www.pwc.com

State of the cyber threat and the consequences of inaction

Presented to:
Swiss Cyber Storm Event 2015

pwc

Agenda

1. Biography
2. Transformation
3. The threat
4. Threat actors
5. Forensic conclusions
6. Risk & impact: case histories

Biography

1

Brief biography

- Senior Managing Director of Cybercrime & Breach Response at PricewaterhouseCoopers LLP
- Previously CISO at Textron (Bell Helicopter, Cessna, EZGO, Kautex, Textron Systems, Textron Financial, Jacobsen)
- Over 20 years' experience in IT Security, Forensics and IT Audit
- Certification in IT Security, IT Forensics, IT Audit, IT Governance and IT Data Privacy
- A frequent speaker at CIO Talk Radio, CXO Magazine, CSO Perspectives, CISO Executive Summit, MIT CIO Symposium

Transformation

Unprecedented change

Witnessing the transformation from an IT- and productivity-driven era to one defined by cyber security risk management

This is happening because of a fundamental shift

Boards and management are seeing the results of decades of misaligned threat and risk dynamics and response

And they are seeing greater impact and potential impact

Era of executive and cyber transformation

Board meetings in 2010 and before

- 20 minutes with Audit & Risk Committees
- Cyber is an IT issue and relegated to CTO, CIO

90 minutes with full board and senior executives

Board meetings in 2014 and beyond

All things cyber have two high impact termination points

Regulation and litigation

Driving change

Frequency and complexity of attacks	Unprecedented levels and impact
Regulatory evolution	U.S. Securities and Exchange Commission 2011 Guidance, European Union Privacy Directive
Threat diversity and proliferation	Insiders and vendors/terrorists/nation-states/transnational organised crime/hacktivists
The Internet of Things	The interrelationships between previously unconnected elements

The threat

3

“On a scale of 1-10, U.S. preparedness for a cyber strike is about a 3.”

Gen. ***Keith Alexander,*** former head of the U.S. National Security Agency, in 2012

“It’s only a matter of the ‘when’, and not the ‘if’, that we are going to see something dramatic.”

Admiral ***Michael Rogers,*** director of the U.S. National Security Agency, in a November 2014 warning about the cyber threat against the US from other nations

“… the most significant incident of domestic terrorism involving the grid that has ever occurred in the US.”

Former Federal Energy Regulatory Commission Chairman ***Jon Wellinghoff*** on the May 2013 assault on the Metcalf substation in California’s Silicon Valley

THE WALL STREET JOURNAL.

"On a visit to our offices last year, a U.S. lawmaker with knowledge of intelligence affairs explained that, when it comes to cyber-espionage, there are only two kinds of American companies these days: Those that have been hacked, and those that don't know they've been hacked."

The Wall Street Journal
"Barbarians at the Digital Gate"

“Without any sense of restraint …”

U.S. military official

Cyber attacks are on the rise

U.S. Nuclear Security Enterprise

→ 10 million attacks daily

→ 1 in a 100 are successful: that’s 1,000 successful attacks a day

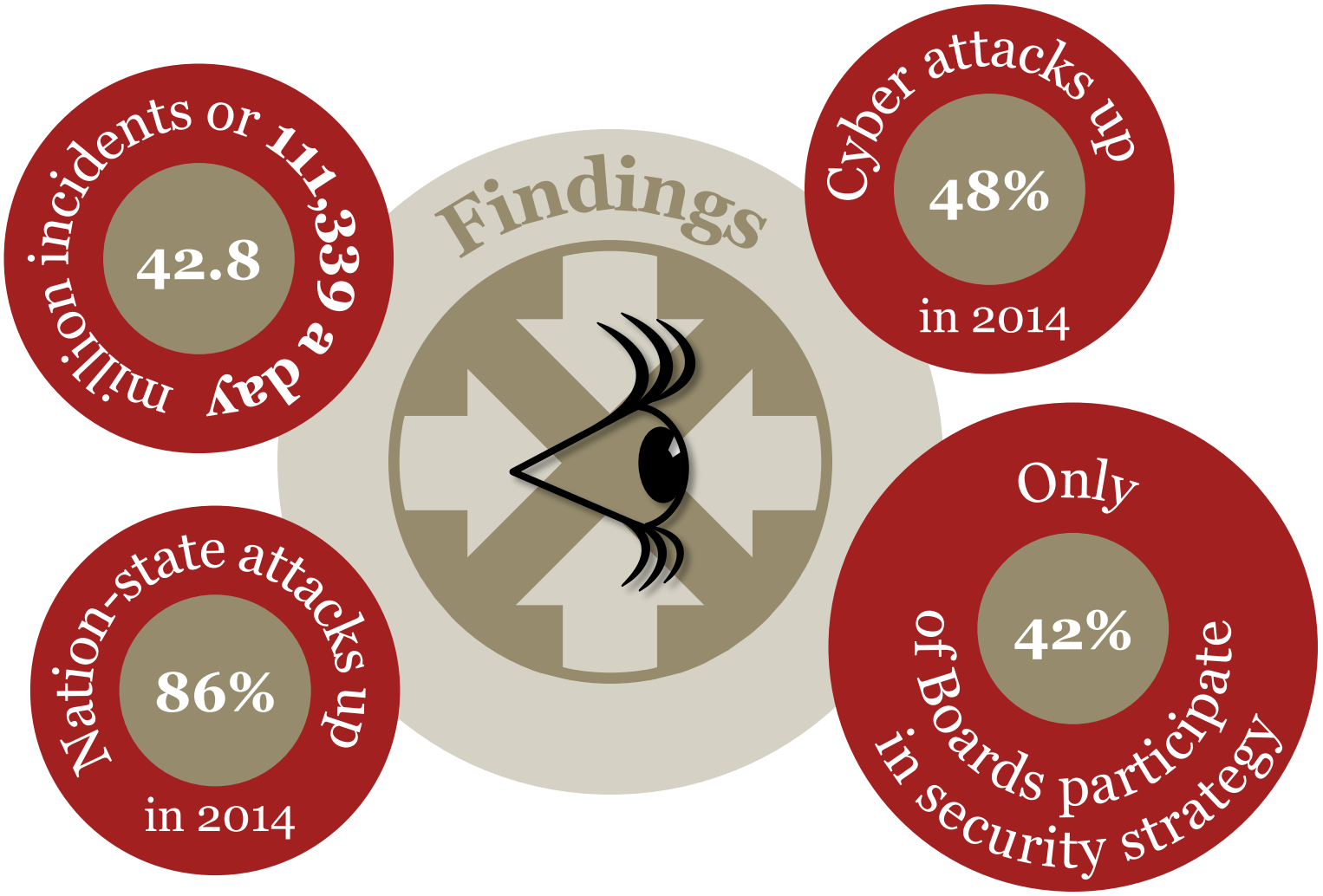
U.S. Navy Intranet

→ 87 Million attacks monthly

17-fold increase in cyber attacks between 2009 and 2011

U.S. FEMA reports 650% increase in cyber attacks 2006 to 2010

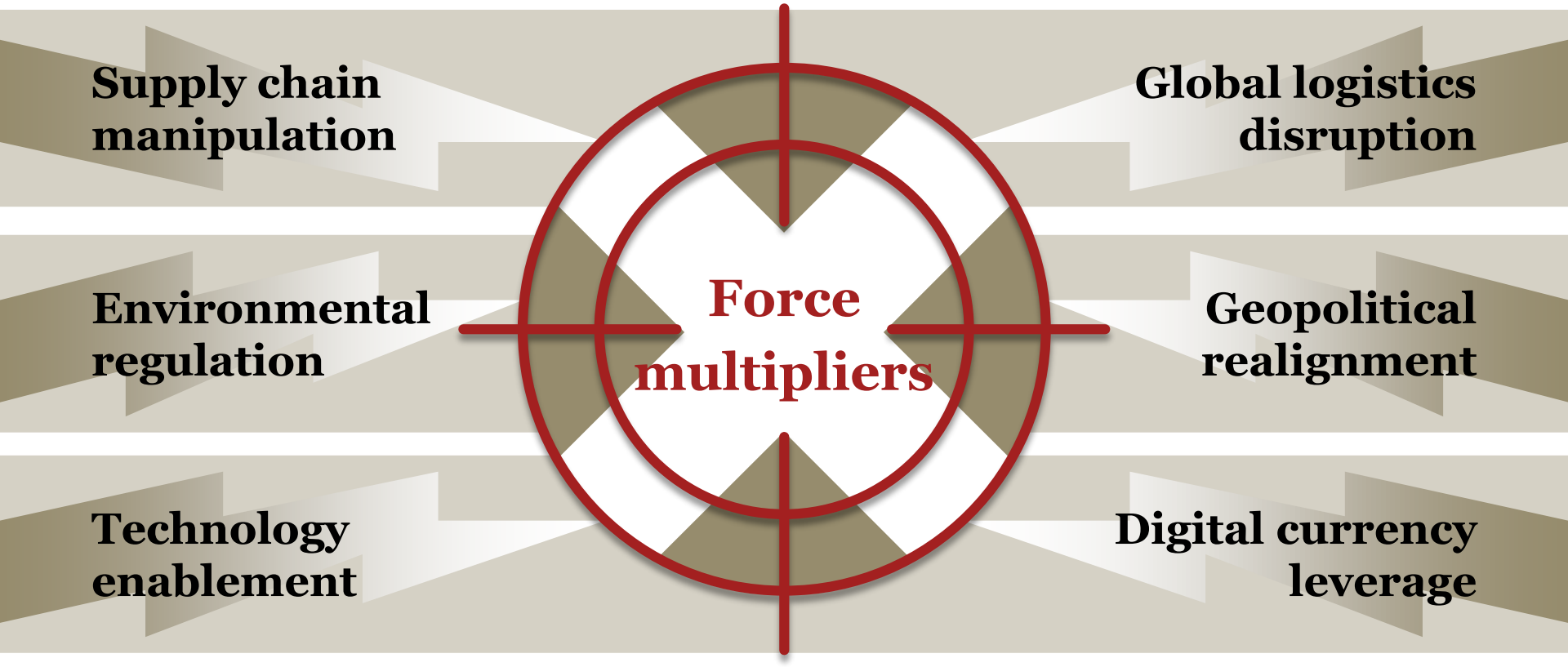
From a recent PwC Cyber Crime Survey



Threat actors

Principal cyber attack actors

Nation-state cyber attacks are grounded in strategic economic expansionist impact

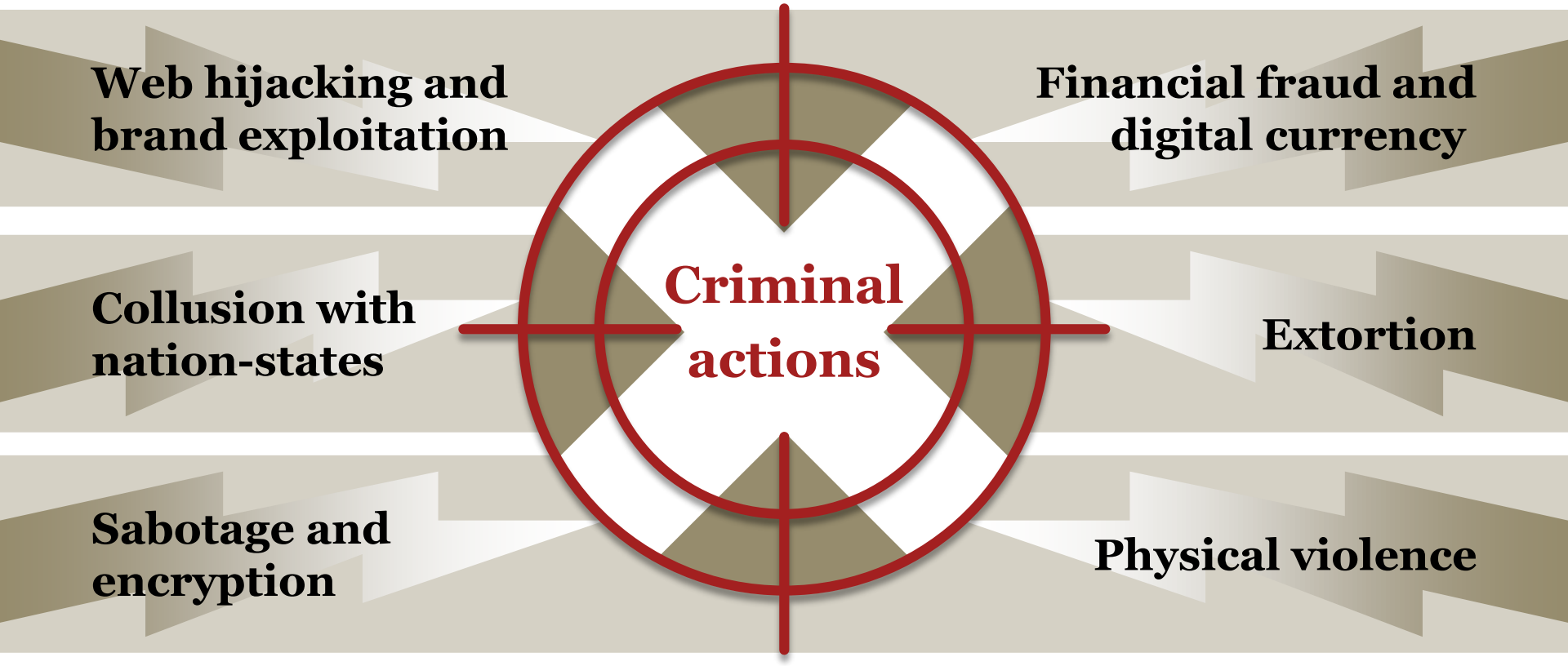


Watch for strategic indicators that will alter the status quo

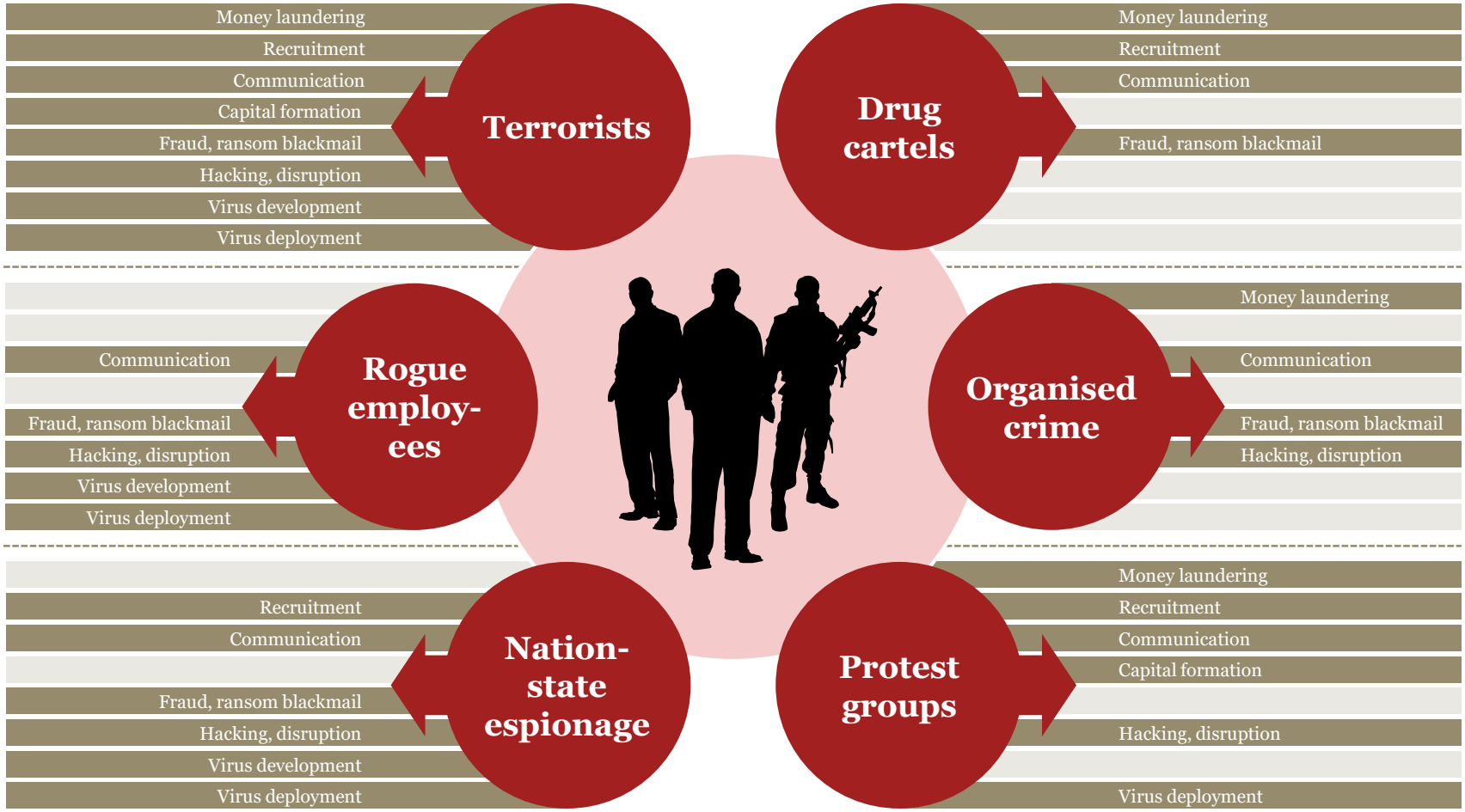
Think about key nation-states as economic competitors, not strictly flagged political, military, intelligence, and diplomatic powers.

The key to future global economic risk will be influenced by logistics technology, global supply chain disruption strategy, environmentally clean shipping regulation and unregulated digital currency leverage in support of geopolitical realignment.

Transnational criminal cyber attacks are tactical



How adversaries use the internet



Forensic conclusions

5

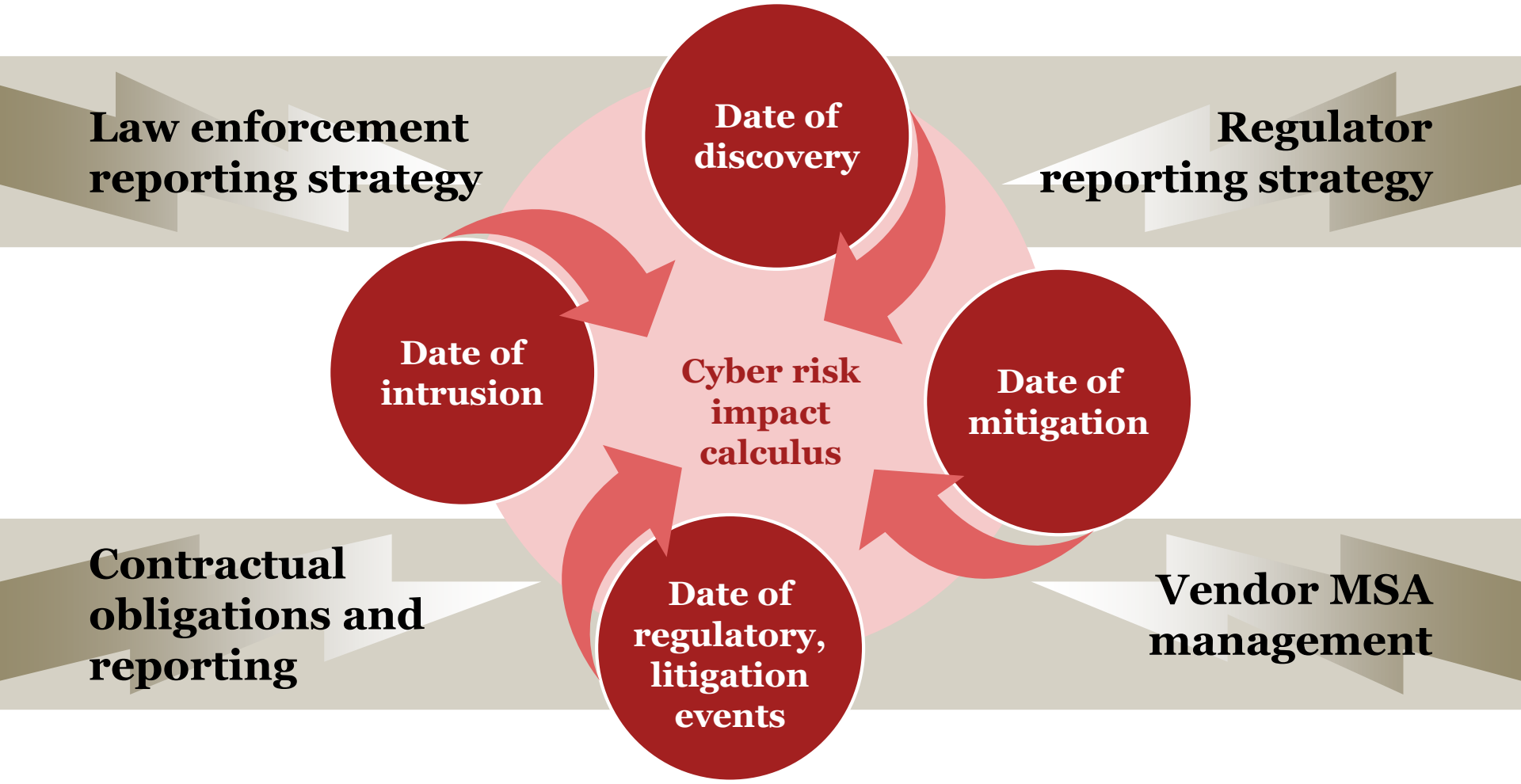
Attack trends

- Infiltrations occur without detection
- Protracted periods of adversary intelligence collection
- More than 200 days between date of intrusion, date of discovery
- 5-7 years not uncommon
- Correlation between date of intrusion, date of discovery
- Sabotage may include use of military grade encryption
- Look for Internet of Things to enable crippling and even destruction of industrial smart-plants and smart-buildings
- May include catastrophic events including personal injury, loss of life, toxic spills
- Increasingly aggressive nation-state attacks

What information do they want?

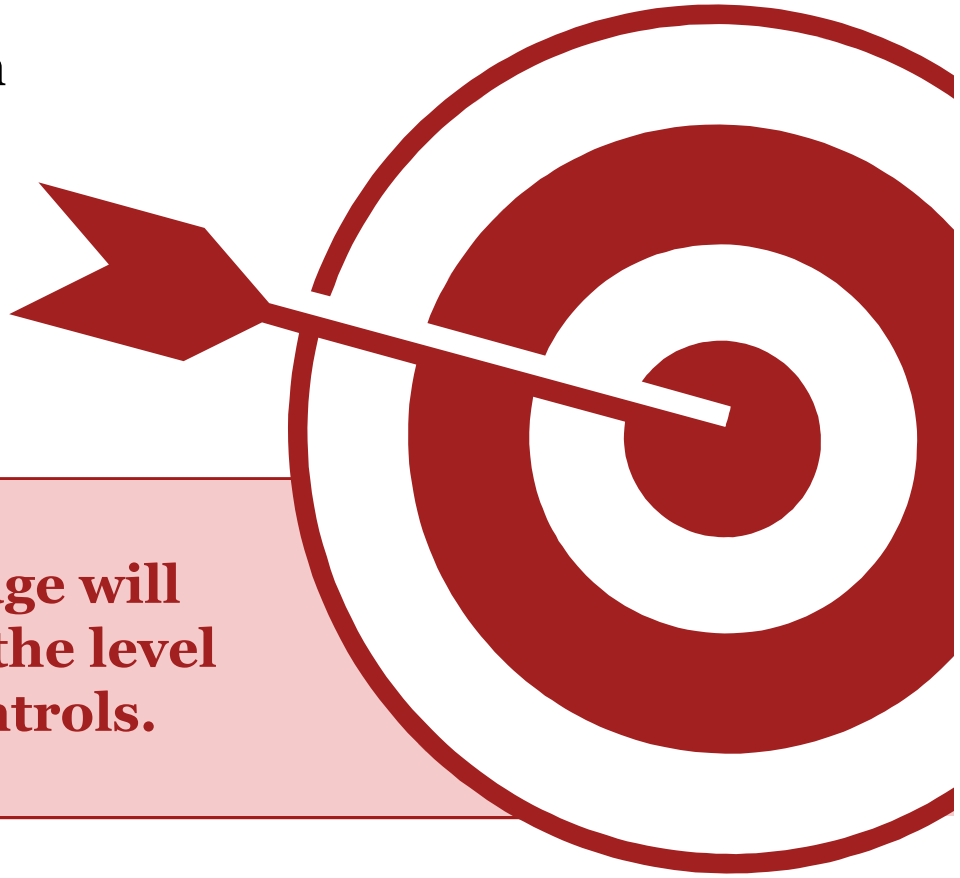
- Healthcare data
- Financial data
- Intellectual property and trade secrets across multiple sectors
- Merger and acquisition information
- Marketing data
- Cost data
- Shipping and logistics data
- All data may prove useful, even encrypted data

Managing cyber risk outcomes – key elements



Internet-accessible controls

Internet-accessible controls can be hijacked by nation-states and organised crime syndicates – and even individual rogues – intent on sabotage and extortion.



Digital competitor sabotage will rise commensurate with the level of Internet-accessible controls.

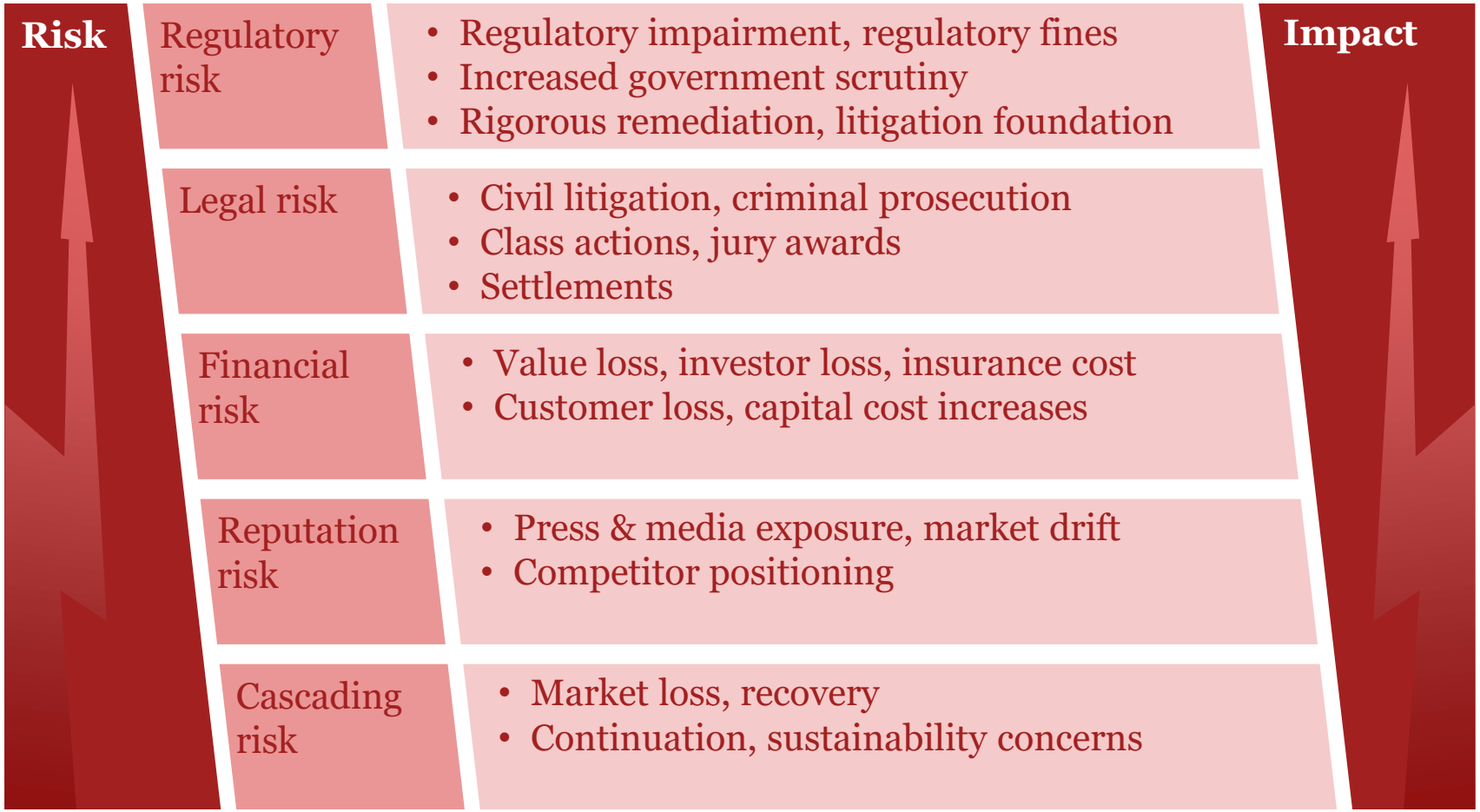
Target range

Cyber attackers are compromising

- Networks of industrial control systems
- Electrical grids
- Nuclear power plants
- Air traffic control
- Subway systems
- Financial systems
- Business strategy and operations

Risk impact: case histories

AT

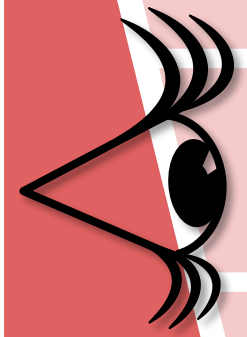

Risk
Impact
Regulatory risk
• Regulatory impairment, regulatory fines
• Increased government scrutiny
• Rigorous remediation, litigation foundation
Legal risk
• Civil litigation, criminal prosecution
• Class actions, jury awards
• Settlements
Financial risk
• Value loss, investor loss, insurance cost
• Customer loss, capital cost increases
Reputation risk
• Press & media exposure, market drift
• Competitor positioning
Cascading risk
• Market loss, recovery
• Continuation, sustainability concerns

Case history:

Organised crime – how one U.S. company was impacted by money laundering scam

Personal brand compromise	Corporate web site compromise	TOC franchise strategy	Proximity wireless attack

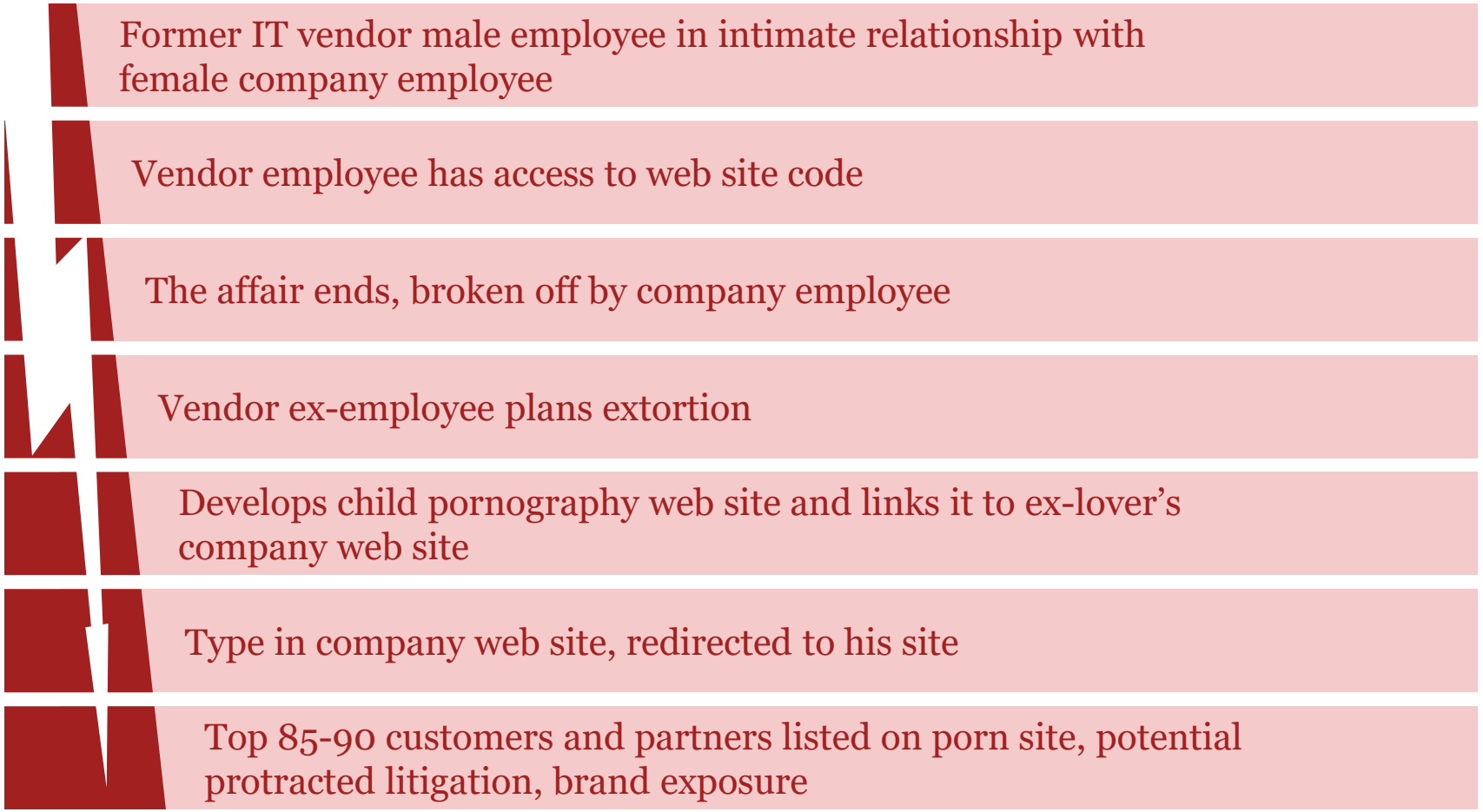
Third-party vendor linked to original breach



Extortion demand:
USD 1M to deactivate each website
Up to 100 websites

Impact analysis:
Executive displacement |deficient security | increased federal scrutiny | possible foreign agent penetration

Case history—insider/third-party vendor and lone wolf



One question I always ask the board and executive management

Contact information

Richard Dorough

Sr Managing Director, Cybercrime & Breach Response
PricewaterhouseCoopers LLP
301 Commerce Street Suite 2350 Fort Worth, TX. 76008
Mobile +1.817.296.2835 Richard.E.Dorough@pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

©2015 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.