Hewlett Packard
Enterprise

Can we insure against cyber security disaster?

Secure South West 6

9th February 2015

Agenda

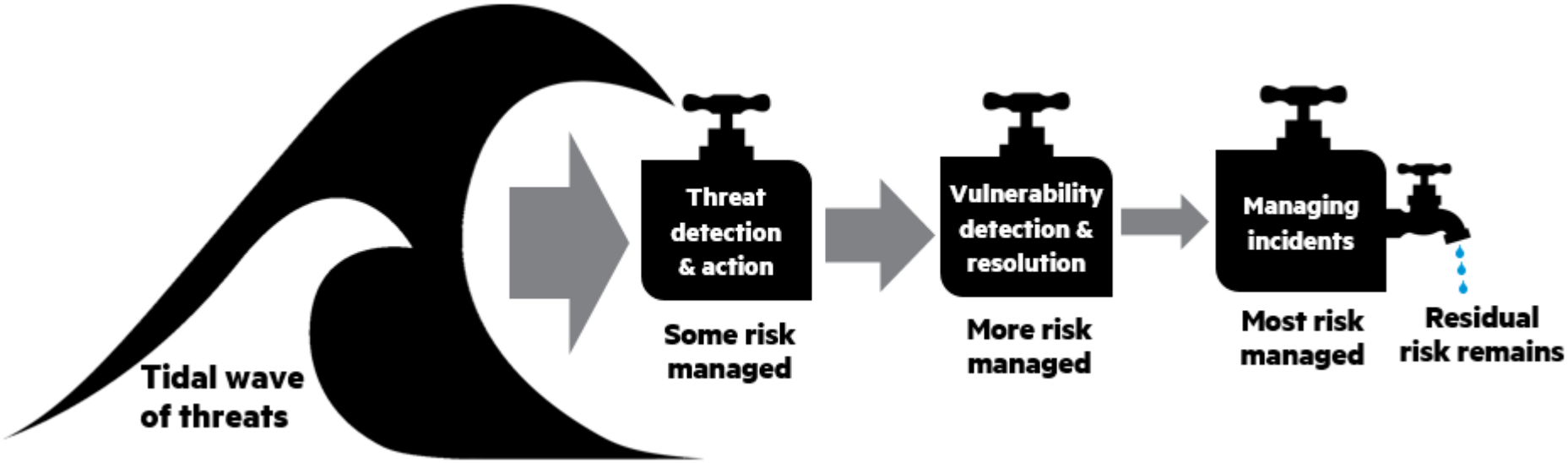
- Options for dealing with cyber risk
- Cyber insurance – the state of the market
- Cyber insurance challenges and potential
- Meeting the challenges
- Looking to the future

What is cyber risk?

Cyber risk definition:

Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

Source: ISO/IEC 27005:2008



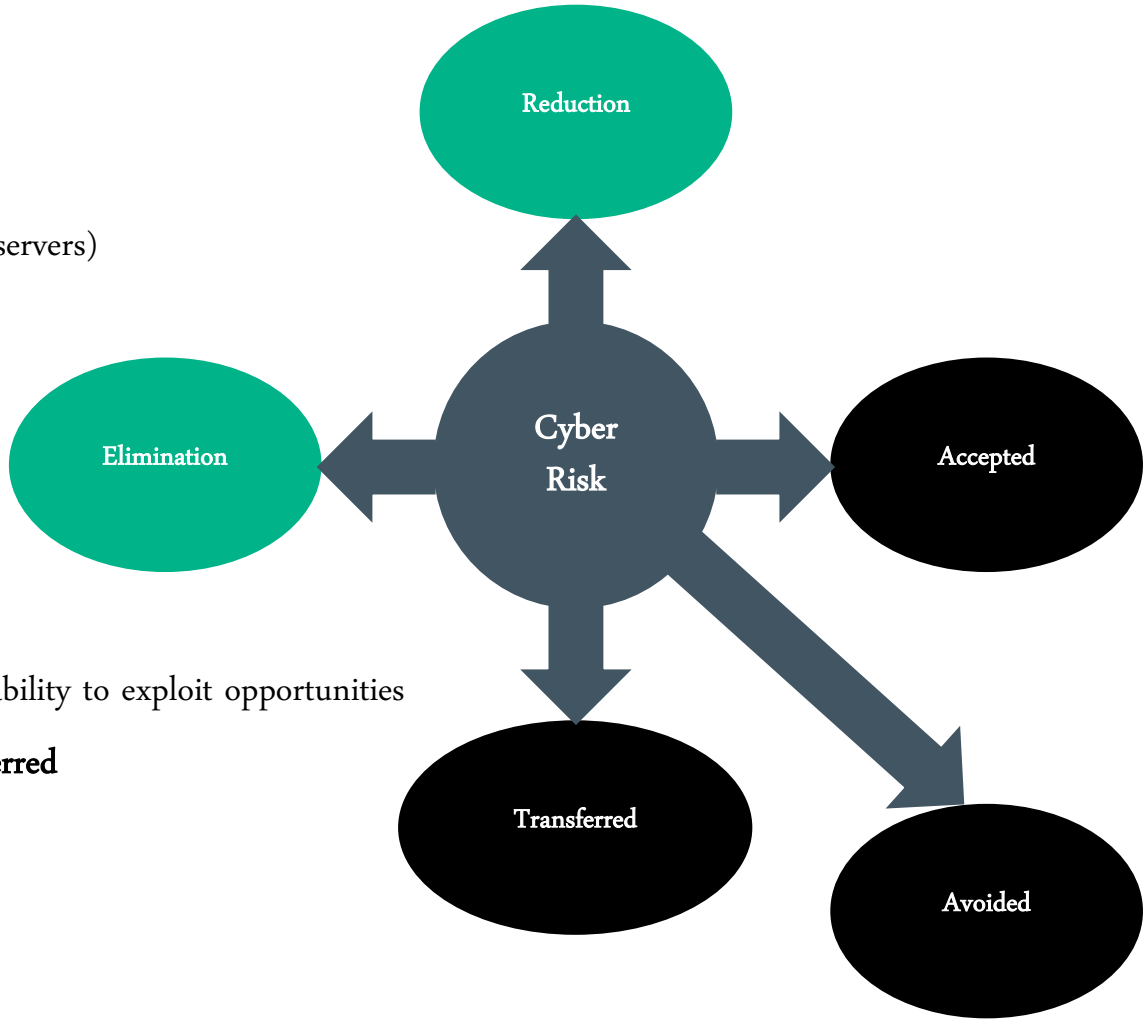
Options for dealing with cyber risk

IT approach:

- Assets at risk are technical (applications and servers)
- Focus is on threats and vulnerabilities
- Risk **reduction** or **elimination** is the aim

Business approach:

- Assets at risk are business-related
- Focus is on harm to business objectives and ability to exploit opportunities
- Risks can also be **accepted**, **avoided** or **transferred**



Source: Gartner Symposium – Assessing and Communicating Information Security Risks, October 2011

Hewlett Packard Enterprise

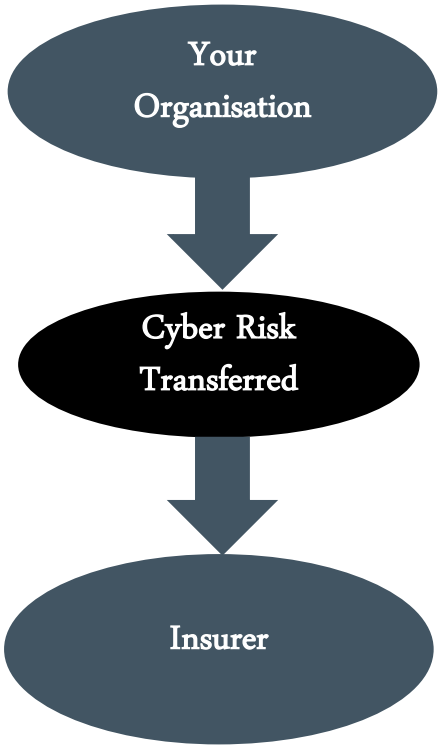
What is cyber insurance?

Businesses should consider cyber insurance as an effective component of a cyber-risk management strategy.

Managing cyber risks with insurance. PWC report June 2014.

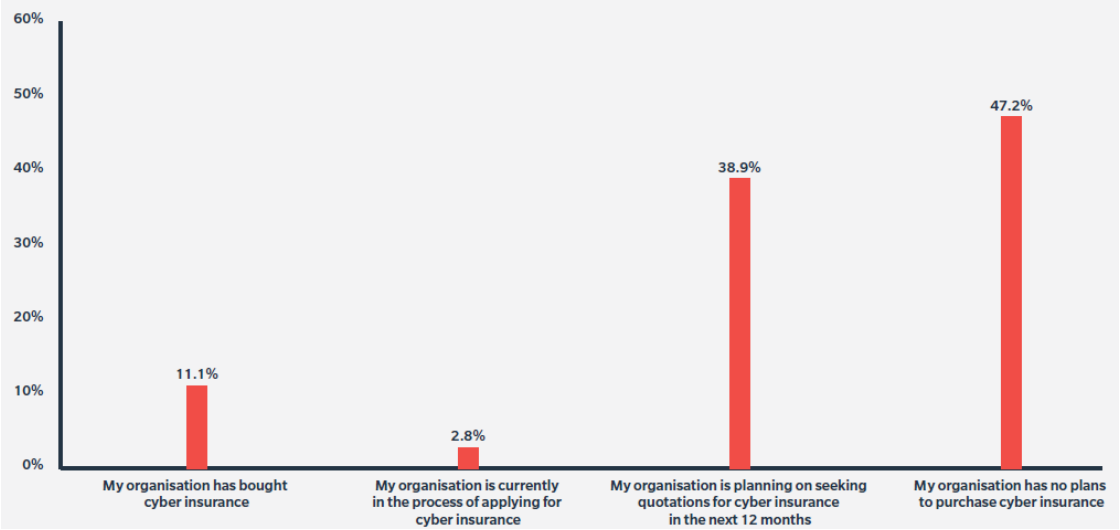
Cyber insurance transfers cyber risk from your organisation to the insurer:

- Risk transfer enables opportunities to be taken which would otherwise have to be either accepted or avoided.
- Risk is shared between insured and insurer



The cyber insurance market

- **Market growth**:
  2015 - $2.5 billion (90% in USA).
  2020 (predicted) - $7.5 billion.
- **Take-up currently low:**
  - nearly 50% of UK organisations have no plans to use cyber insurance
- **Not all liabilities currently insured:**
  - Covered:
    - Exposure of customer information
    - Business interruption.
  - Through other policies:
    - Computer crime/fraud.
  - Possibly covered:
    - Reputational loss.
  - Not usually covered:
    - Loss of intellectual property.

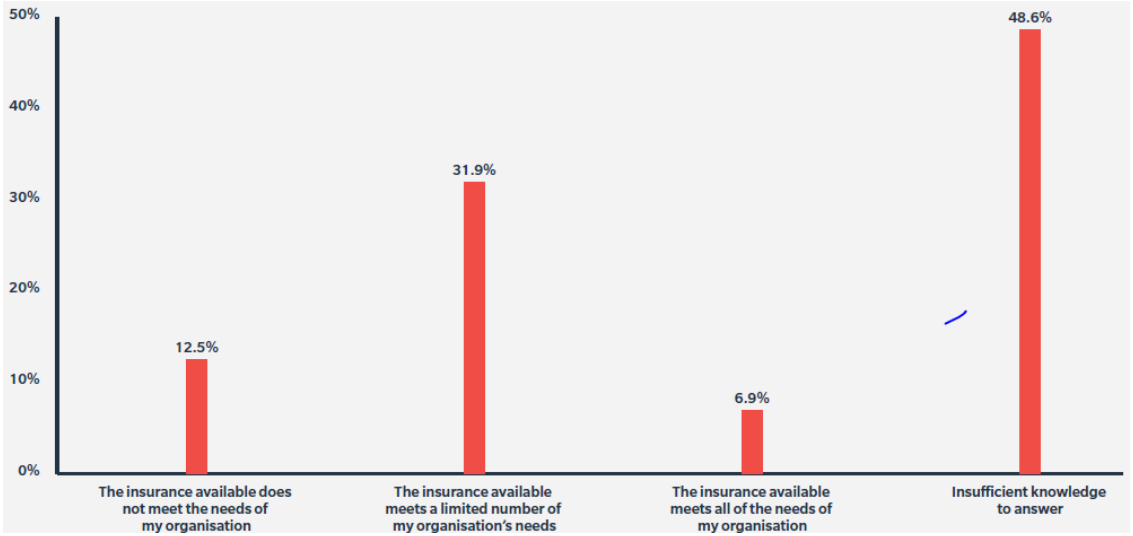


Source: UK 2015 Cyber Risk Survey Report. Marsh June 2015.

Hewlett Packard Enterprise

Why is take-up low?

- Cyber insurance covers only some cyber risks
- Policies can be complex – different risks covered by different policies.
- The cyber insurance market is still immature – insurers don't know how to calculate premiums.
- Organisations don't understand what cyber insurance can do
- Organisations don't understand enough about their cyber risk – and how to measure it



Source: UK 2015 Cyber Risk Survey Report. Marsh June 2015.

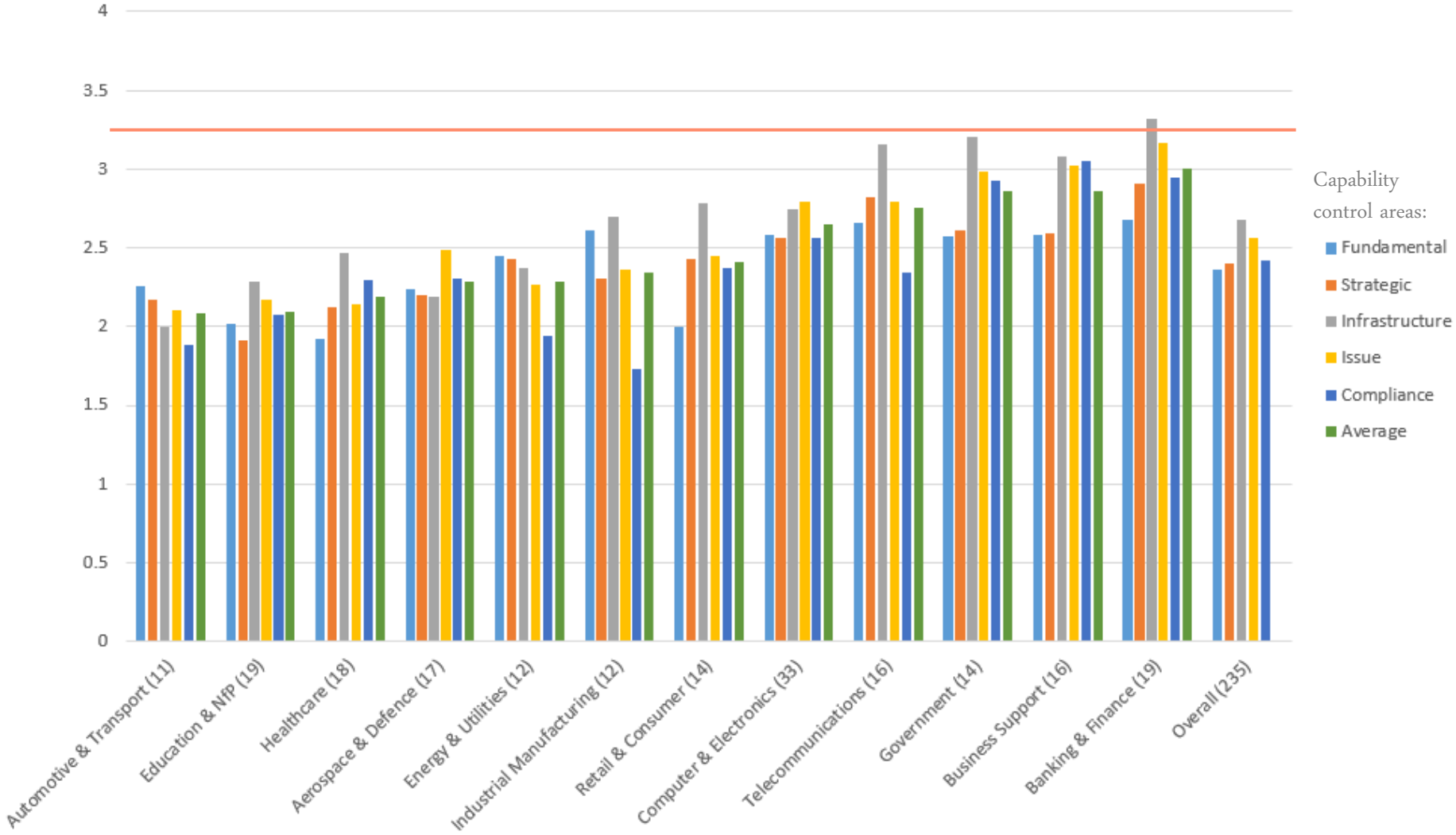
Cyber insurance challenges

- **Cyber risk exposure**:
  - $150 billion (globally)[1]
  - Insurers rate cyber as the biggest risk facing their industry[1].
- **Seen as low profile risk by business:**
  - Only 45.8% of UK companies have cyber as a "top 10" risk[2]
  - Only 19.4% of UK companies have Board-level ownership of cyber risk[2]
- **Legal and regulatory concerns:**
  - Mandatory reporting of cyber breaches
  - Fines for breaches
- **Cost of cover:**
  - 3 x that of other liability risks[1].
  - Rates for retailers up 32% in 2015[1].
- **Limited number of insurers:**
  - It's a new market
  - Traditional insurers can't calculate premiums
- **Insured limits are relatively low:**
  - In most cases below $100 million[3].
  - In 2014 Target dealt with a cyber attack that cost them $264 million. Their insurer paid $90 million[3].
- **Lack of digital forensics capability:**
  - Difficulty in identifying genuine cyber crime and tracking perpetrators

Sources:
1: Insurance 2020 and beyond. PWC 2015.
2: UK 2015 Cyber Risk Survey Report. Marsh June 2015.
3: Reuters Report October 2015.

Cyber risk challenge – poor security capability maturity

Please note that 3 is considered the acceptable maturity level



Source: HPE benchmarking survey data 2013-2015.

Cyber insurance has potential to drive improvements in:

- **Understanding of risk:**
  - Makes cyber security more of a Board-level issue
  - Enables business to see cyber security as a "normal" operational risk
  - Potential to manage risk when exploiting new opportunities
- **Security metrics and benchmarking:**
  - Calculating premiums requires actuarial data
  - Businesses will need to collect data and provide it to insurers
  - Insurers will collect data across insured sectors to enable anonymous benchmarking
- **Cyber security capability maturity:**
  - Premiums linked to security control measures implemented
  - Regular reviews of security capability linked to insurance renewal
  - Insurers will insist on minimum standards to reduce their liabilities
  - Availability of digital forensics capability

Meeting the challenges

Cyber insurance drives:	Cyber Risk and Insurance Challenges							
	Cyber risk exposure	Cost of insurance cover	Limited number of insurers	Legal & regulatory compliance	Low insured limits	Business ownership of cyber risk	Poor security capability maturity	Pursuit of cyber crime
Board-level understanding of cyber risk			X		X	X	X	
Managing opportunities by cyber risk transfer	X					X		
Gathering cyber security data	X	X	X	X	X	X	X	
Gathering sectoral benchmarking data	X	X	X	X	X	X	X	
Gathering security capability data		X	X	X	X		X	
Regular reviews of security capability		X	X	X	X		X	
Enforcing minimum cyber security standards		X	X	X	X		X	
Improved digital forensics		X	X		X			X

X = improvements that can address the challenges

Hewlett Packard Enterprise

Looking to the future

- **Understanding risk:**
  - Cyber risk is seen as a normal item on the risk register
  - Boards recognise they have to deal with it through risk management
  - Boards own the risk and drive cyber security awareness through the organisation
- **Security metrics and benchmarking:**
  - Security events and incidents are properly monitored and data is collected
  - Data is collected about threats and vulnerabilities
  - Data is shared to enable anonymous benchmarking
- **Cyber security capability maturity:**
  - Controls are implemented to meet assessed cyber risk management requirements
  - Control capabilities are monitored and reported on at Board level in terms of risk management
  - Controls are regularly updated to reflect changing business risk requirements

Hewlett Packard
Enterprise

Thank you

Jeremy Ward
jeremy.ward@hpe.com