



Cyber threats and your business

Patrick Nuttall, CISSP, CISM, CBCI
Executive Advisor, Cyber Security
KPMG UK

Insurance Technology Forums
Q3 'Security Matters' Forum
23 August 2017

Cyber attackers and cyber attacks



Organised crime



Hacktivism



The insider



State-sponsored

Commoditised attacks



Hundreds of millions of victims
\$300–\$10,000
High impact

Targeted attacks



Tens of thousands of victims
\$10,000–\$1 million
High impact

High-end attacks



Dozens of victims
\$1 million–\$100 million
Extreme impact

Source: “Closing the gap – Insuring your business against evolving cyber threats, June 2017” from Lloyds of London, KPMG LLP, and DAC Beachcroft

Industry focus

The infographic is based on KPMG's analysis of publicly available references⁹ and KPMG's industry insights.

Key

- Primarily targeted
- Frequently targeted
- Occasionally targeted
- Rarely targeted

The order of the circles in the same category does not indicate relative frequency.

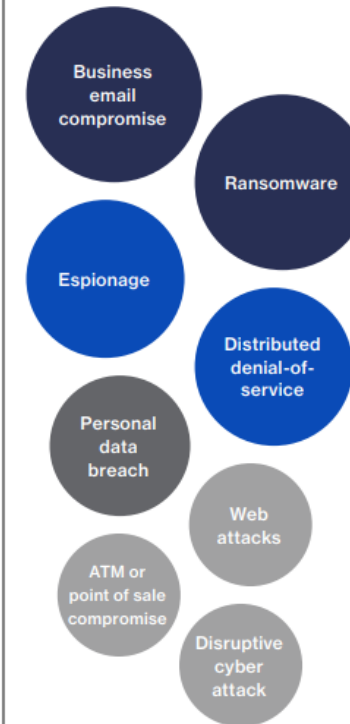
Financial services



Information technology

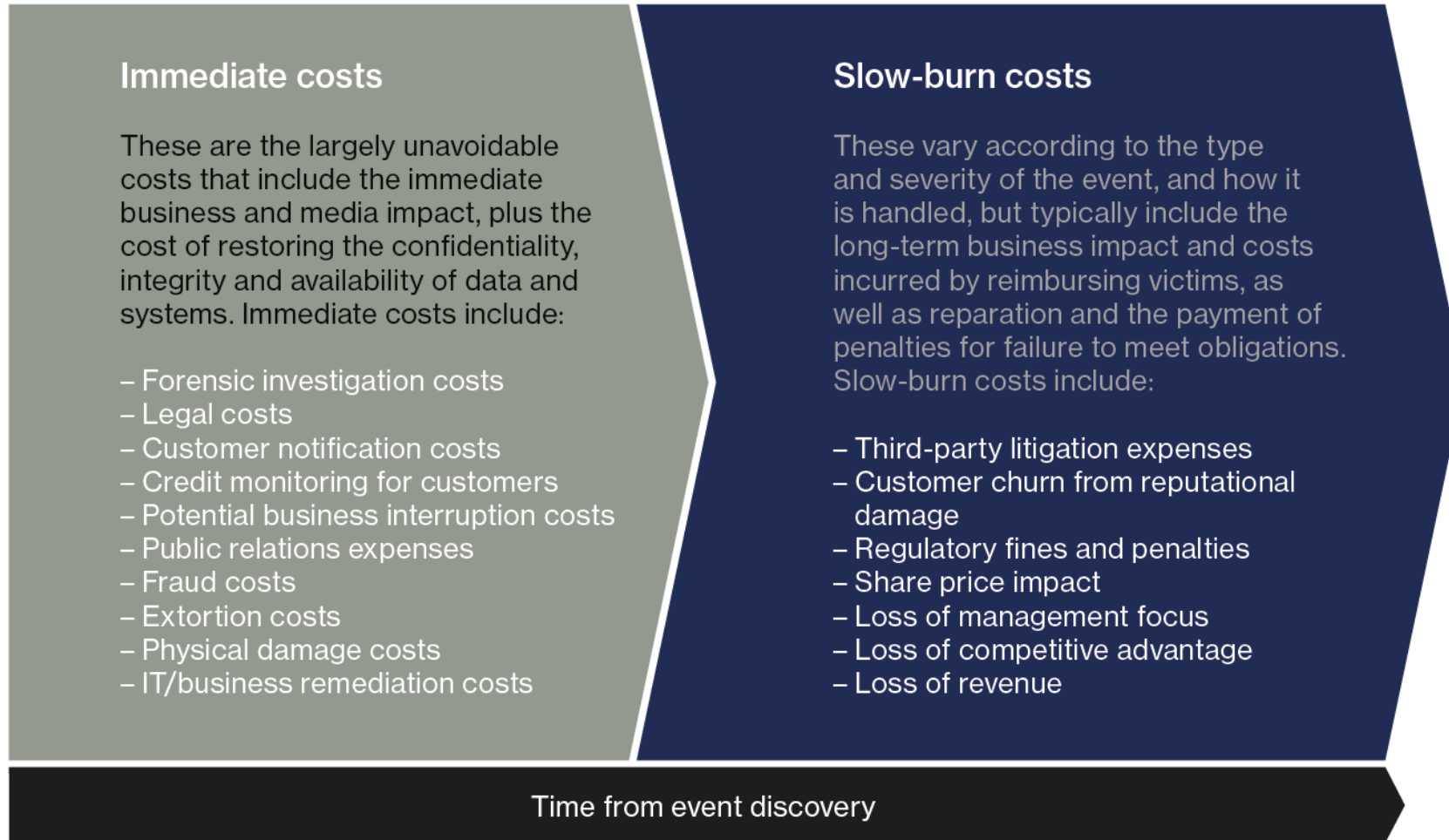


Professional services



Source: "Closing the gap – Insuring your business against evolving cyber threats, June 2017" from Lloyds of London, KPMG LLP, and DAC Beachcroft


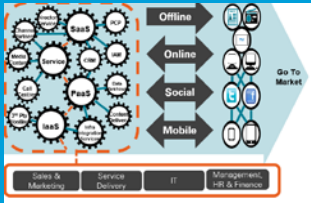

Cost of a cyber attack




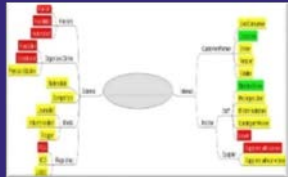

Source: “Closing the gap – Insuring your business against evolving cyber threats, June 2017” from Lloyds of London, KPMG LLP, and DAC Beachcroft

Developing a cyber strategy

Key Assets


Threat and risk assessment


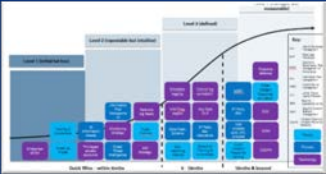

OSP	Baseline	Intermediate	Good	High
Programme	3.5	3.5	3.5	3.5
Business	4.0	4.0	4.0	4.0
People	3.0	3.0	3.0	3.0
Process	4.2	4.2	4.2	4.2
People	4.3	4.3	4.3	4.3
IT O&M	4.0	4.0	4.0	4.0

Gap Analysis / Penetration Testing





Cyber Strategy

What next?

- Understand the specific threats to your company, including both the immediate and slow-burn costs – everything from reputation as perceived by customers and the value of the data held, to supply chain vulnerabilities and business-leader profiles.
- Evaluate both current and future threats: underwriters will evaluate both so they can offer you the insurance cover that best suits your needs.
- Ensure all employees, including management, have a comprehensive understanding of the cyber threats your company faces and promote a cyber-risk management culture.
- Seek expert help when it comes to arranging cyber insurance to ensure that your risks are adequately covered.

Source: “Closing the gap – Insuring your business against evolving cyber threats, June 2017” from Lloyds of London, KPMG LLP, and DAC Beachcroft



© 2016 KPMG LLP, a UK limited liability partnership 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.



Thank you

Patrick Nuttall, CISSP, CISM, CBCI
Executive Advisor, Cyber Security
KPMG UK

T: +44 (0)7717 512486

E: Patrick.Nuttall@KPMG.co.uk



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 endeavour 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 LLP, a UK limited liability partnership 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.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.