RSA®CONFERENCE2013

EXTREME CYBER SCENARIO PLANNING & FAULT TREE ANALYSIS

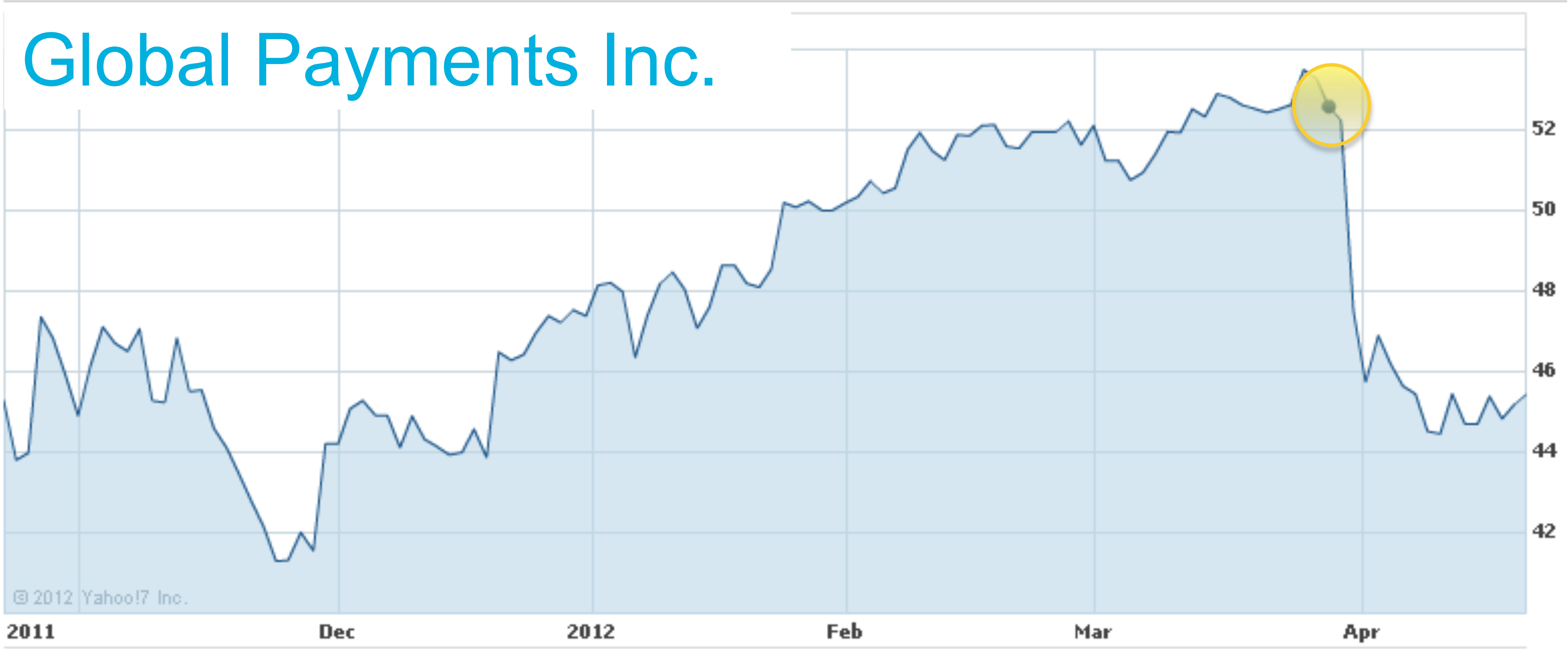
Security in knowledge

Ian Green
Manager, Cybercrime & Intelligence
Commonwealth Bank of Australia

Session ID: STU-W21B

Session Classification: ADVANCED

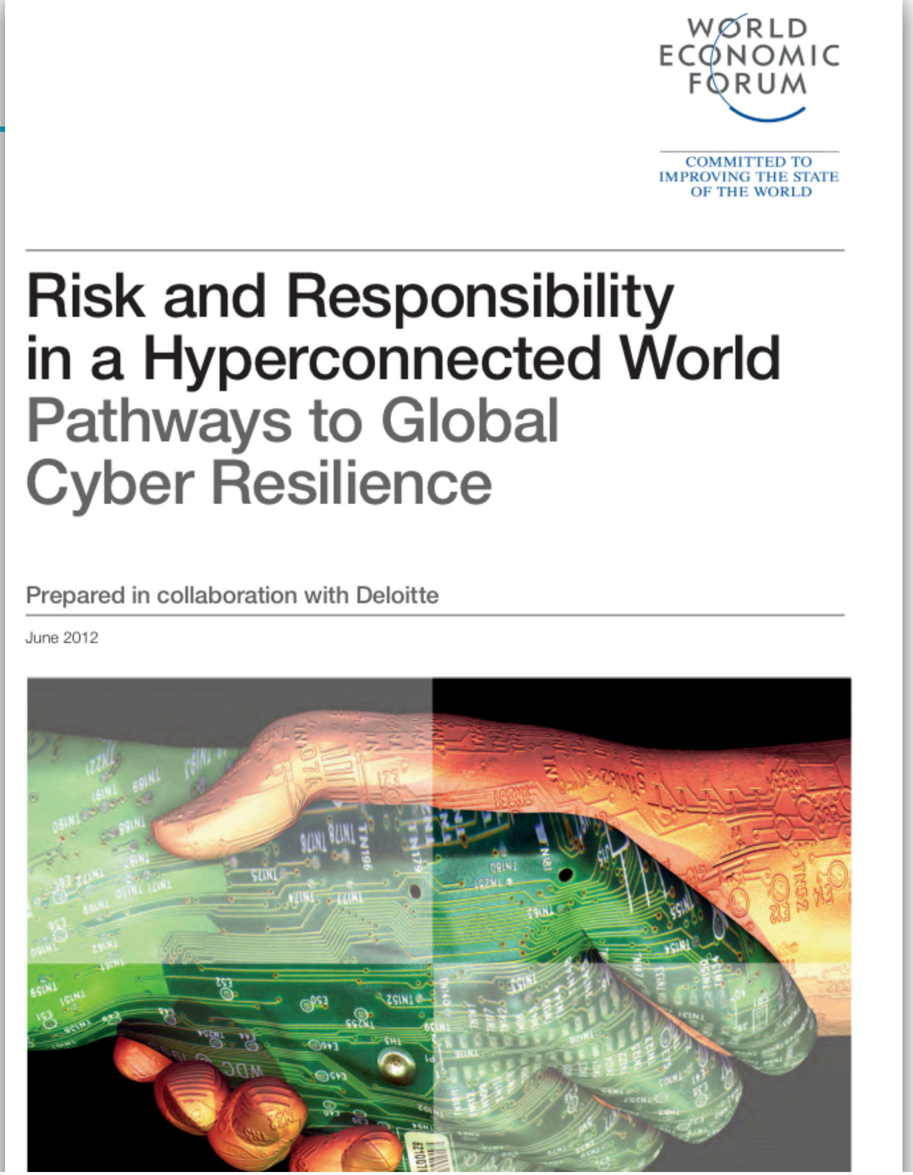
Extreme events are costly



Global Payments Inc.

© 2012 Yahoo!7 Inc.

- 10% or $400m wiped off market cap



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience

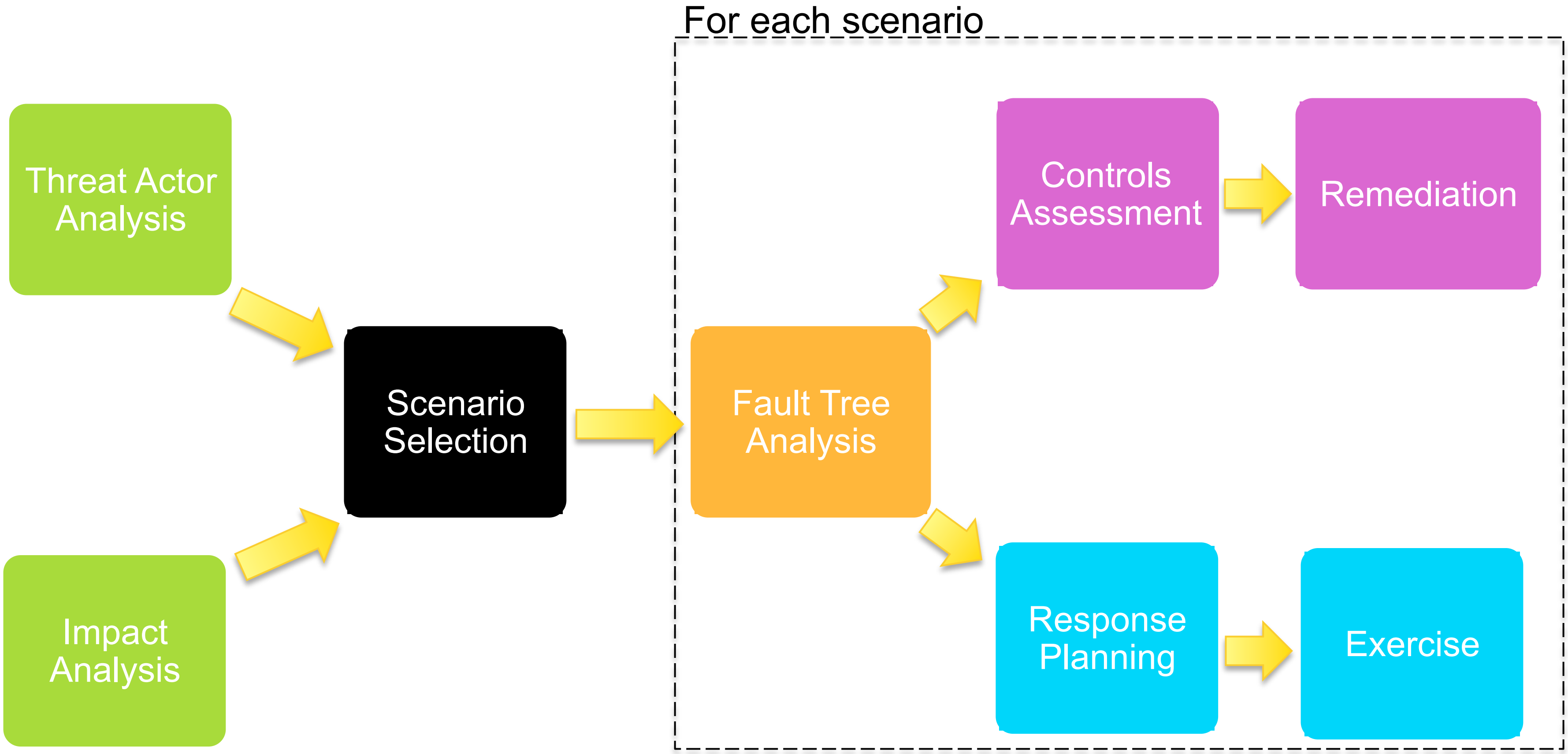
Prepared in collaboration with Deloitte

June 2012

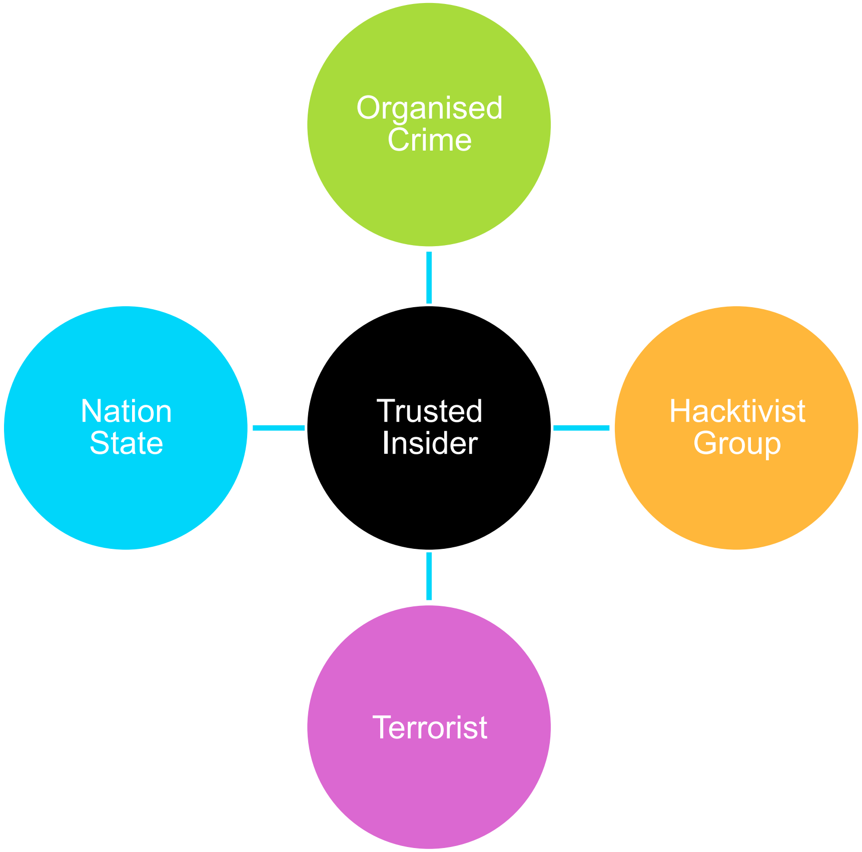
- "While failures are unavoidable, cyber resilience prevents systems from completely collapsing"
- "Can only be achieved by adopting a holistic approach of the management of cyber risk"
- Cyber Resilience
  - mean time to failure
  - mean time to recovery

http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Extreme Cyber Scenario Planning



Threat Actor Analysis



<u>Hacktivist Group</u>

Intent: Hostile
Access: External
Skill Level: Adept
Resources: Organisation
Limits: Extra-legal (major)
Visibility: Overt
Objective: Copy, Injure
Outcome: Damage, Embarrassment

<u>Organised Crime</u>

Intent: Hostile
Access: External
Skill Level: Adept
Resources: Organisation
Limits: Extra-legal (major)
Visibility: Covert
Objective: Take
Outcome: Acquisition / Theft

<u>Nation State</u>

Intent: Hostile
Access: External
Skill Level: Adept
Resources: Government
Limits: Extra-legal (major)
Visibility: Clandestine
Objective: Copy
Outcome: Technical Advantage

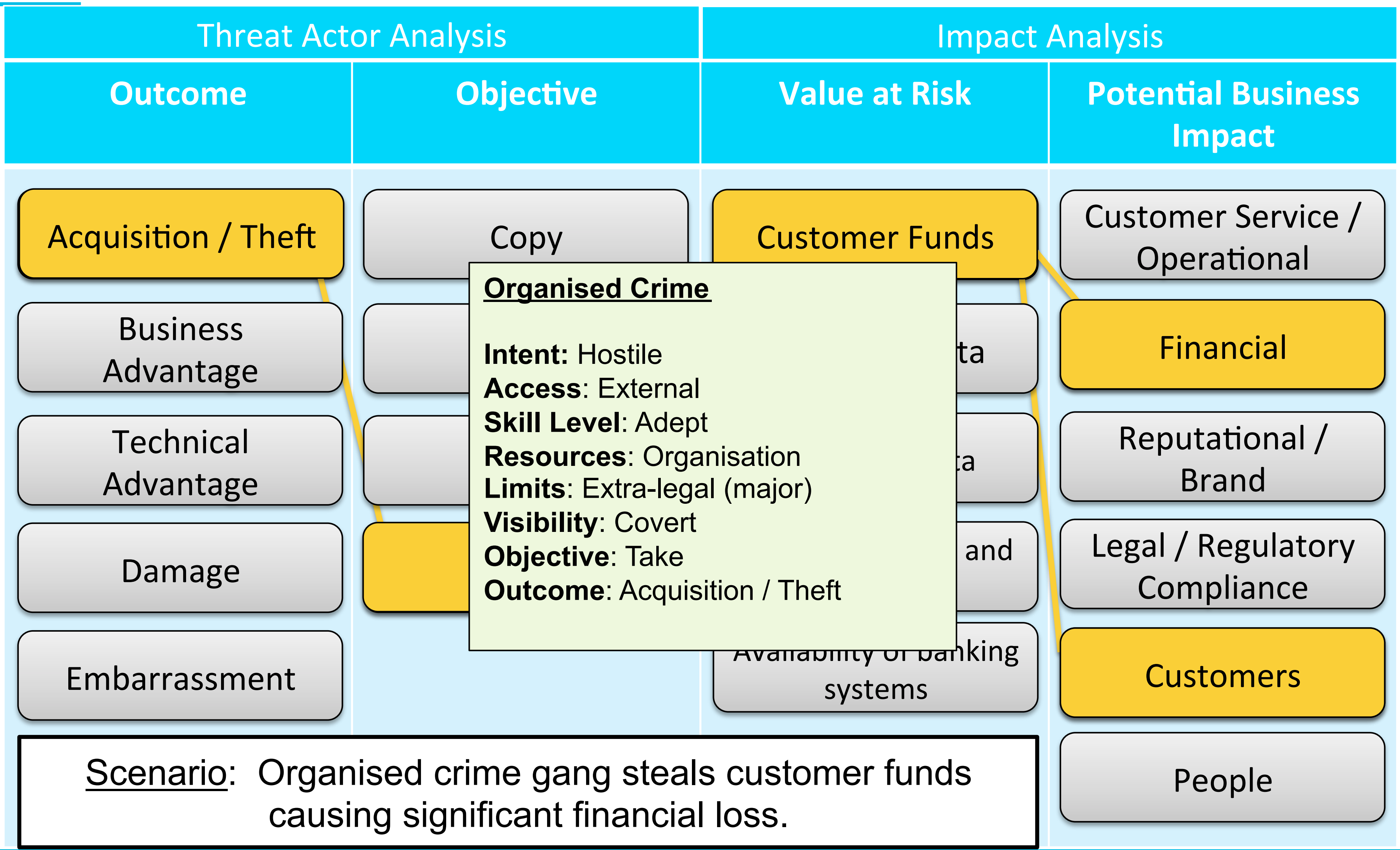
<u>Terrorist</u>

Intent: Hostile
Access: External
Skill Level: Adept
Resources: Organisation
Limits: Extra-legal (major)
Visibility: Covert
Objective: Destroy
Outcome: Damage

Scenario Selection

Threat Actor Analysis		Impact Analysis	
Outcome	**Objective**	**Value at Risk**	**Potential Business Impact**
Acquisition / Theft	Copy	Customer Funds	Customer Service / Operational
Business Advantage	Destroy	Customer Data	Financial
Technical Advantage	Injure	Corporate Data	Reputational / Brand
Damage	Take	Employee health and safety	Legal / Regulatory Compliance
Embarrassment		Availability of banking systems	Customers
			People

Scenario Selection



Threat Actor Analysis

Impact Analysis

Outcome

- Acquisition / Theft
- Business Advantage
- Technical Advantage
- Damage
- Embarrassment

Objective

- Copy

Value at Risk

- Customer Funds
- ta
- ta
- and
- Availability of banking systems

Potential Business Impact

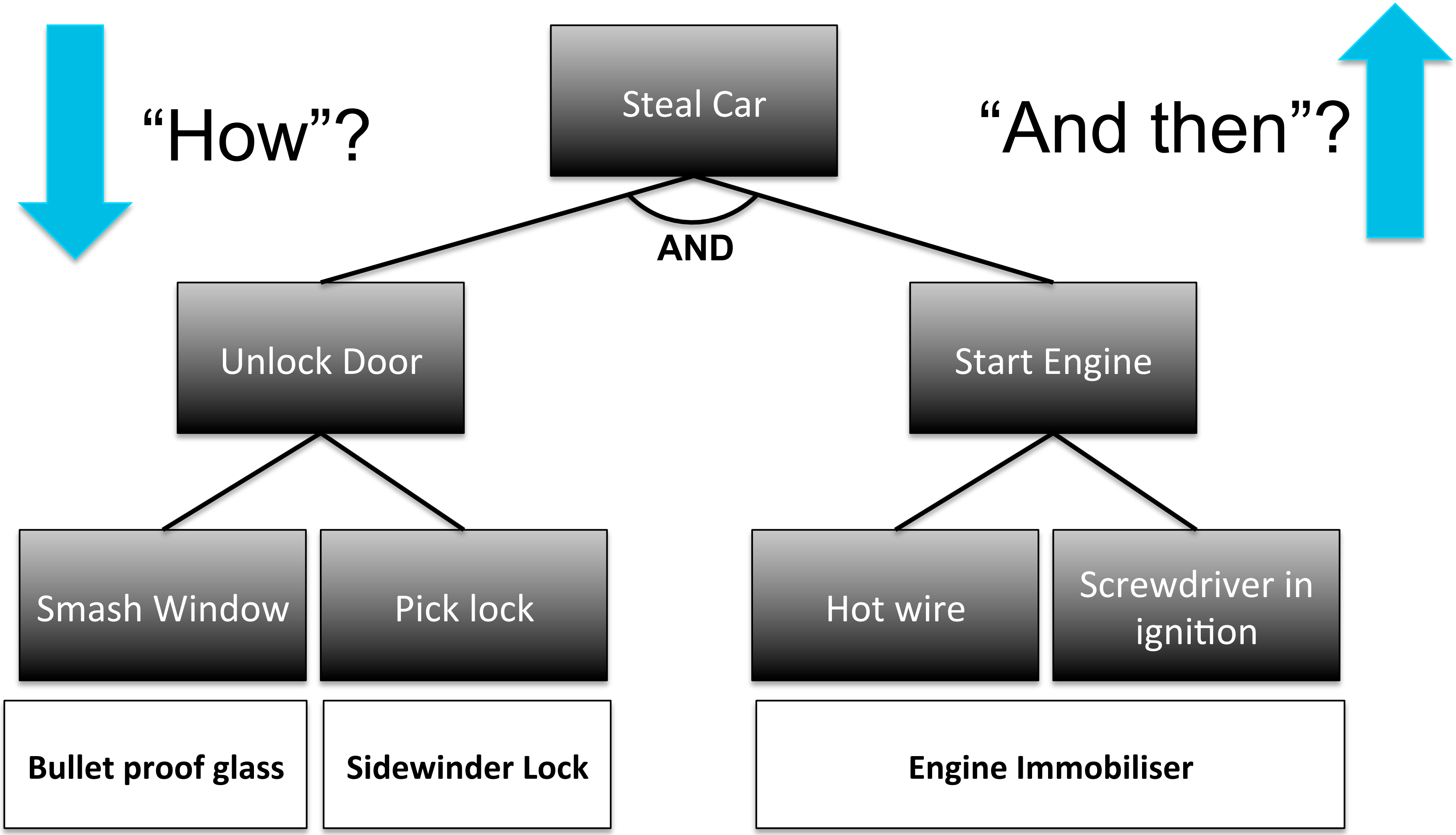
- Customer Service / Operational
- Financial
- Reputational / Brand
- Legal / Regulatory Compliance
- Customers
- People

Organised Crime

Intent: Hostile
Access: External
Skill Level: Adept
Resources: Organisation
Limits: Extra-legal (major)
Visibility: Covert
Objective: Take
Outcome: Acquisition / Theft

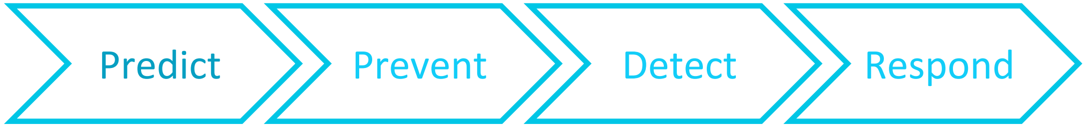
Scenario: Organised crime gang steals customer funds causing significant financial loss.

Fault Tree Analysis



Controls Assessment

- Type of control:



Predict

Prevent

Detect

Respond

- Status of control:

Control has not been implemented	Control has known gaps	Control operating effectively

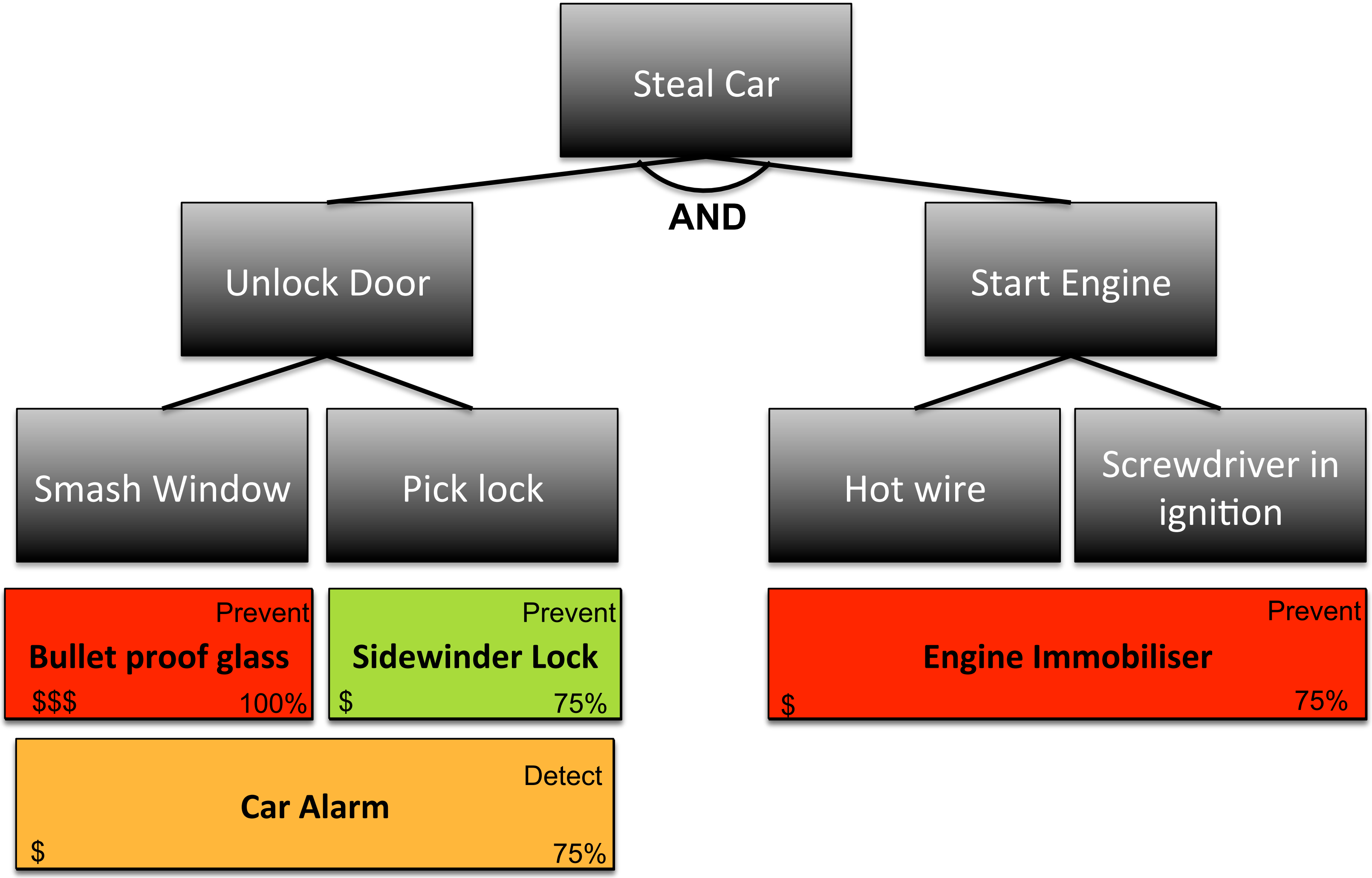
- Potential to mitigate:

25%	50%	75%	100%

- Cost of control:

$ Low cost	**$$** Moderate cost	**$$$** High cost

Control Mapping



Steal Car

AND

Unlock Door

Start Engine

Smash Window

Pick lock

Hot wire

Screwdriver in ignition

Prevent
Bullet proof glass
$$$ 100%

Prevent
Sidewinder Lock
$ 75%

Prevent
Engine Immobiliser
$ 75%

Detect
Car Alarm
$ 75%

EXTREME CYBER SCENARIO PLANNING

CommonwealthBank

7 Extreme Scenarios

1 Large scale malware campaign against bank customers to steal funds.

2 High value fraud conducted against back end payment system

3 Targeted, prolonged DDoS against multiple Internet facing systems.

4 Exfiltrate and disclose large sets of corporate data to embarrass or discredit the bank.

5 Attacker gains access to network and exfiltrates confidential data

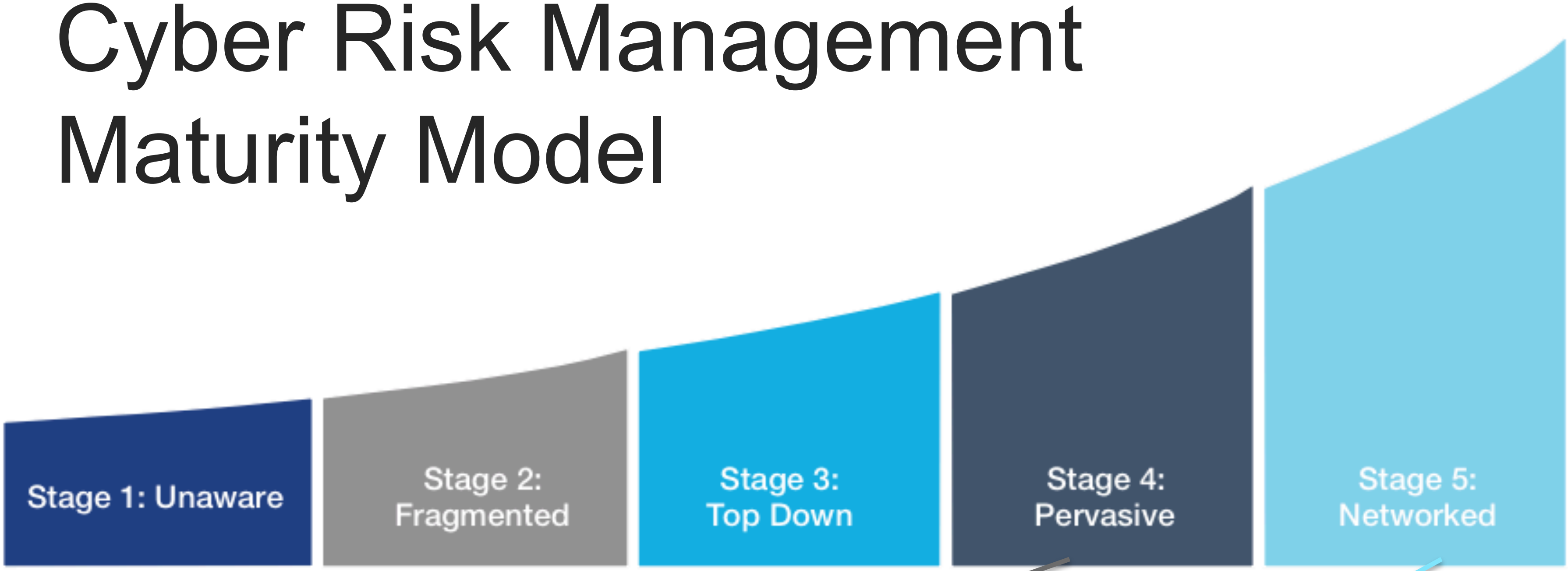
6 Exfiltrate corporate intellectual property for strategic, commercial or political gain.

7 Destructive cyber-attack against multiple bank data centers.

Response Planning

- Will your incident response plans hold up to extreme scenarios?
- What outside resources will you lean on for assistance in an extreme scenario?
- Have you documented and shared all your contacts into government, law enforcement, service providers?
- Have you discussed & planned your response with external stakeholders? Do you know what you will expect from each other if such a scenario occurs?
- Have you practiced your incident response?

Cyber Risk Management Maturity Model

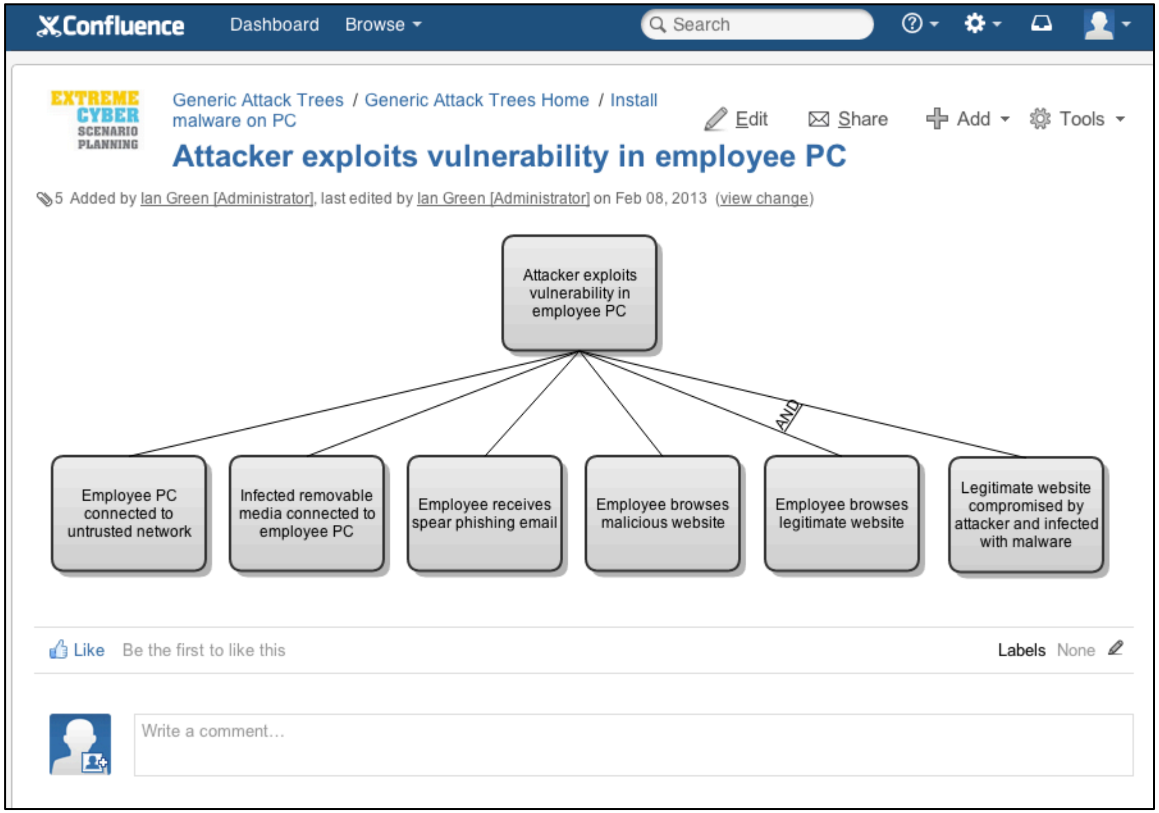


The organisation's leadership takes ownership of cyber risk management… they understand the organisation's vulnerabilities and controls.

The organisation is highly connected to their peers and partners, sharing information and jointly mitigating cyber risk

Source: World Economic Forum
http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

extremecyber.net


Confluence
Dashboard
Browse
Search
Edit
Share
Add
Tools
EXTREME CYBER SCENARIO PLANNING

Generic Attack Trees / Generic Attack Trees Home / Install malware on PC

Attacker exploits vulnerability in employee PC

5 Added by Ian Green [Administrator], last edited by Ian Green [Administrator] on Feb 08, 2013 (view change)

Attacker exploits vulnerability in employee PC
AND
Employee PC connected to untrusted network
Infected removable media connected to employee PC
Employee receives spear phishing email
Employee browses malicious website
Employee browses legitimate website
Legitimate website compromised by attacker and infected with malware
Like
Be the first to like this
Labels None
Write a comment...

- Traffic light protocol
- Methodology
- Control taxonomy
- Threat actor library
- Generic attack trees
- Full scenario analysis

- Join “Extreme Cyber Scenario Planning” on LinkedIn