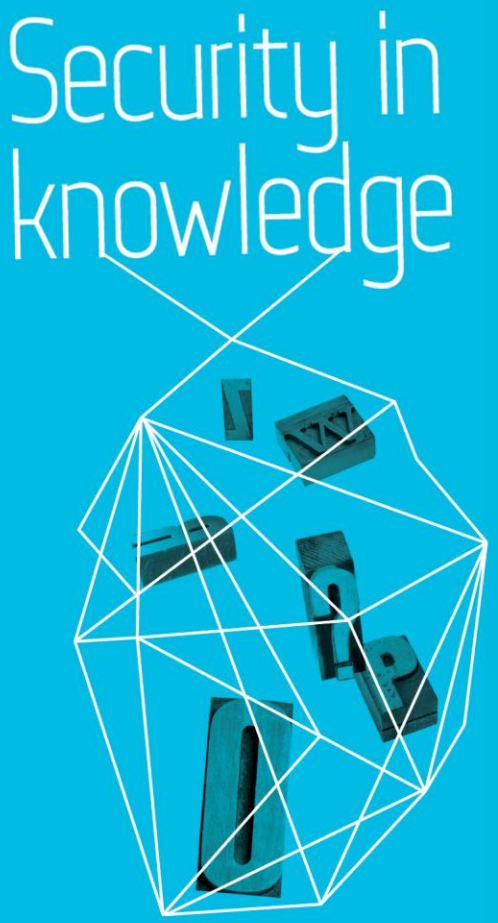
RSA CONFERENCE 2013

EXTREME CYBER SCENARIO PLANNING & FAULT TREE ANALYSIS



Ian Green
Manager, Cybercrime & Intelligence
Commonwealth Bank of Australia

Session ID: GRC-T17

Session Classification: ADVANCED

“What keeps you up at night?”

“What keeps you up at night?”

NEWS

TJX hack the bi

Antony Savvas
Monday 02 April 2007 13:39

The TJX hack

US Sec
debi

GIZMODO

SECURITY

Lockheed Martin’s Security Networks Were Hacked

Lockheed Martin, one of the world's largest defense contractors, was hit hard by hackers this week who used falsified SecurID electronic tokens to gain access. The breach threatens the security of vital data on present and future military technology.

Which, you know, sucks for us and our allies in the UK.

TOP STORIES

MAY 28, 2011 11:00 AM

BY KWAME OPAM

which

X's computer network,
millions of accounts from

Extreme events are costly

- 10% or $400m wiped off market cap

How prepared are you?

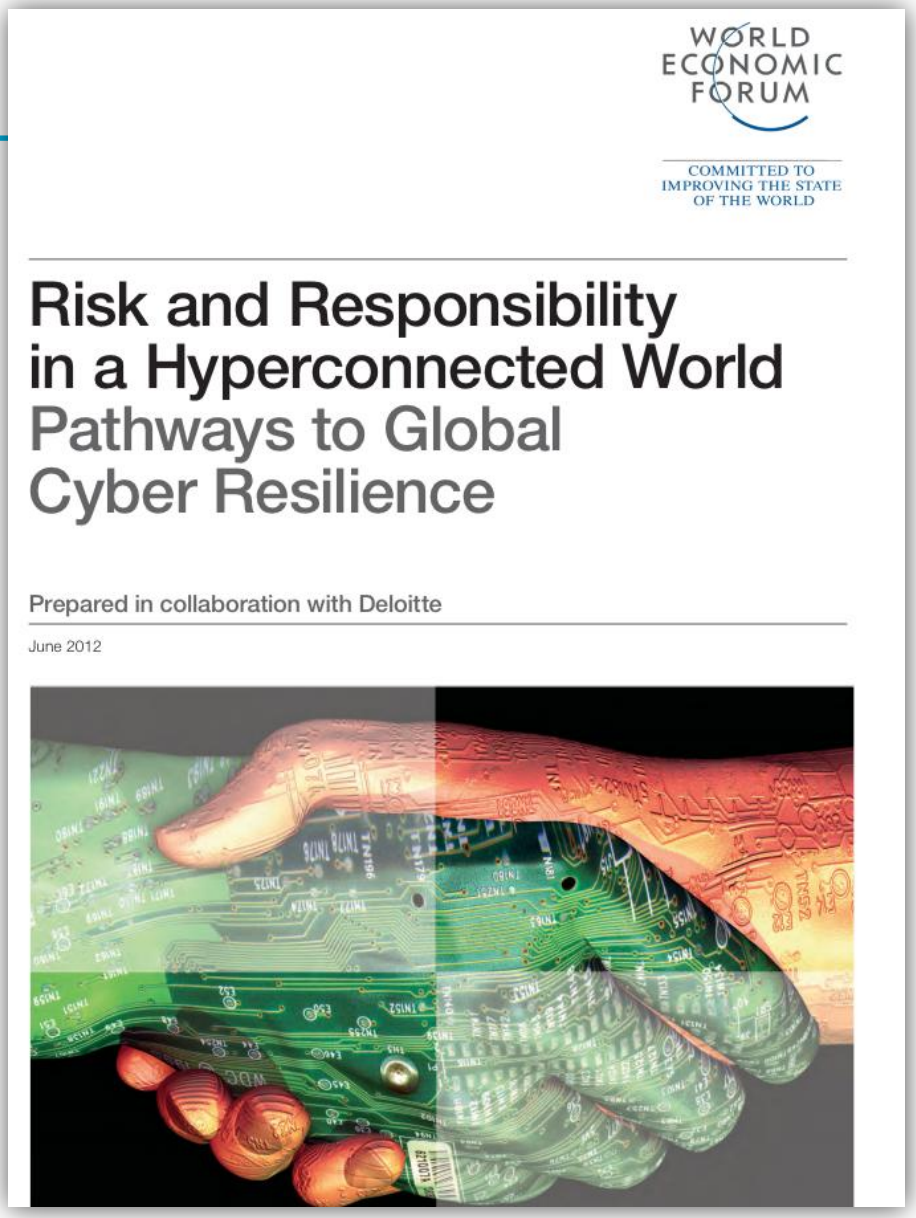
General Keith Alexander
Director, National Security Agency
Commander, United States Cyber Command

Source: The Aspen Security Forum 2012
http://www.youtube.com/watch?v=rtvi_RiFzOc&feature=plcp

How prepared are you?

General Keith Alexander
Director, National Security Agency
Commander, United States Cyber Command

Source: The Aspen Security Forum 2012
http://www.youtube.com/watch?v=rtvi_RiFzOc&feature=plcp

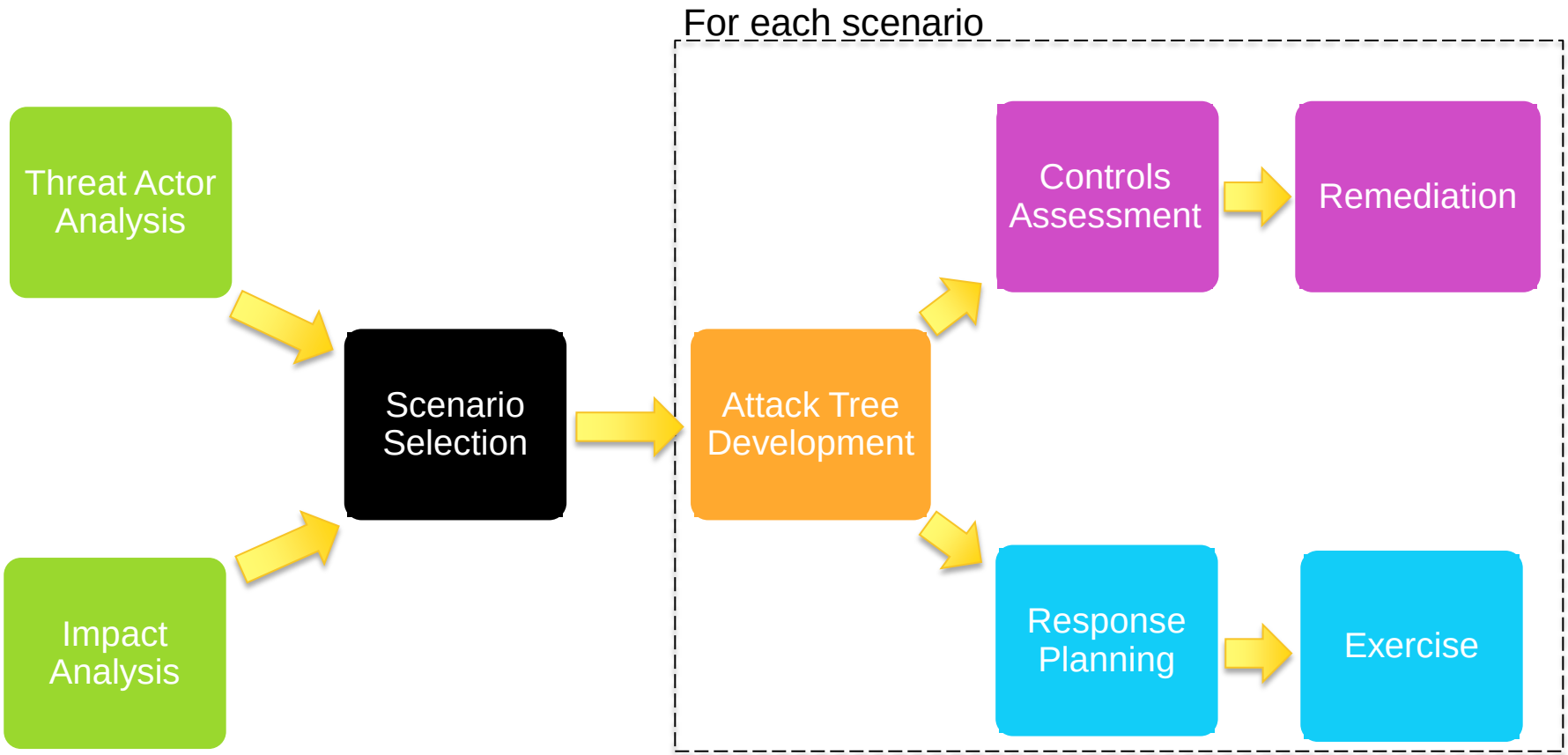


- "While failures are unavoidable, cyber resilience prevents systems from completely collapsing"
- Cyber Resilience
  - mean time to failure
  - mean time to recovery
- "Can only be achieved by adopting a holistic approach of the management of cyber risk"

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

HOW?

Threat Actor Analysis



Aim: Identify actors who pose a significant threat to the organisation

Threat Agent Library – Intel

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal	■	■	■						■		■	■							■		■
	External				■	■	■	■	■		■			■	■	■	■	■	■		■	
Outcome (1-2)	Acquisition/Theft												■			■				■		
	Business Advantage						■	■	■			■			■							■
	Damage	■	■	■	■					■	■			■			■	■	■		■	
	Embarrassment	■	■	■		■				■	■			■	■		■	■				
	Tech Advantage						■	■	■			■	■									■
Limits (max)	Code of Conduct		■	■																		
	Legal	■													■							■
	Extra-legal, minor					■	■	■	■				■				■	■		■	■	
	Extra-legal, major				■					■	■	■		■		■			■			
Resources (max)	Individual	■	■	■						■				■						■		
	Club				■													■				
	Contest																				■	
	Team								■													■
	Organization					■	■						■		■	■	■		■			
	Government							■			■	■										
Skills (max)	None				■									■						■		
	Minimal		■															■				
	Operational			■						■											■	■
	Adept	■				■	■	■	■		■	■	■		■	■	■		■			
Objective (1 or more)	Copy					■	■		■			■	■		■							■
	Deny							■			■											
	Destroy				■					■	■								■			
	Damage									■	■								■			
	Take														■	■			■	■		
	All of the Above/ Don't Care	■	■	■										■			■	■			■	
Visibility (min)	Overt		■		■			■							■		■	■				
	Covert	■				■										■			■		■	
	Clandestine			■			■		■			■	■							■		■
	Multiple/Don't Care																					

Source: Intel IT Threat Assessment Group, 2007

http://www.intel.com/it/pdf/threat-agent-library.pdf

Agent Attributes - Intel

WHO

- **Intent:** Non-hostile, Hostile
- **Access**: Internal, External
- **Skill Level**: None, Minimal, Operational, Adept
- **Resources**: Individual, Club, Contest, Team, Organisation, Government
- **Limits**: Code of conduct, Legal, Extra-legal (minor), Extra-legal (major)

HOW

- **Visibility**: Overt, Covert, Clandestine, Don't Care
- **Objective**: Copy, Destroy, Injure, Take, Don't Care
- **Outcome**: Acquisition / Theft, Business Advantage, Damage, Embarrassment, Technical Advantage

Agent Attributes - Intel

WHO

- **Intent:** Non-hostile, **Hostile**
- **Access**: Internal, External
- **Skill Level**: None, Minimal, Operational, **Adept**
- **Resources**: Individual, Club, Contest, Team, **Organisation, Government**
- **Limits**: Code of conduct, Legal, **Extra-legal (minor), Extra-legal (major)**

HOW

- **Visibility**: Overt, Covert, Clandestine, Don't Care
- **Objective**: Copy, Destroy, Injure, Take, Don't Care
- **Outcome**: Acquisition / Theft, Business Advantage, Damage, Embarrassment, Technical Advantage

Consolidated Threat Actors

- Corrupt Government Official
- Government Cyber Warrior
- Government Spy
- Civil Activist
- Radical Activist
- Mobster
- Terrorist
- ~~Competitor~~
- Internal Spy

Nation State

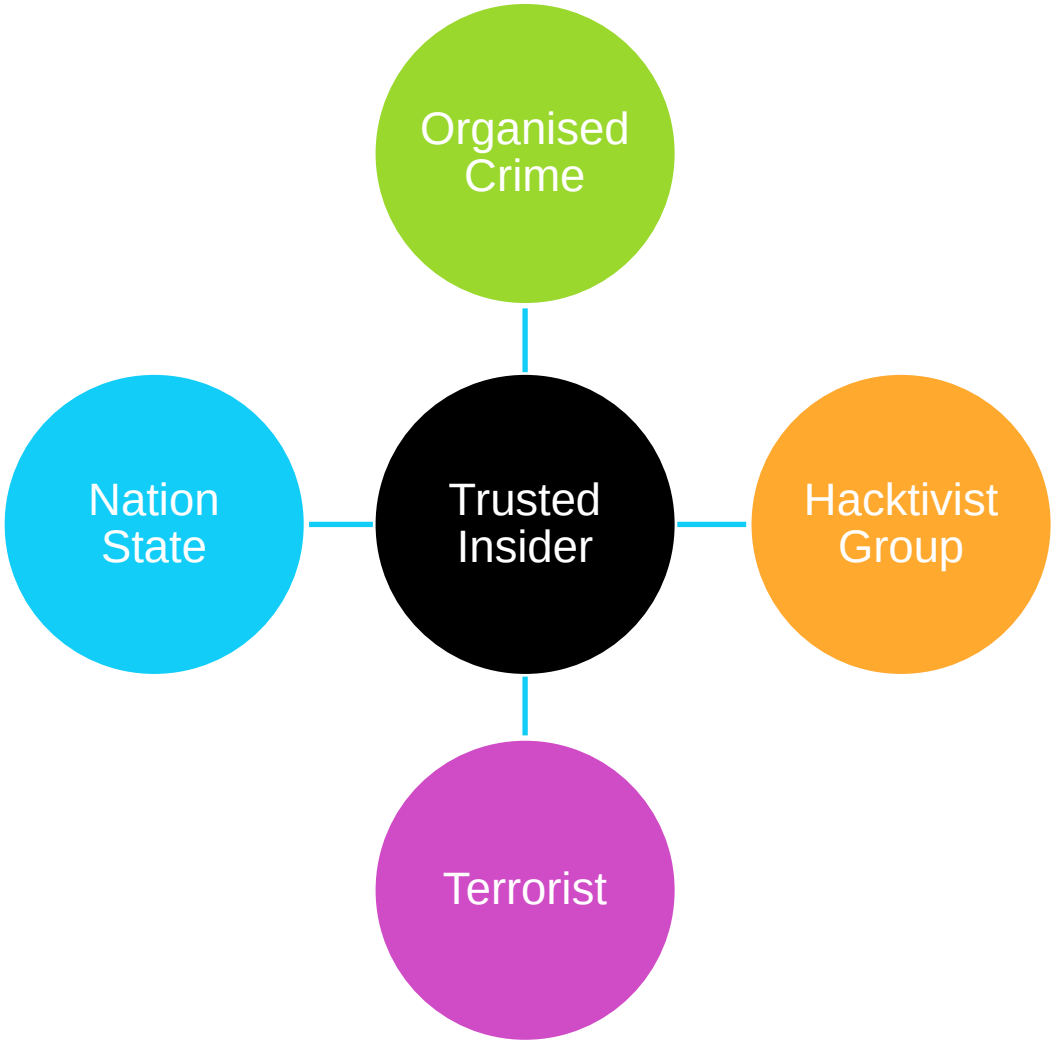
Hacktivist

Organised Crime

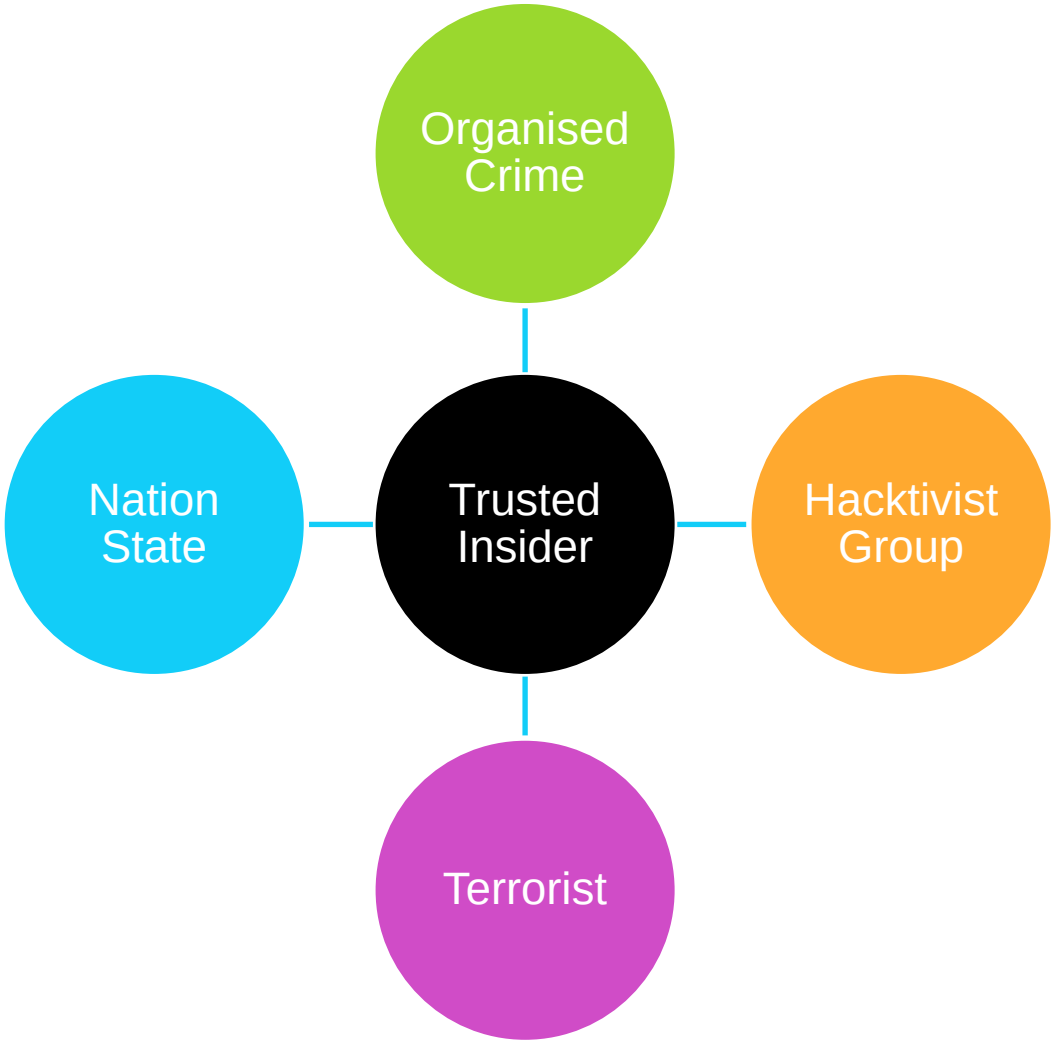
Terrorists

Trusted Insider

Threat Actor Analysis



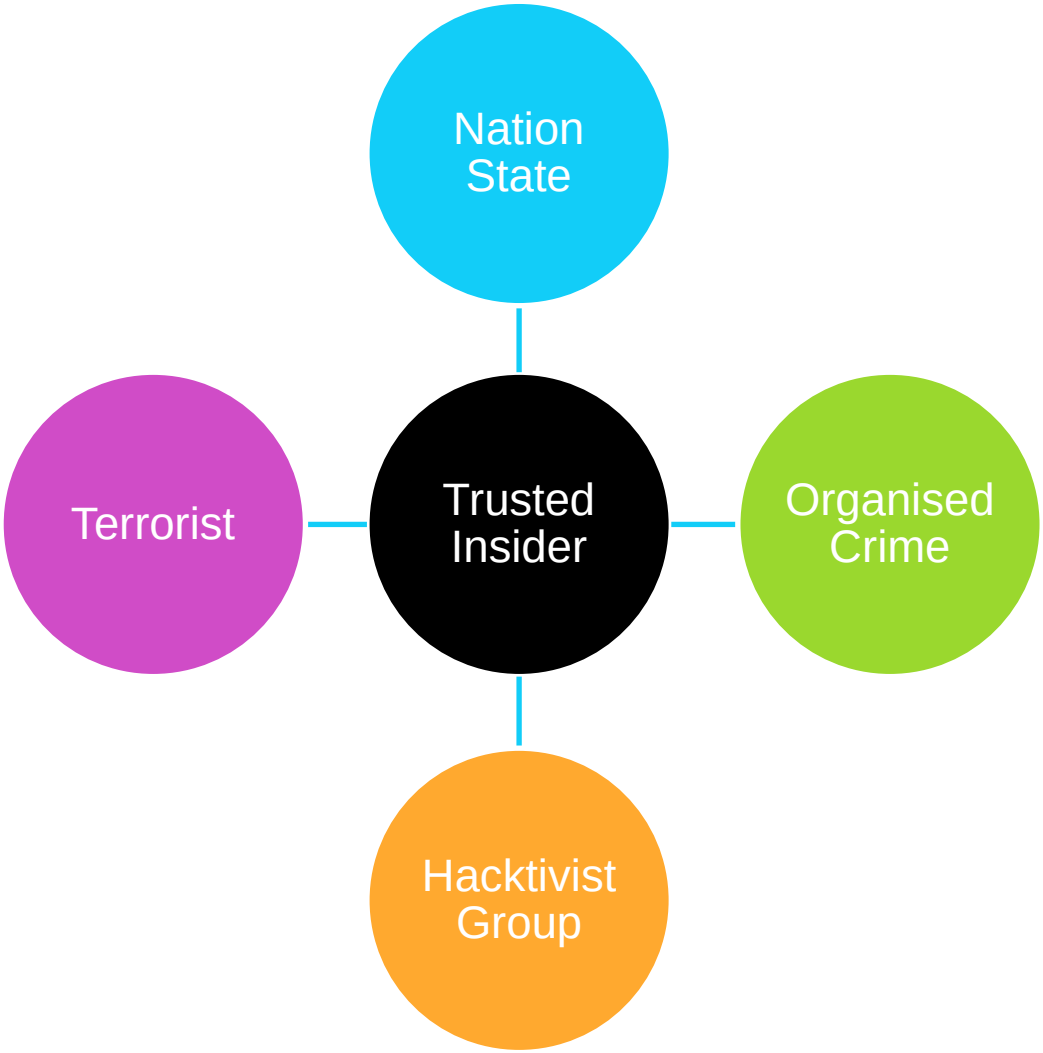
Threat Actor Analysis



Hacktivist Group

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

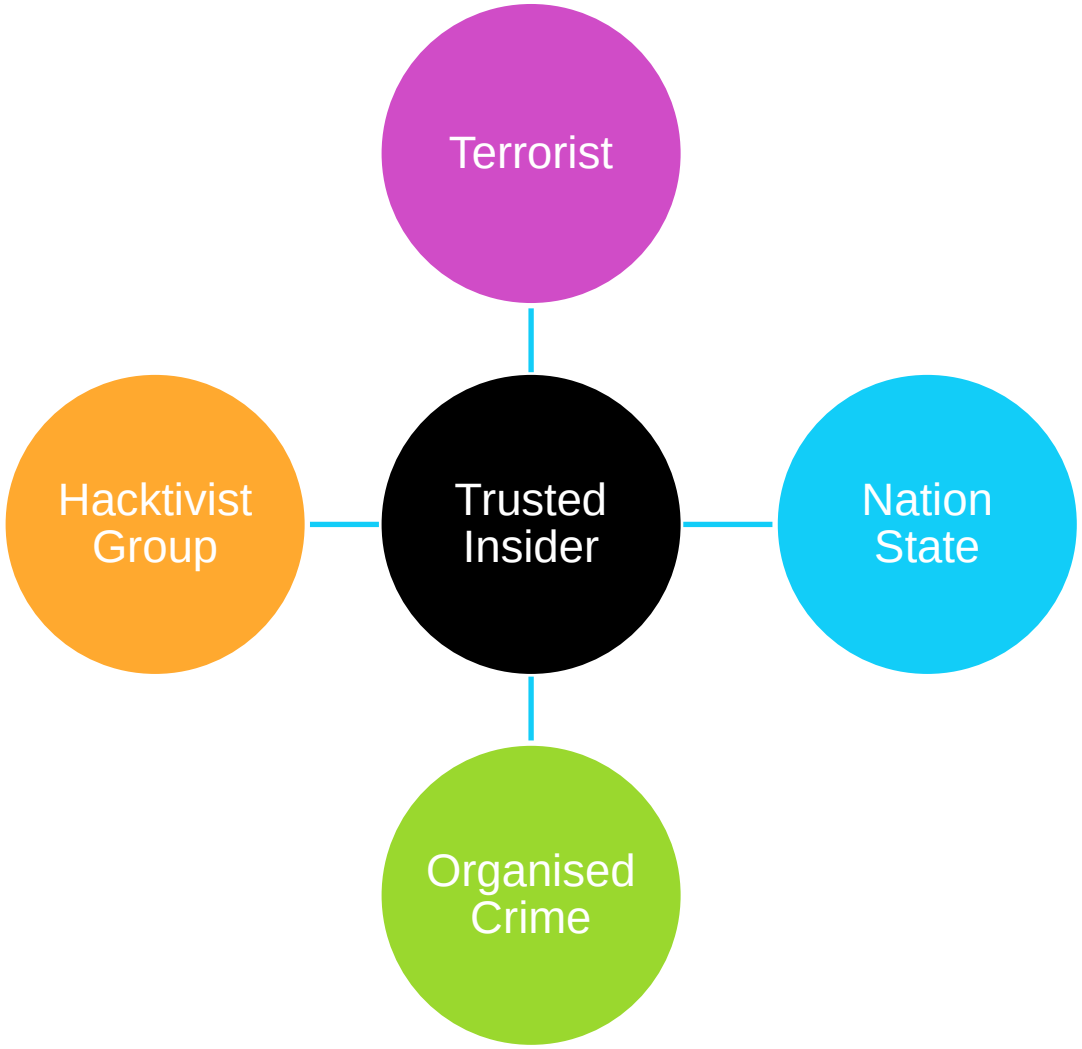
Threat Actor Analysis



Organised Crime

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

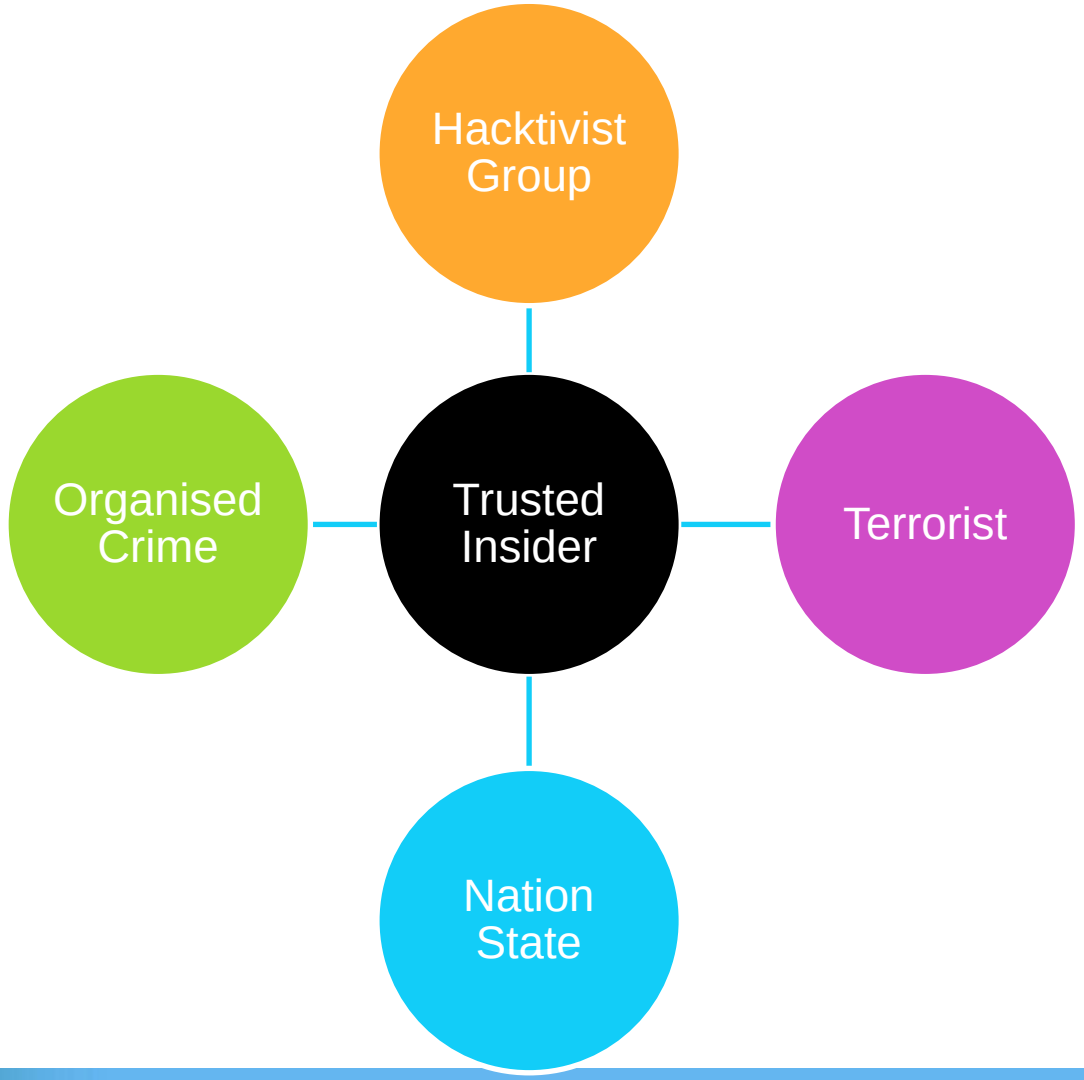
Threat Actor Analysis



Nation State

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

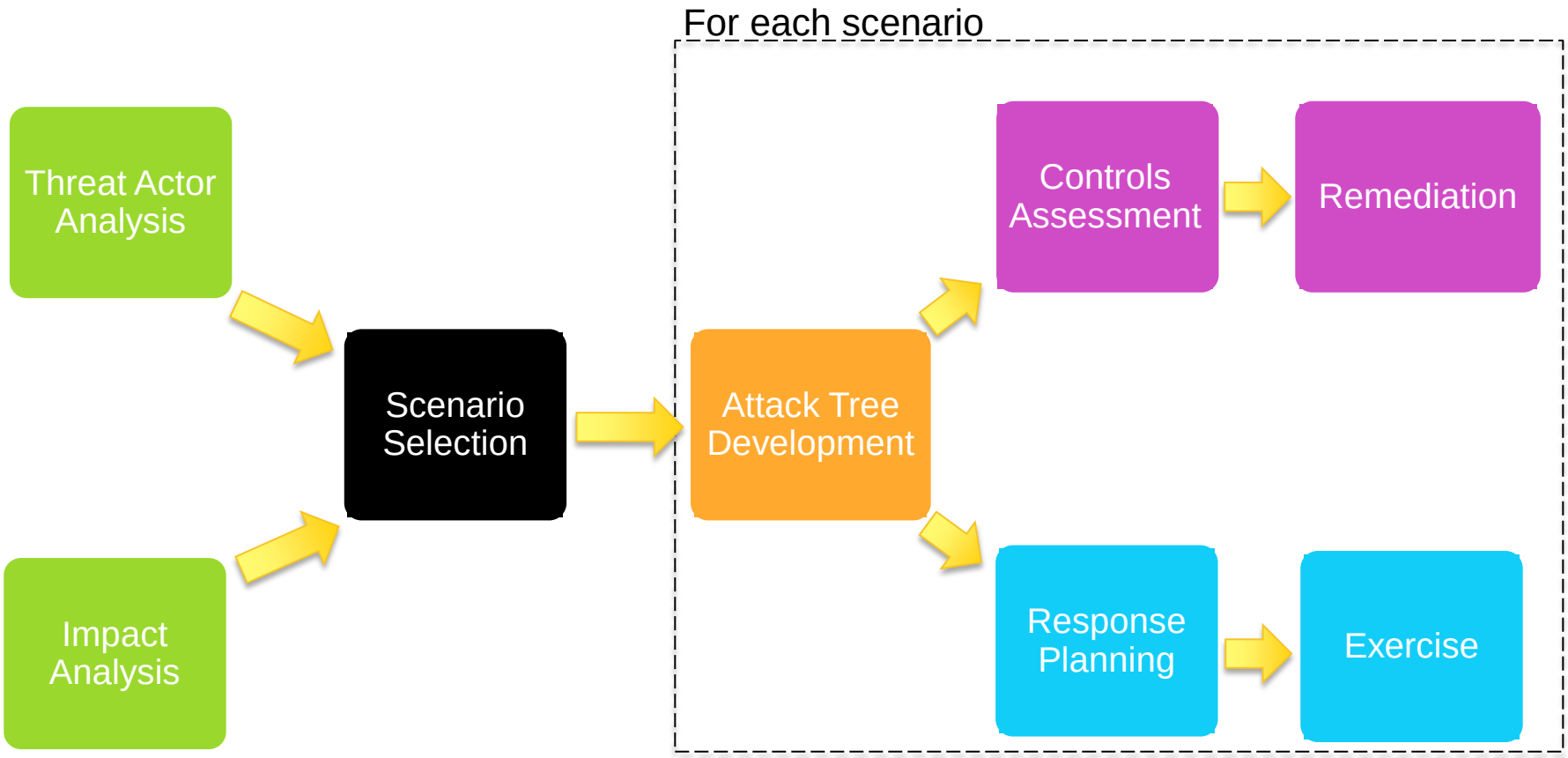
Threat Actor Analysis



Terrorist

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

Impact Analysis



Aim: Determine what your organisation really cares about protecting

Business Impact Matrix

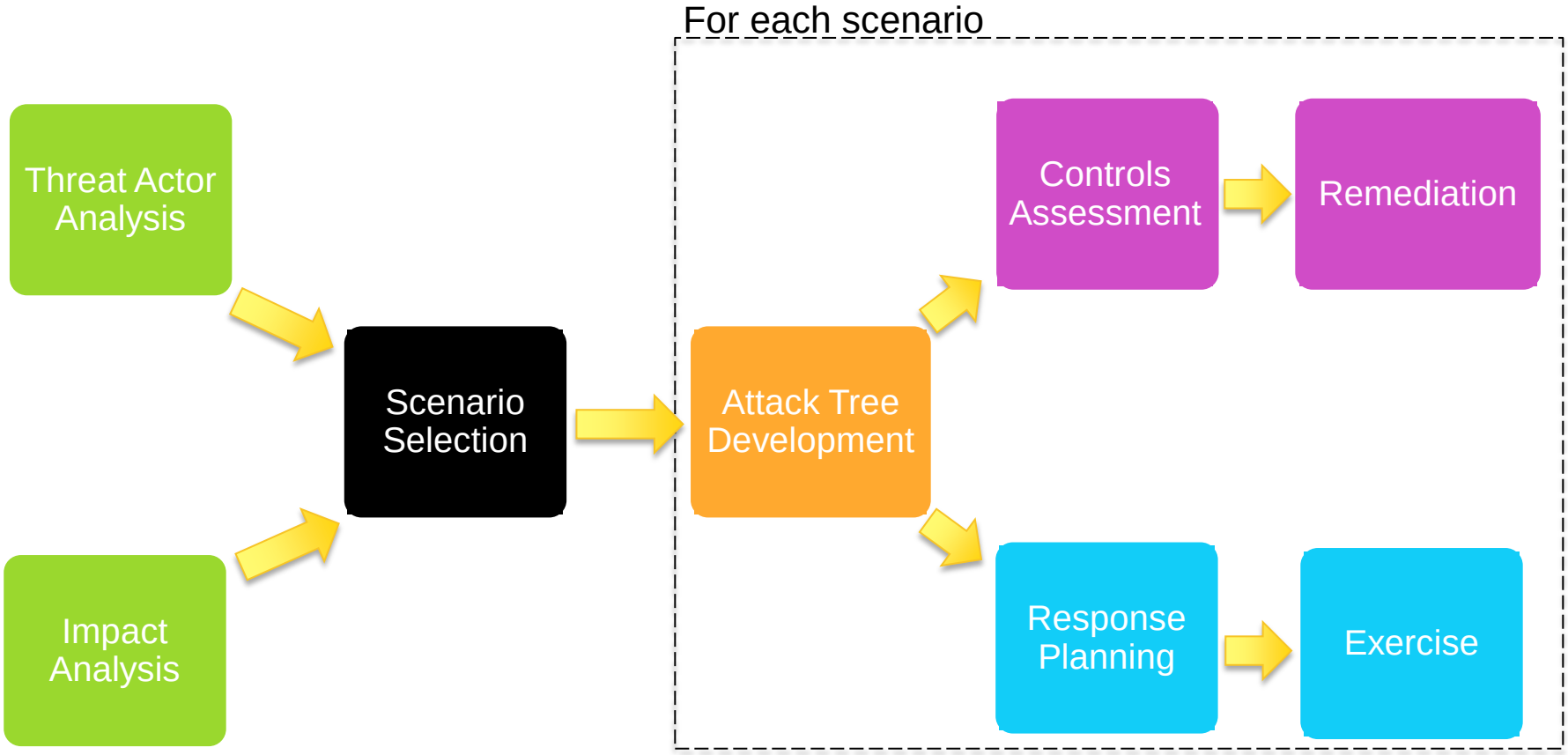
Impact

	Financial	Customer Service & Operations	Reputation / Brand	Legal / Regulatory Compliance	People	Customers
5	>$500m	Significant loss of customers due to extensive interruption to service capability	Substantial damage to brands resulting from extensive negative national publicity	Loss of license, loss of public listing or substantial penalties on Directors	Death or severe injury to employees	Serious financial impact to all customers
4	$200m-$500m	….	….	….	….	….
3	$50m-$200m	…	…	…	…	…
2	<$50m	…	….	…	…	…
1	<$50m	…	…	…	…	…

Values at Risk

- Health and safety of employees
- Customer funds and stocks
- Customer data (private information)
- Customer data (intellectual property)
- Corporate data (sensitive information)
- Corporate data (intellectual property)
- Availability of banking channels (Internet facing)
- Availability of banking channels (back end)

Scenario Selection



Aim: Select scenarios that could have a catastrophic impact on the organisation

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	**Objective**	**Value at Risk**	**Potential Business Impact**
Acquisition / Theft	Copy	Customer Funds	Customer Service / Operational
Business Advantage		ta	Financial
Technical Advantage		a	Reputational / Brand
Damage		and	Legal / Regulatory Compliance
Embarrassment		Availability of banking systems	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.

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		Data	Financial
Technical Advantage		Data	Reputational / Brand
Damage		alth and	Legal / Regulatory Compliance
Embarrassment		Availability of banking systems	Customers
			People

Hacktivist Group

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

Scenario: Socio-political group performs prolonged denial-of-service attack causing sustained outages.

Is it "Extreme"?

Impact

	Financial	Customer Service & Operations	Reputation / Brand	Legal / Regulatory Compliance	People	Customers
5	>$500m	Significant loss of customers due to extensive interruption to service capability	Substantial damage to brands resulting from extensive negative national publicity	Loss of license, loss of public listing or substantial penalties on Directors	Death or severe injury to employees	Serious financial impact to all customers
4	$200m-$500m	…	…	…	…	…
3	$50m-$200m	…	…	…	…	…
2	<$50m	…	….	…	…	…
1	<$50m	…	…	…	…	…

Scenarios on Risk Matrix

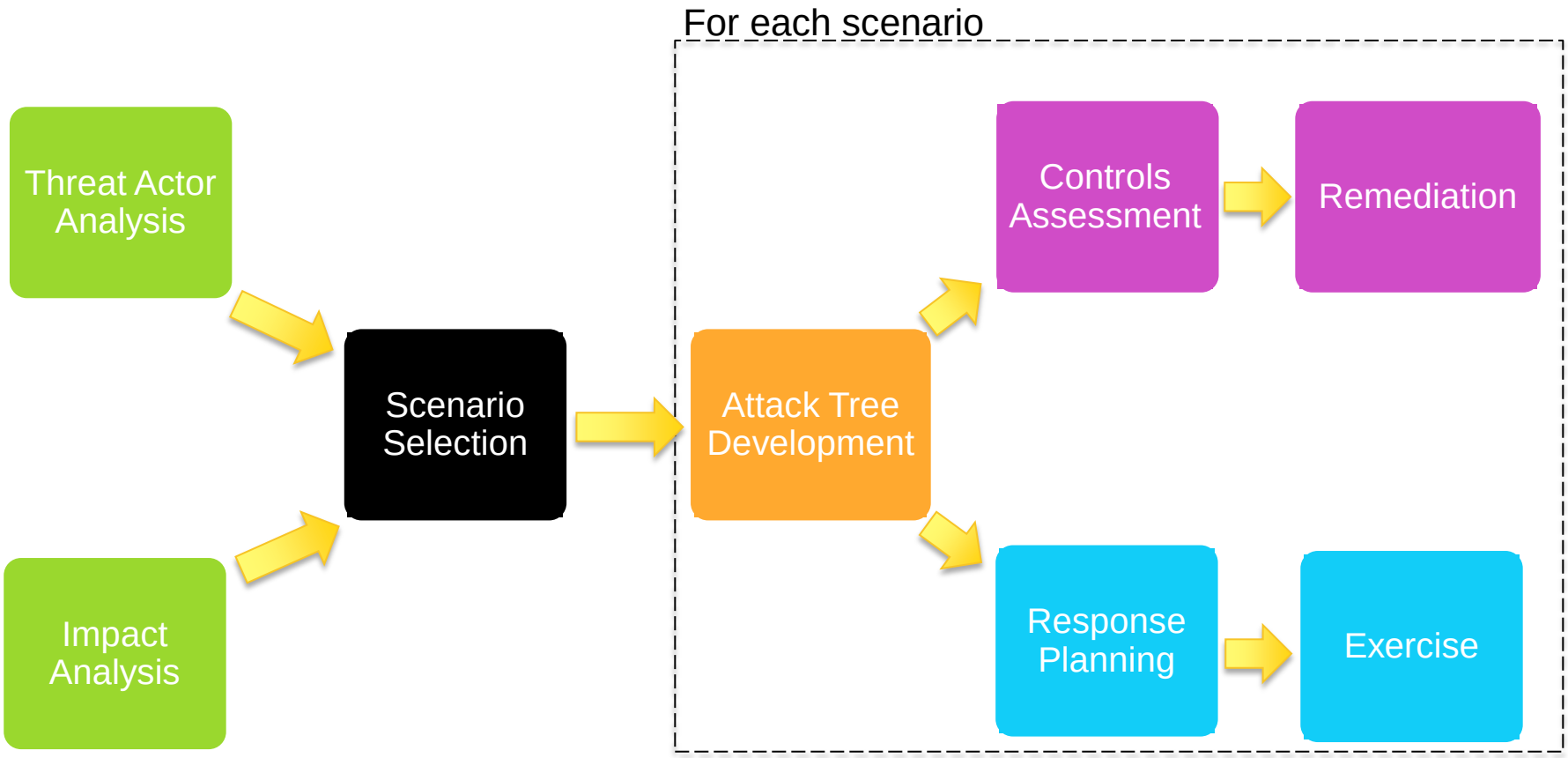
Likelihood						
	5	L	M	M	H	VH
	4	L	L	M	H	VH
	3	I	L	M	H	VH
	2	I	L	M	H	VH
	1	I	I	L	M	H
		1	**2**	**3**	**4**	**5**
		Impact				

4 3 5 1 6 2 7

Scenario Selection

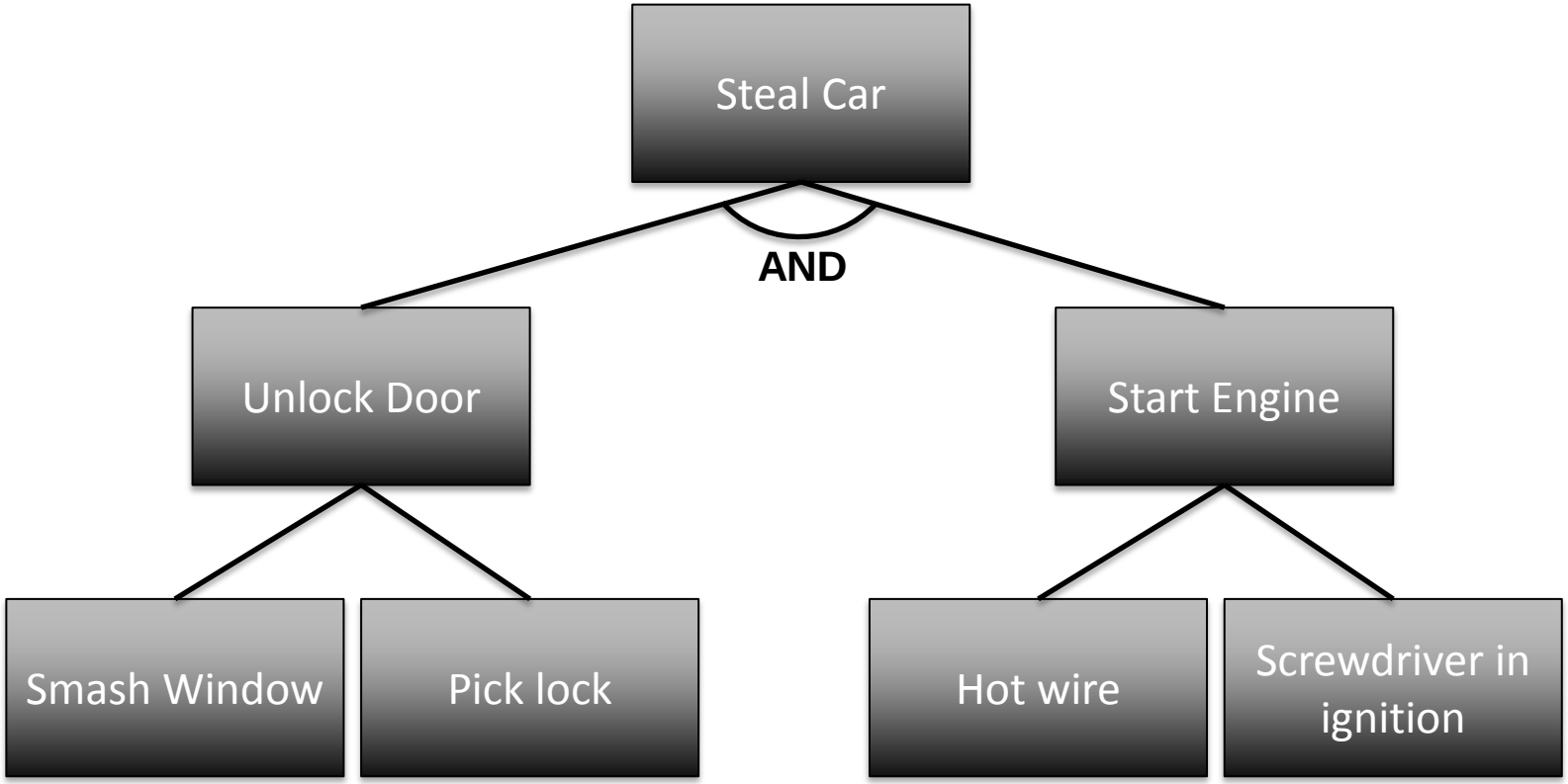
	Organised Crime	Hacktivist Group	Nation State	Terrorist
Financial Gain	1 Large scale targeting of bank customers using malware to steal funds.			
	2 High value fraud conducted against backend payment system.			
Theft / Exposure		4 Exfiltrate and disclose large sets of corporate data to embarrass or discredit the bank.	6 Exfiltrate corporate intellectual property for strategic, commercial or political gain.	
	5 Compromise bank IT systems and exfiltrate large sets of customer data.			
Sabotage / Operations Impact		3 Targeted, prolonged DDoS against multiple Internet facing systems.		7 Destructive cyber-attack against multiple bank data centres.

Attack Tree Development

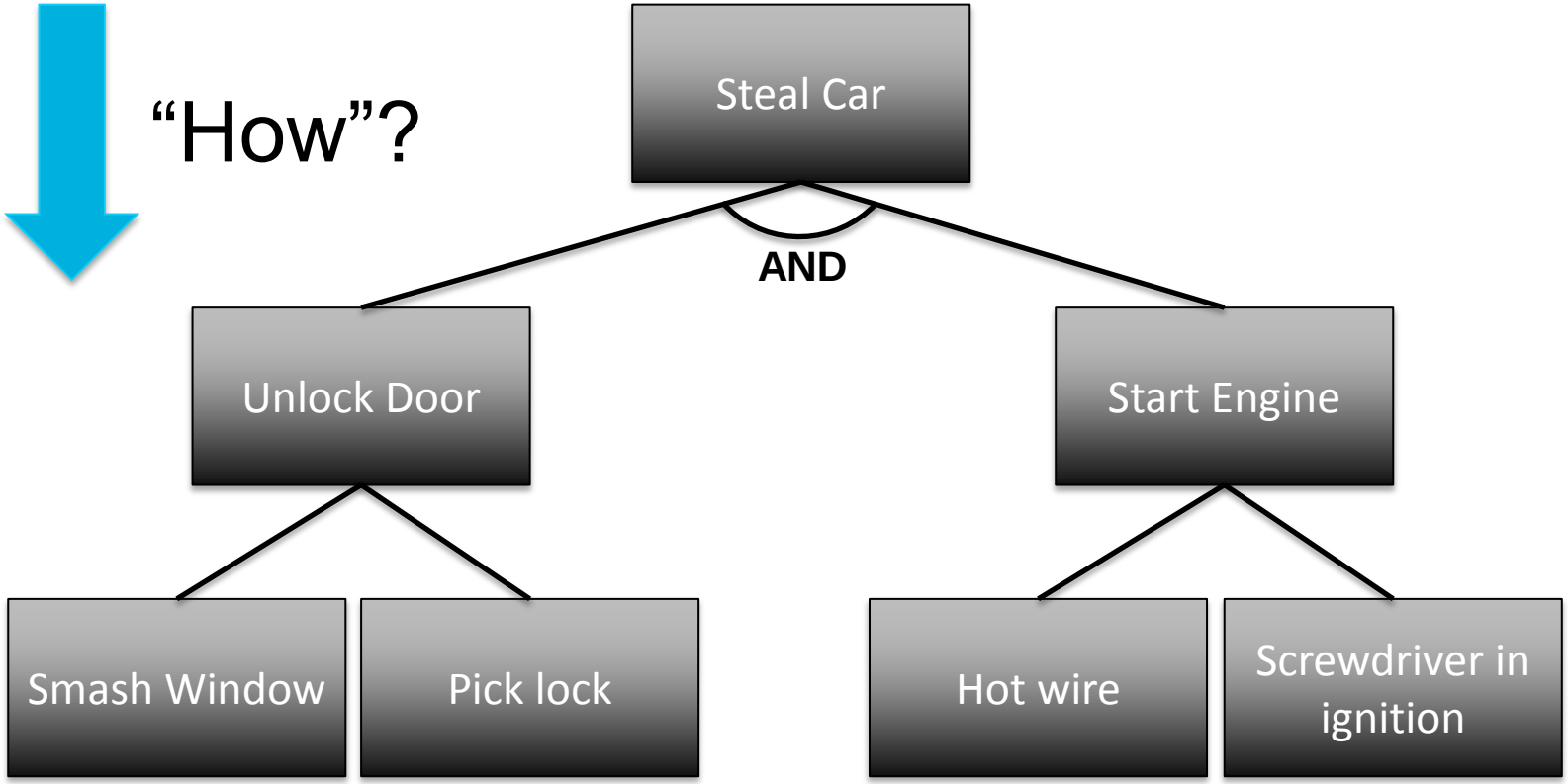


Aim: Develop detailed attack trees for each extreme scenario

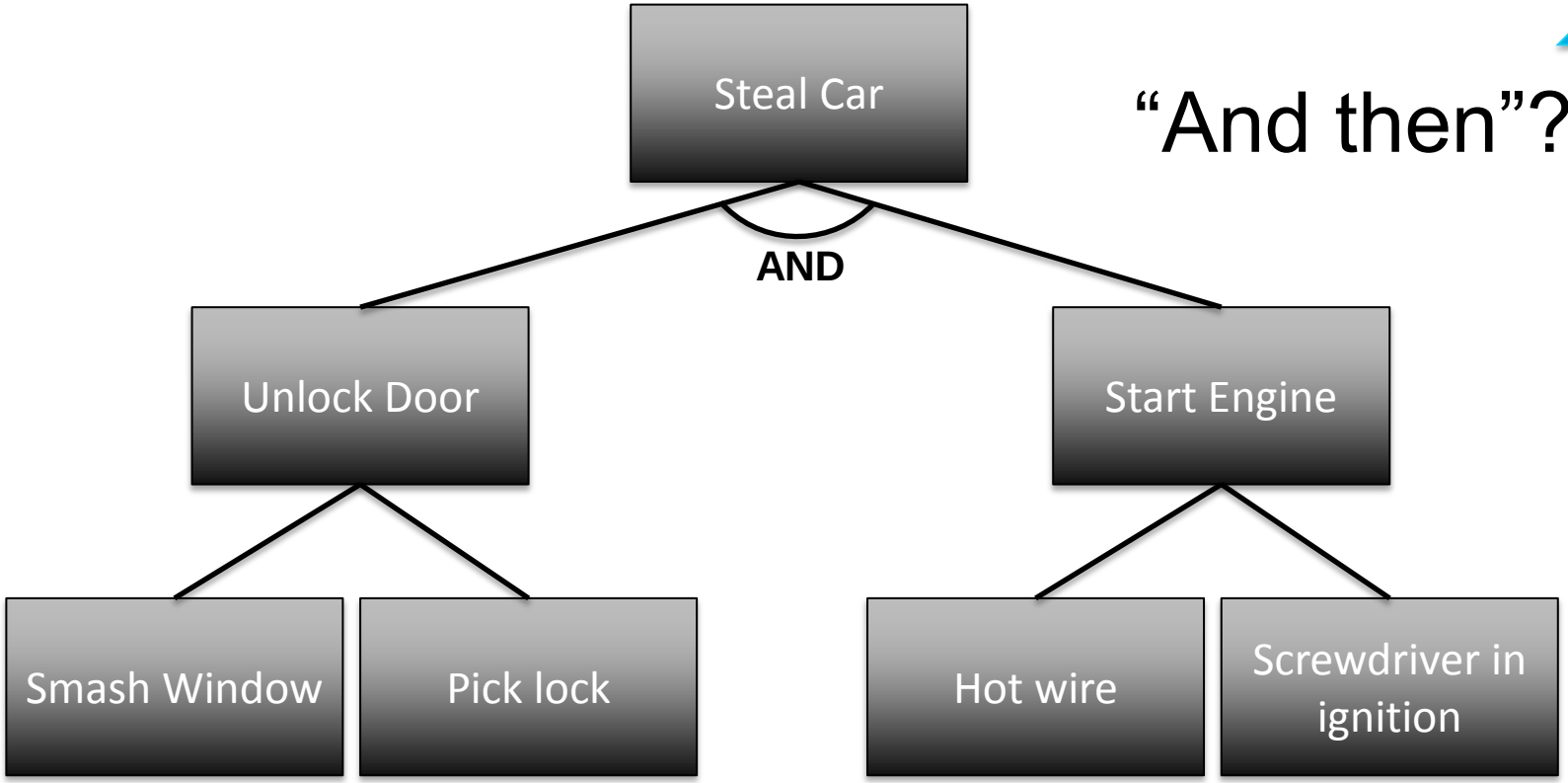
Attack Tree Analysis



Attack Tree Analysis



Attack Tree Analysis



"And then"?

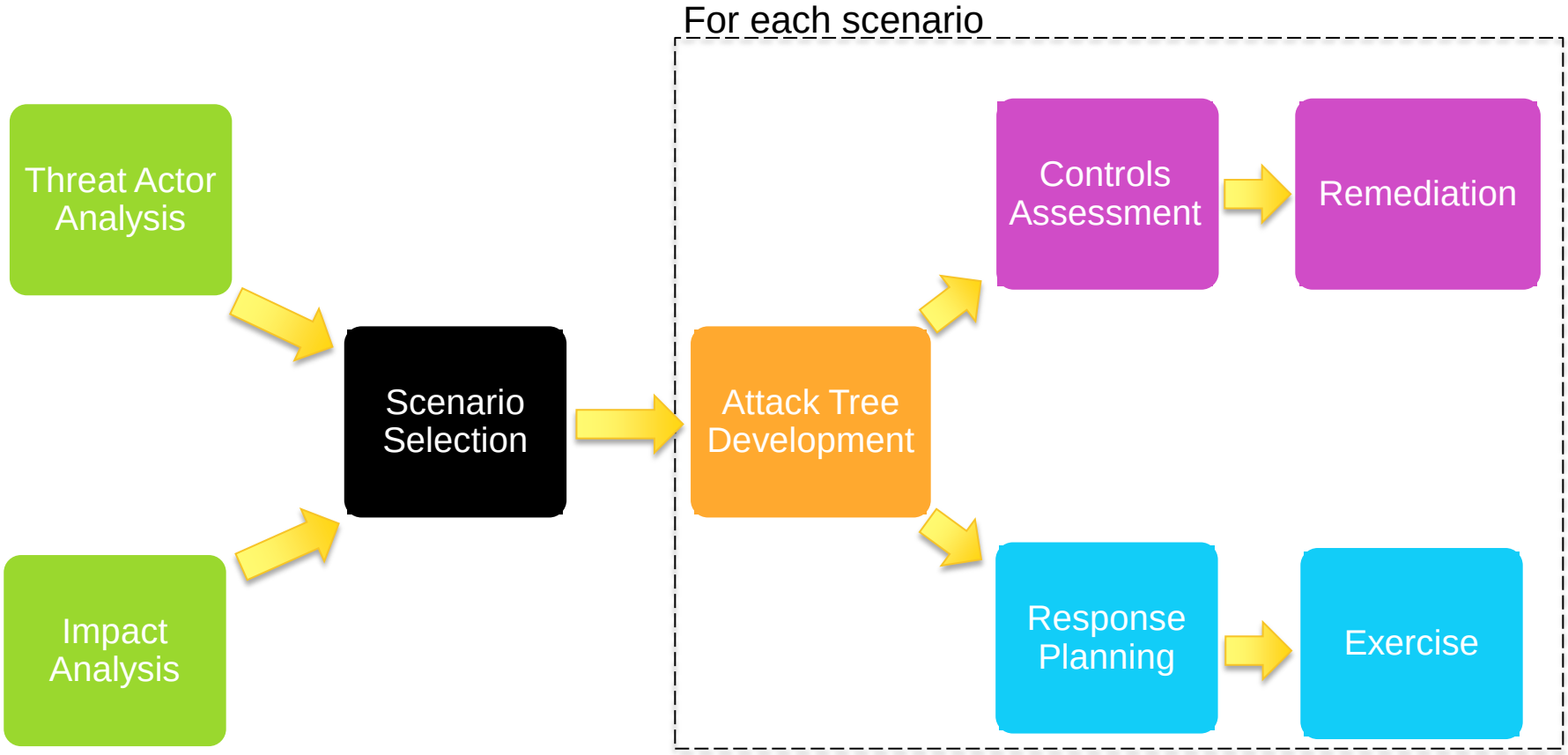
EXTREME CYBER SCENARIO PLANNING

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.

Controls Assessment



Aim: Map controls to attack trees and assess effectiveness

Industry Standard Control Sets

- Provides a consistent set of controls for assessment and comparison

- May not be relevant to a particular scenario
- May not be pitched at the right level to be useful

- Options available:
  - DSD Top 35 Mitigation Strategies
    - http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
  - NIST Special Publication 800-53
    - http://web.nvd.nist.gov/view/800-53/home
  - SANS 20 Critical Controls for Effective Cyber Defense
    - http://www.sans.org/critical-security-controls/

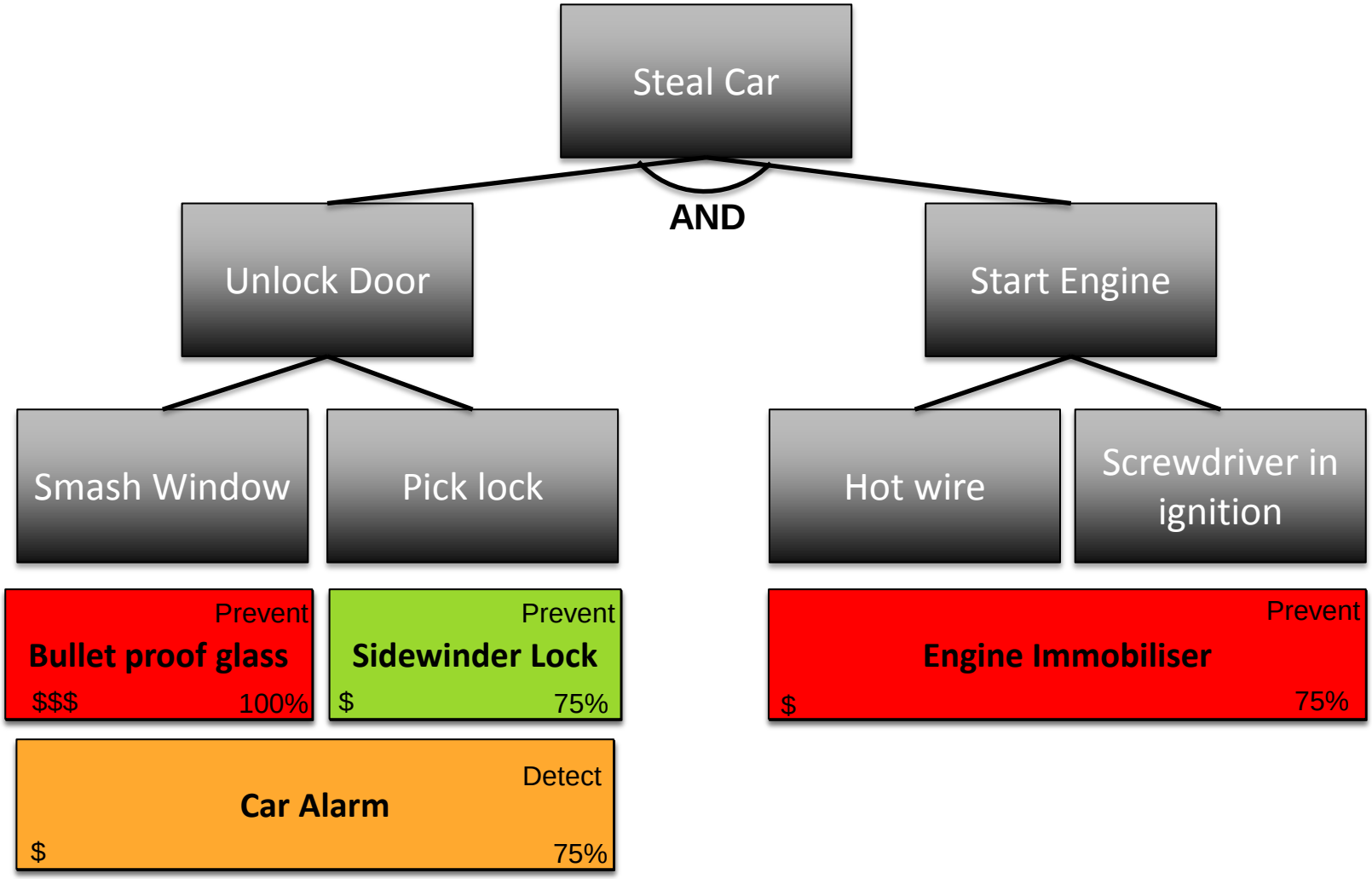
Hybrid Control Set

Application Whitelisting	Data Encryption	Physical Security Controls
Third Party Governance	Data Loss Prevention	Penetration Testing
Layer 7 DDoS Prevention	Network Segmentation	MiTB Detection

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



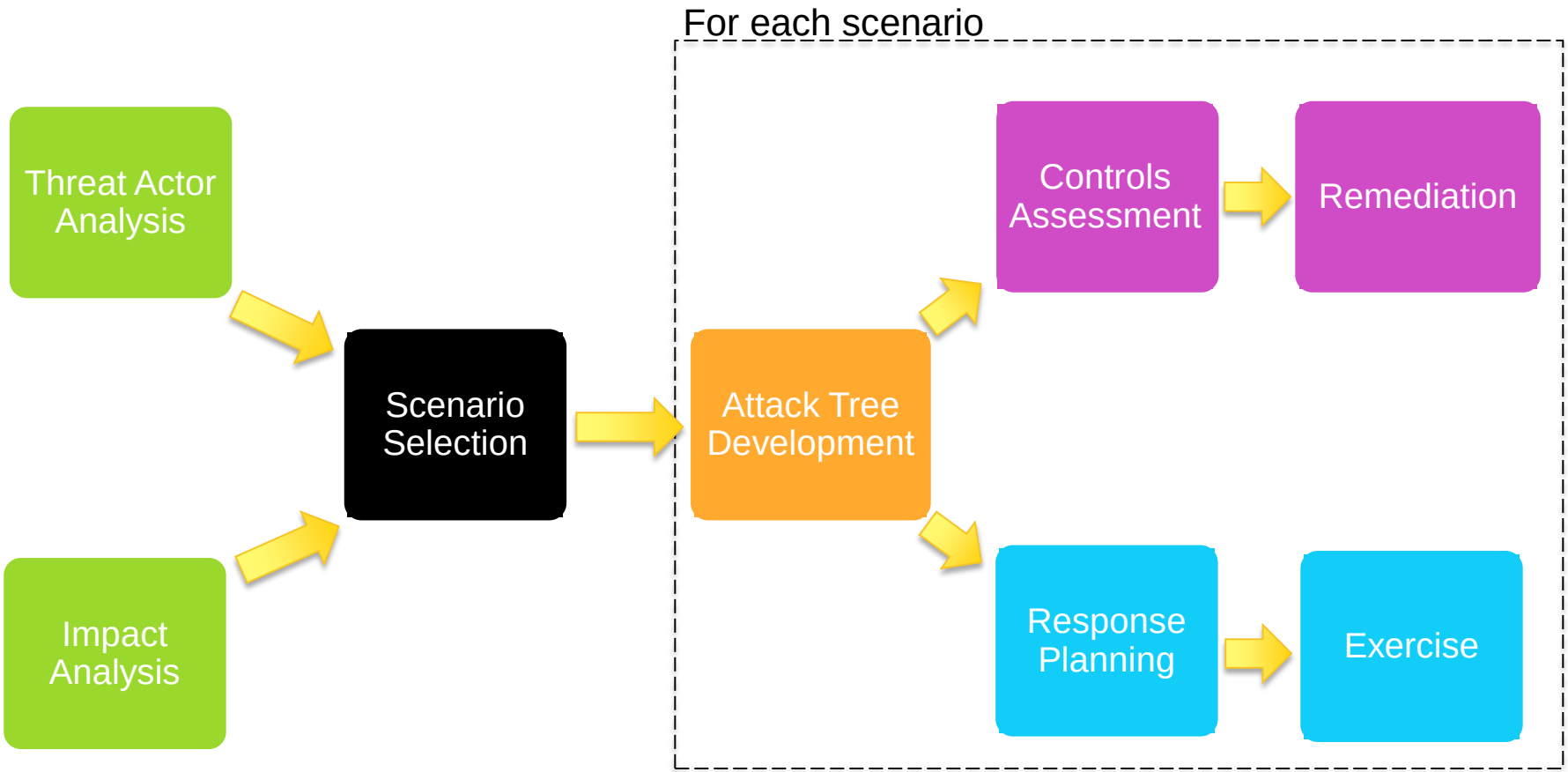
EXTREME CYBER SCENARIO PLANNING

CommonwealthBank

7 Extreme Scenarios

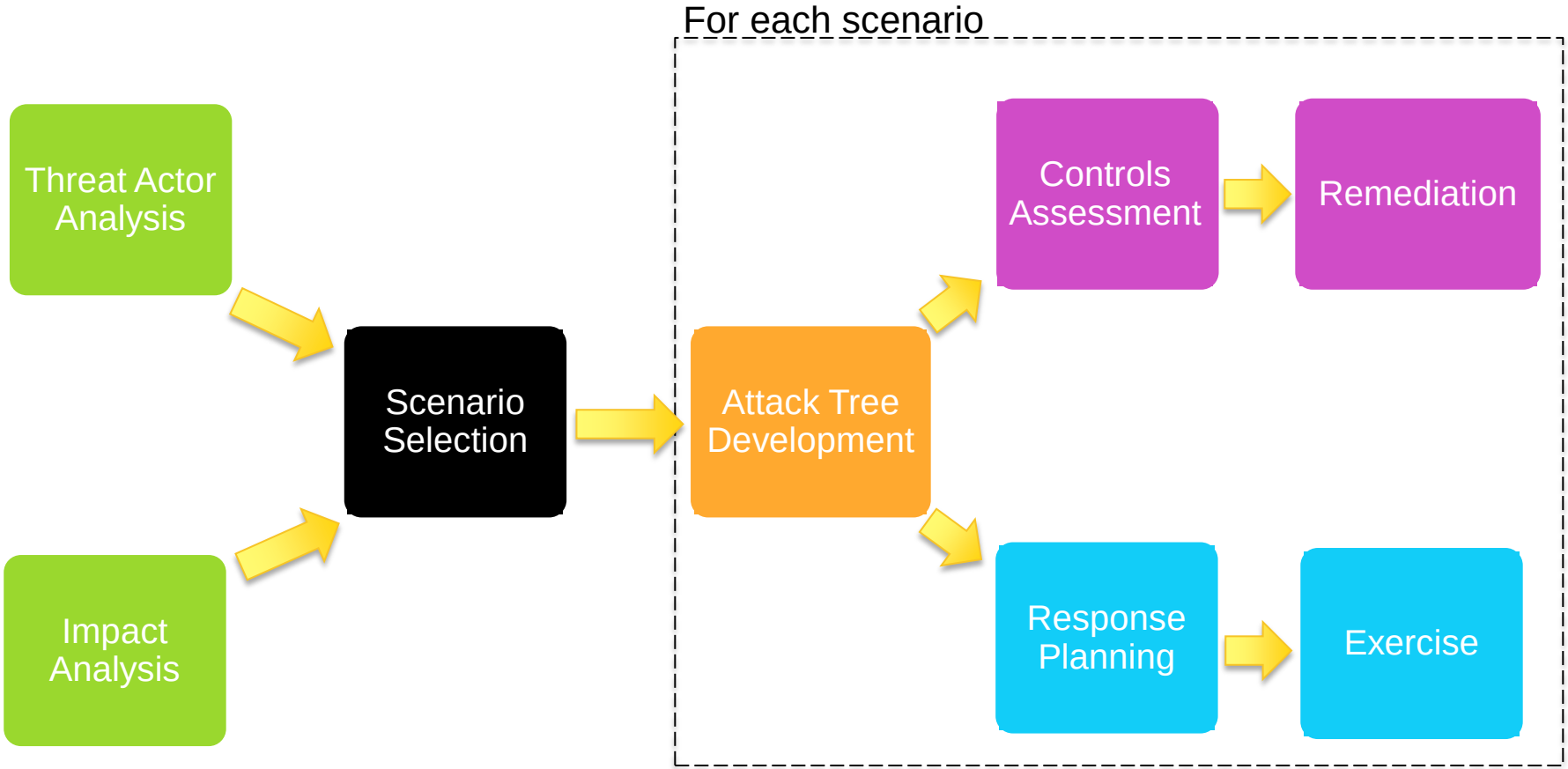
1. Large scale malware campaign against bank customers to steal funds.
2. High value fraud conducted against back end payment system
3. Targeted, prolonged DDoS against multiple Internet facing systems.
4. Exfiltrate and disclose large sets of corporate data to embarrass or discredit the bank.
5. Attacker 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.

Remediation



Aim: Use controls assessment to plan remediation projects which address control gaps

Response Planning



Aim: Create or enhance existing response plans to cater for extreme scenarios

Incident Response Framework

IRP

- Incident Response Plan

IRSOP

- Incident Response Standard Operating Procedure

IRG

- Incident Response Guidelines

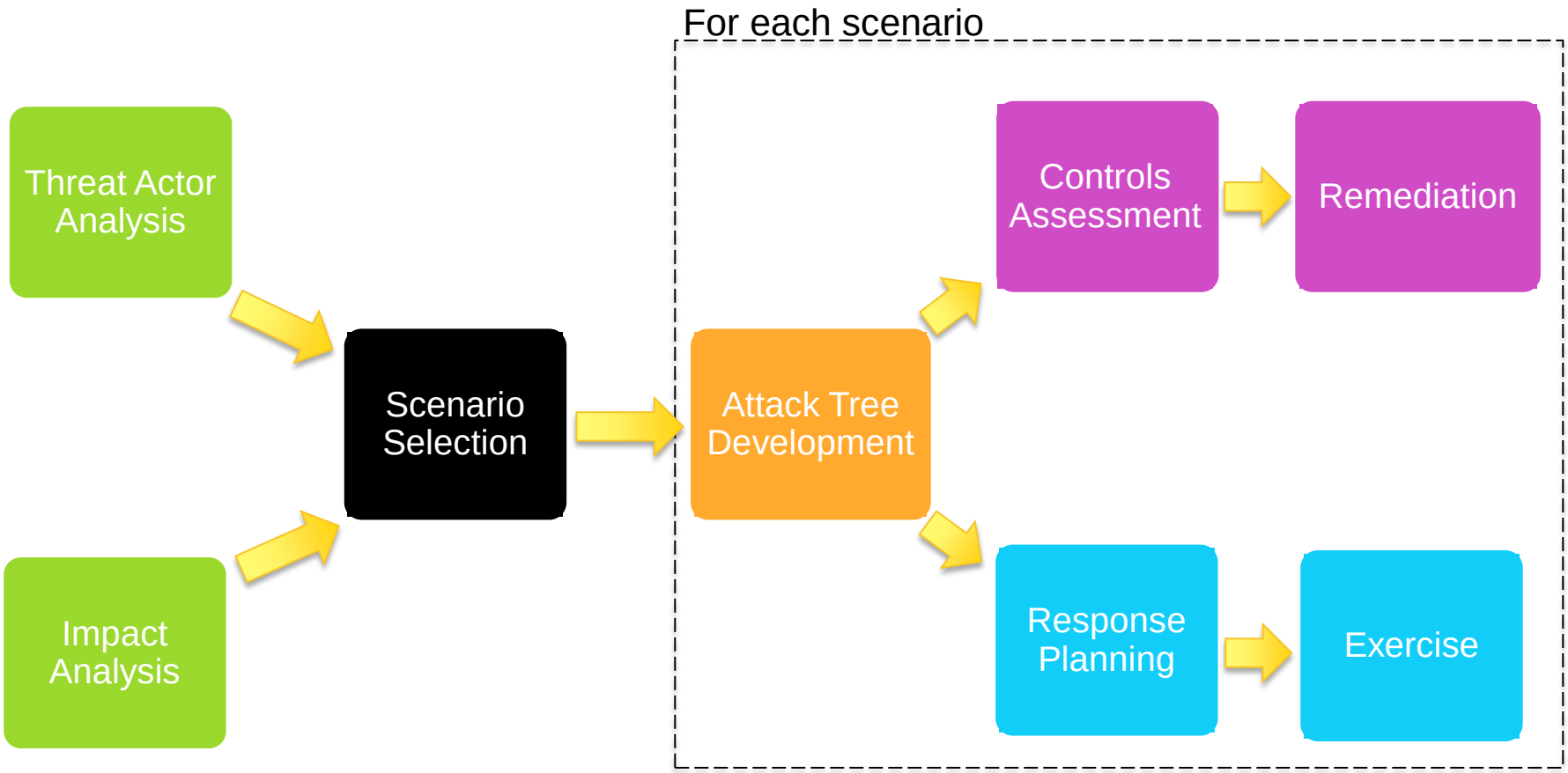
Incident Response Standard Operating Procedures

- Denial of Service
- Compromised Information
- Compromised Asset
- Unlawful Activity
- Probing
- Malware

Response Considerations

- 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?

Exercise

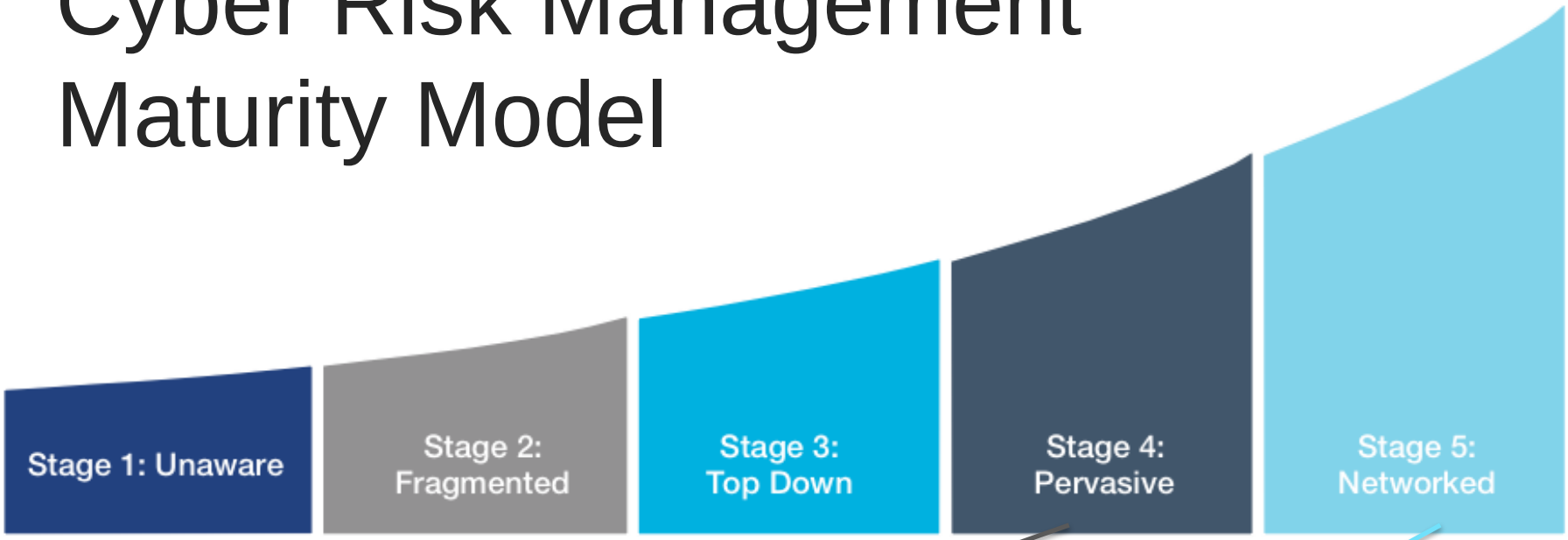


Aim: Test control strength, response plan and overall preparedness

Example: “BYO Botnet”

- HTTP “large resource” request
- HTTPS “large resource” request
- HTTPS “slow” POST attack
- HTTPS search query attack
- SSL Exhaustion
- DNS Query attack
- TCP SYN flood
- IP Fragmentation Attack
- ICMP flood

Cyber Risk Management Maturity Model

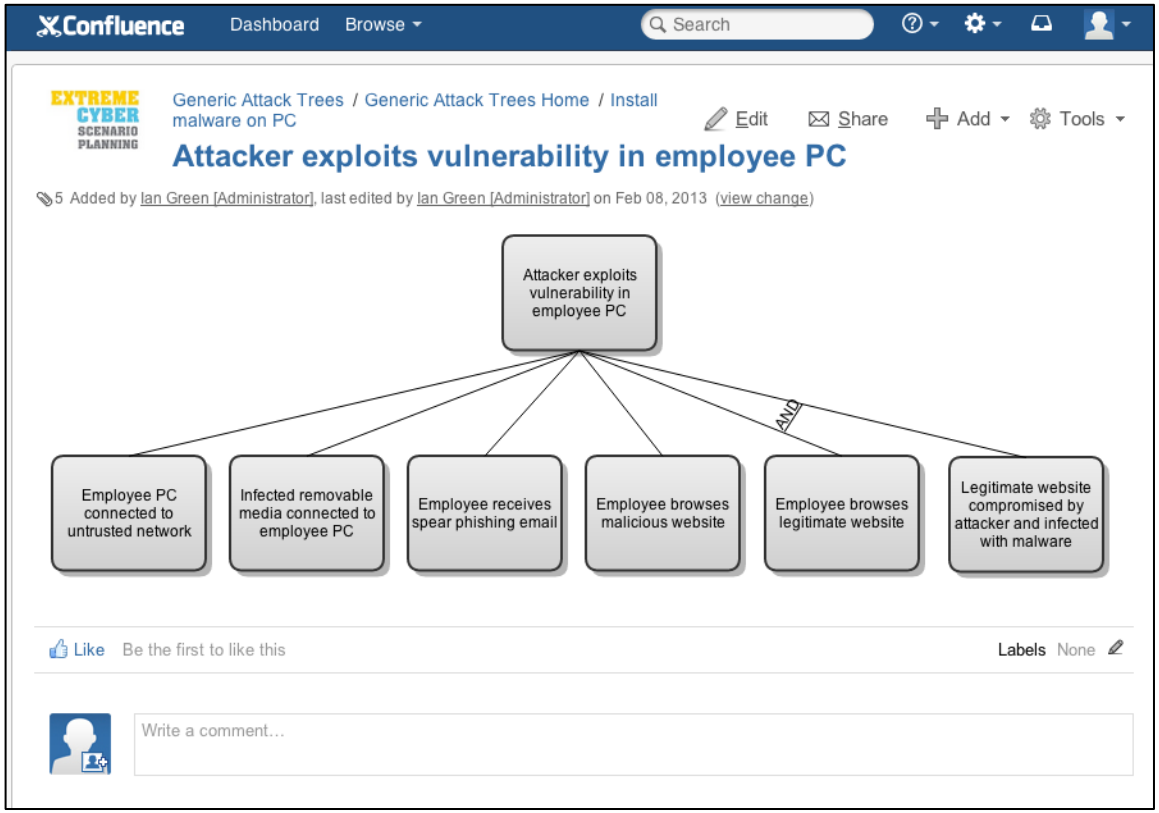


The organisation's leadership takes ownership of cyber risk management… they understand the organisation's vulnerabilities and controls.

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



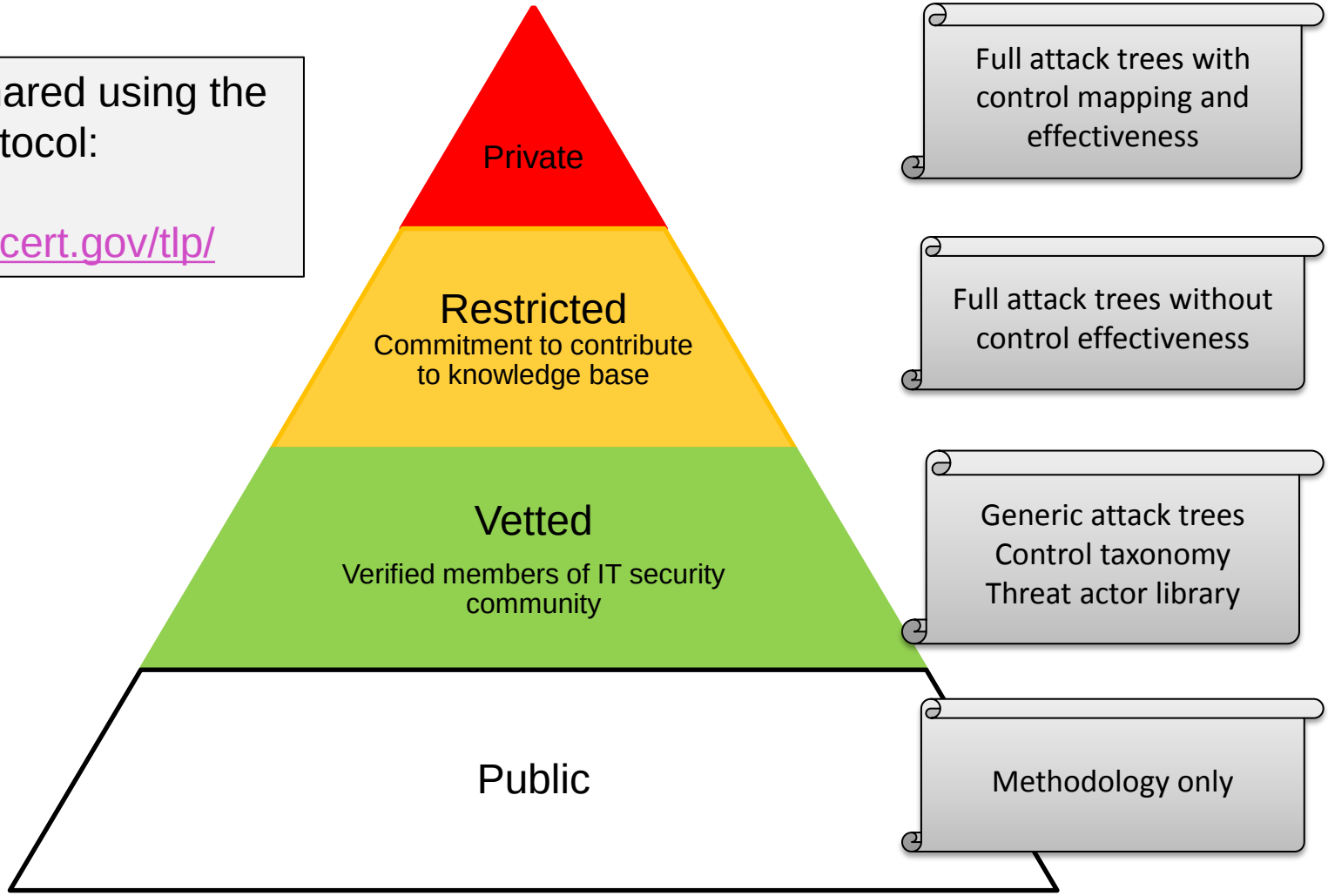
- Traffic light protocol
- Methodology
- Control taxonomy
- Threat actor library
- Generic attack trees
- Full scenario analysis

- Join “Extreme Cyber Scenario Planning” on LinkedIn

extremecyber.net

Information shared using the traffic light protocol:

http://www.us-cert.gov/tlp/



Questions?

- LinkedIn Group “Extreme Cyber Scenario Planning”
- @pragmaticsec
  #extremecyber
- cybercrime@cba.com.au