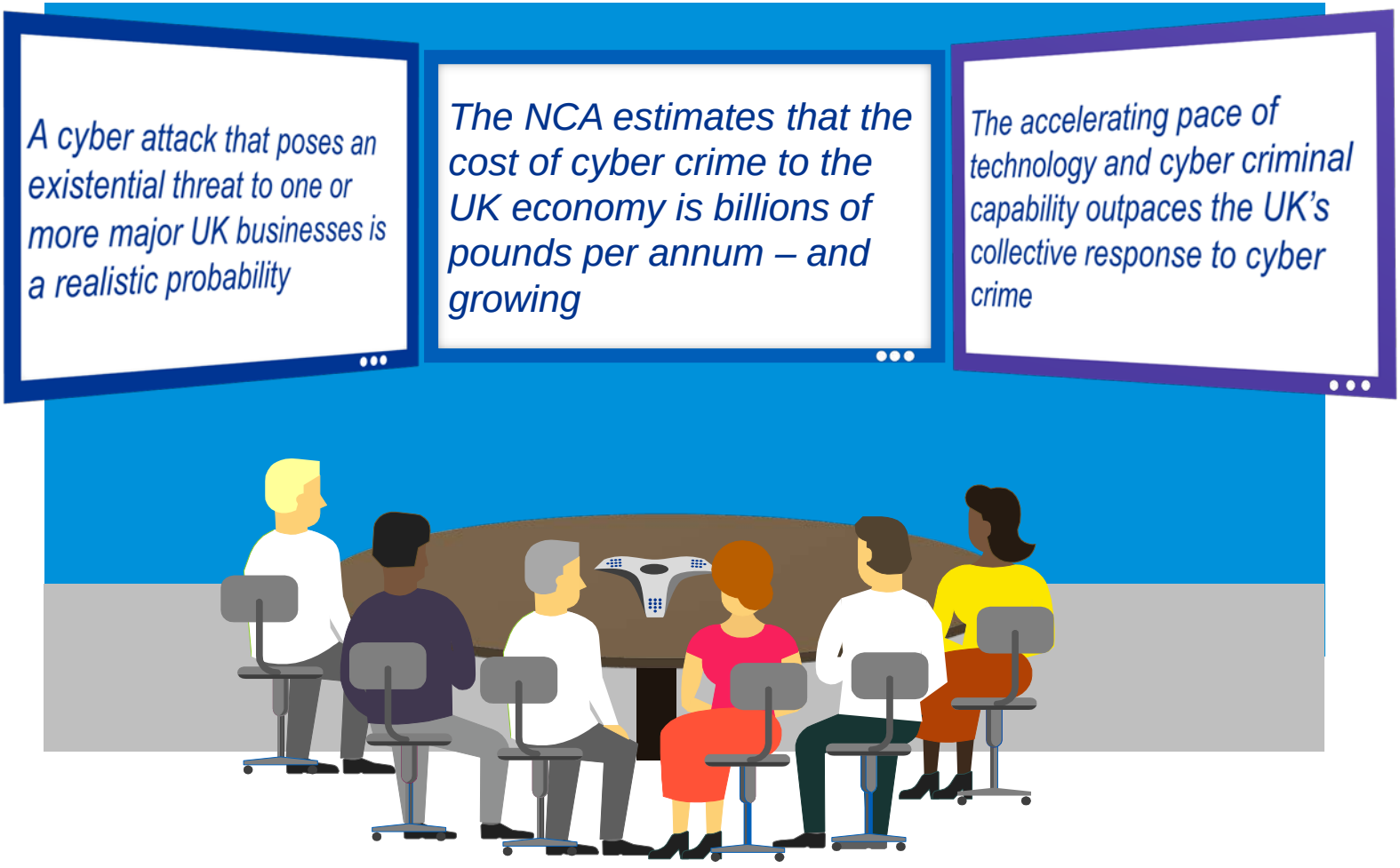
Agenda:

1. Combatting Cyber Fatigue!
2. Taking the Business Perspective
3. Privacy & the GDPR

KPMG

Combatting Cyber Fatigue!

NCA: Cyber Crime Assessment 2016



What's behind the headlines?

Hackers target Garda Síochána computers

7 August 2016

An investigation has been launched following an attempt to hack into the Garda Síochána (Irish Police) computer system.

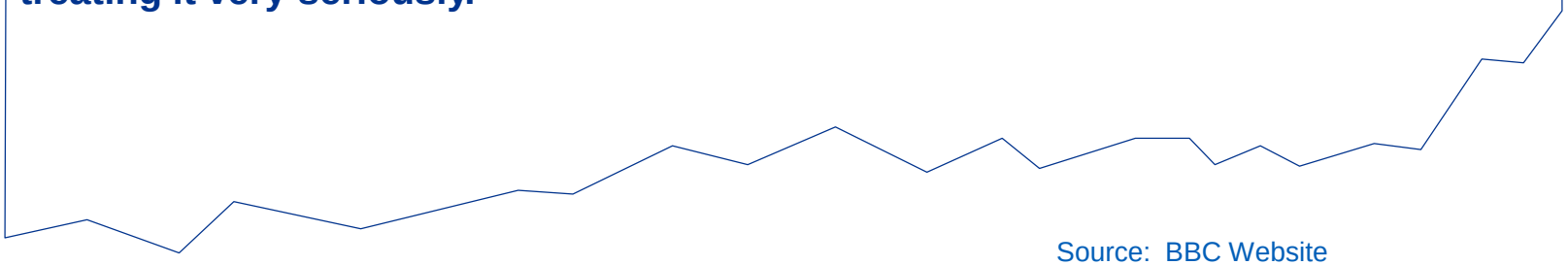
The incident forced the shut down of a number of internal systems last week according to Irish broadcaster, RTÉ.

It is not clear who was behind the attack.

The force's IT security team had not previously seen the type of threat involved.

The garda computer systems contain highly sensitive data ranging from open criminal investigation files to data relating to members of the public and staff.

It is understood no data was compromised in the attack but garda management is treating it very seriously.



Source: BBC Website

What's behind the headlines?

'Project Sauron' malware hidden for five years

9 August 2016

A sophisticated form of malware known as Project Sauron went undetected for five years at a string of organisations, according to security researchers.

The malware may have been designed by a state-sponsored group.

It can disguise itself as benign files and does not operate in predictable ways, making it harder to detect….

……The malware can steal files, log all keystrokes and open a "back door" allowing wide-ranging access to the compromised computer, according to Symantec.

Project Sauron did not share any code with other known examples of similarly powerful malware, said Kaspersky's director of threat research Costin Raiu.

"It really stands out by itself as something very, very sophisticated," he told the BBC.

Source: BBC Website

What's behind the headlines?

Could online bug hunting make me rich?

5 August 2016

I'm going to have a good look for cross-site scripting bugs on popular websites.

This is more than just a way to fill an idle hour. More and more security researchers are spending time finding and reporting bugs so they can be fixed. Many companies now run bug bounty programmes that pay people to disclose errors responsibly so they can be fixed, rather than exploited.

Apple is the latest to launch such a programme, years after tech rivals such as Facebook and Google. The smartphone giant offers a top reward of $200,000…

…."There's a critical talent shortage globally," says Casey Ellis, who started the Bugcrowd site. It now has 30,000 skilled hackers on its books who help to find security bugs on the web.

"At the moment there are just not enough good guys to go around," he says, making me wonder if I can join their ranks.

Source: BBC Website

A thriving cyber crime market ....on the dark web!

Single UK MasterCard	**$40**
Popular US email account (Gmail, Hotmail, etc)	**$129**
Corporate email account	**$500 per mailbox**
UK Passport scan	**$25**
$27,000 Bank Account transfer (UK Bank)	**$2,000**
Computer IP address	**$90**
Hacker tools – Remote Access Toolkit	**$5-$10**
DDoS attack	**$5-$10 per hour**
Hacking Website (and stealing data)	**$350**
Company dossier (lease agreements, tax info, etc)	**$550-$850**
ATM skimming device	**$400-$1,775**

Source: Underground Hacker Markets – Annual Report 2016

5 Ways to Combat Cyber Fatigue

KPMG

Taking the Business Perspective

Cyber Risk

To manage cyber risk effectively the business will need to understand several factors:

THE THREAT

- A variety of threat actors
- Identifying the threat actors relevant to the business and their intent
- The likelihood of being a target

THE VALUE OF THE ASSET

- Operational and Intellectual property
- Financial data
- Strategic plans and business critical information
- Customer and personnel data

THE IMPACT OF A CYBER INCIDENT.

- Market Value and Share Price
- Reputation
- Competitive Advantage
- Market Share
- Disruptive investigation

THE BUSINESS BENEFITS OF MANAGING CYBER RISK

- Enhanced corporate governance
- Managing emerging threats such as cyber-based threats
- Maximise commercial opportunities
- Satisfy regulators

Assets at risk

What are we trying to prevent?

Theft of client information

Names and contact info | NI numbers | Investment details

Theft of intellectual property

Investment strategy | Business plans | Allocations

Theft of corporate data

Employee data | Payroll data

Denial of service

Access to funds | Communication channels

Supplier compromise

Administrators | Service providers | IT suppliers

Data manipulation

Threats

Who would target you and why?

Organised crime – Global, difficult to trace and prosecute

Motivation: Financial advantage

Impact to business: Financial loss

Competitors – Competition or rivalry

Motivation: Gain business edge

Impact to business: IP theft, reputation damage

The insider – Intentional or unintentional

Motivation: Grudge, financial gain

Impact to business: Distribution or destruction, theft of information, reputation loss

Hacktivism – Hacking inspired by ideology

Motivation: Shifting allegiances – dynamic, unpredictable

Impact to business: Public distribution, reputation loss

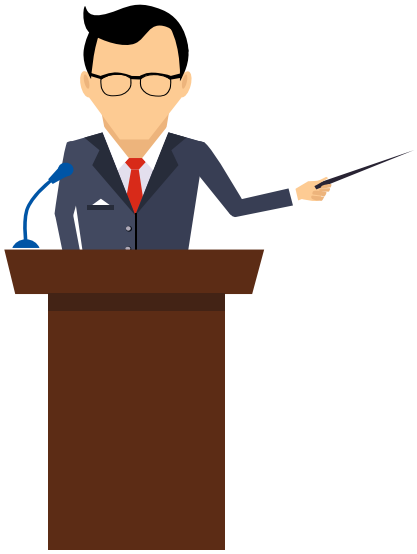
State-sponsored – Espionage and sabotage

Motivation: Political advantage, economic advantage, military advantage

Impact to business: Disruption or destruction, theft of information, reputational loss

Impact of a breach

“WHAT WILL THIS MEAN?”



- Financial loss
- Share price
- Reputational damage
- Loss of investor and customer confidence
- CEO exposure
- Regulatory scrutiny
- Loss of competitive advantage
- Missed business opportunities
- Business disruption
- Management focus shifts
- Expensive transformation programme

Key questions to ask...

CYBER ESSENTIALS

Firewalls	Anti-Virus	Patching	Passwords	Backups	Education/ Awareness

More demanding questions to ask...

Risk Management	Additional Protection	Access Management	Threat Intelligence	Red Teams and Exercises	Cyber insurance	Third Party Security

The most demanding questions to ask...

How do we pool and share intelligence?

How do we stop criminals exploiting our information?

How do we build a cyber resilient organisation?

How do we detect and counter unusual activity?

What is the return on our investment?

How effectively do our defences counter the threat?

What about the wider community?

End to end security | Behavioural monitoring | Community intelligence | Active cyber defence | Cyber resilience | Portfolio optimisation

Effective cyber risk management

Any approach to manage cyber risk should be:

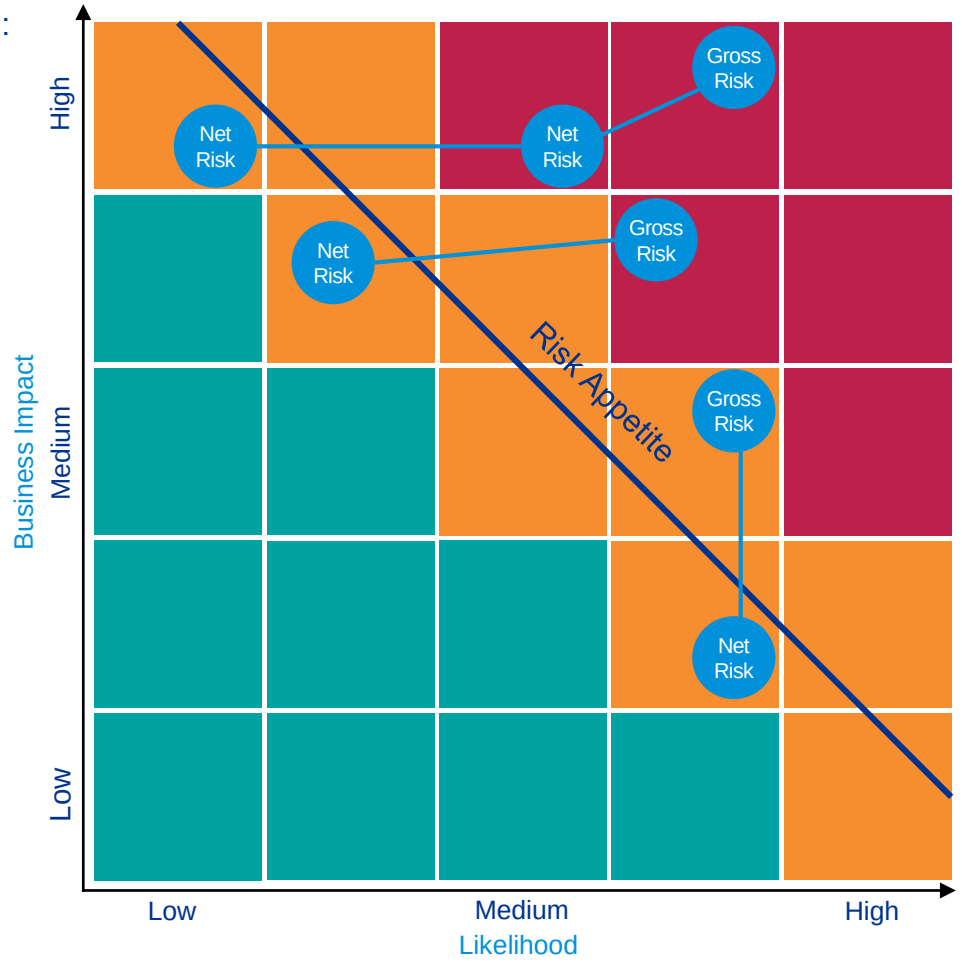
Proportionate to level of risk within the organisation

Aligned with other business activities

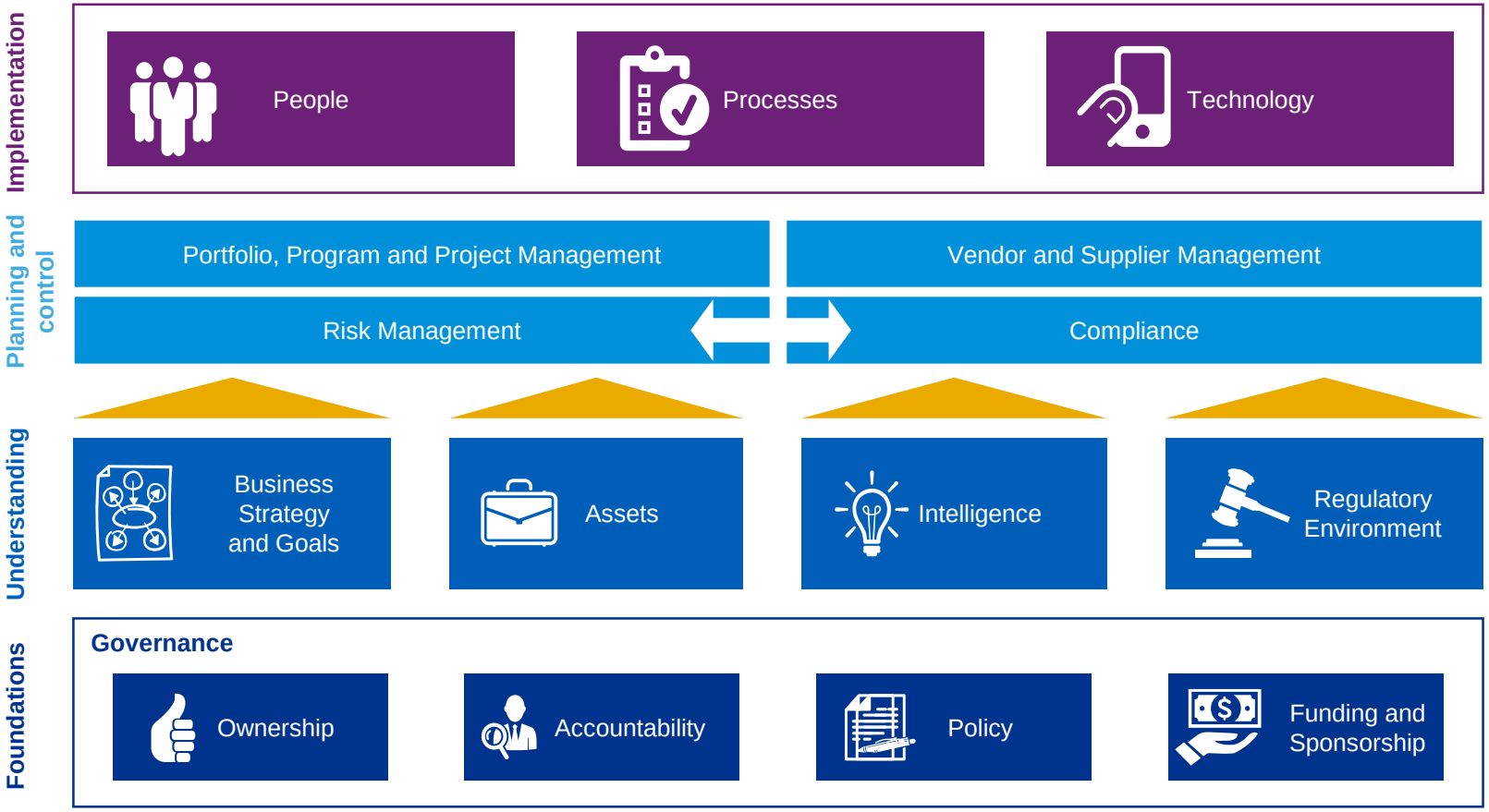
Comprehensive, systematic and structured

Embedded within business processes

Dynamic, iterative and responsive to change



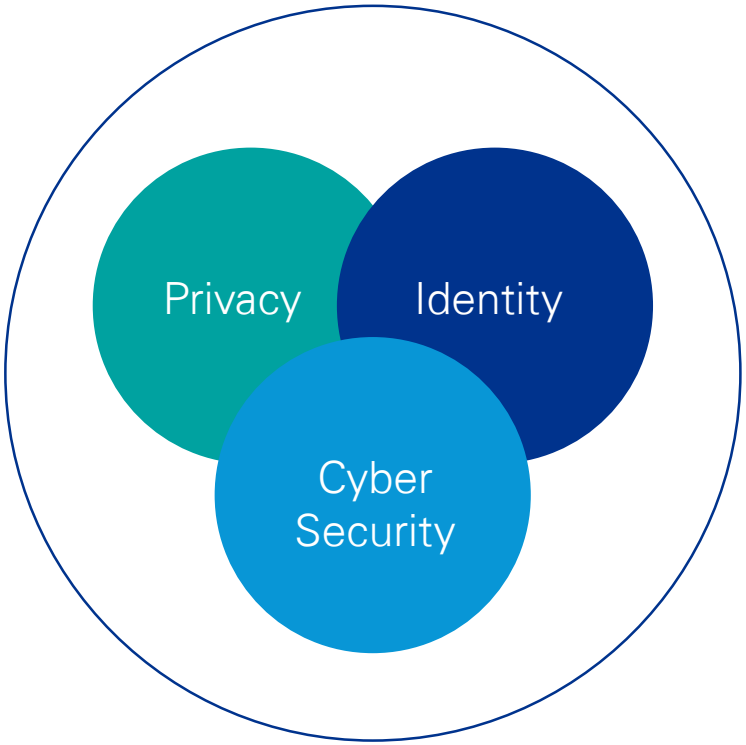
KPMG Cyber Risk Framework



KPMG

Privacy & The GDPR

Privacy: What is it?



"Privacy encompasses the rights and obligations of **individuals** and **organizations** with respect to the collection, use, retention, disclosure, and disposal of personal information."

The American Institute of Certified Public Accountants

GDPR: What are the main changes?

	Current Law	GDPR
	**Fines** Fines vary by jurisdiction (e.g. **UK £500,000)**	**Fines** A tiered fining structure depending on infringement. Level 1 is **2% of global turnover** or €10m (whichever is higher). Level 2 is **4% of global turnover** or €20m (whichever is higher)
	**Data Protection Officer (DPO)** Generally no requirement to appoint a DPO	**Data Protection Officer (DPO)** DPO **required** for "government bodies" and organisations conducting **mass surveillance** or **mass** processing of **Special Categories** of data
	**Inventory** **No requirement** to maintain a personal information inventory	**Inventory** Generally organisations will need a personal information inventory
	**Breach Notification** Generally there are no obligations to report breaches	**Breach Notification** Requirement to **report** Privacy breaches to the regulator within **72 hours** and potentially to the Data Subject
	**Security** **Vague requirements** around security (i.e. 'adequate level')	**Security** **Clear requirements** around monitoring, encryption, anonymisation and availability

GDPR: What are the main changes (cont.)?

Current Law	GDPR
Privacy Impact Assessments (PIAs) There is no mandated requirement to perform PIA's	**Privacy Impact Assessments (PIAs)** Organisations must perform PIAs if the activity is **considered 'high-risk'**
Data Subject's Rights Various rights, including right of access	**Data Subject's Rights** Rights extended to include **Data Portability** and the **Right to Erasure**
Sensitive Personal Data This covers things such as political opinions and religious beliefs	**Sensitive Personal Data** **'Special Categories'** replace 'sensitive personal data', and includes **biometric and genetic data**
Consent Potential to rely on **"implicit"** consent depending on jurisdiction	**Consent** Requirement to gain **unambiguous** consent (i.e. explicit)
Data Processors (DP) Processors are subject to limited scope and liability.	**Data Processors (DP)** Processors **are also covered in scope**. Controllers must conduct **due diligence** into processors suitability.

Thank you for listening!

BCS - Aberdeen

—

October 2016

George Scott

Director, Cyber Security

T: +44 (0)78 2787 4466

E: George.Scott@KPMG.co.uk