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?”

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.
Extreme events are costly

Global Payments Inc.

10% or $400m wiped off market cap
How prepared are you?

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

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

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”
HOW?
Threat Actor Analysis

Aim: Identify actors who pose a significant threat to the organisation
## Threat Agent Library – Intel

<table>
<thead>
<tr>
<th>Intent</th>
<th>NON-HOSTILE</th>
<th>HOSTILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquisition/Theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Advantage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embarrassment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tech Advantage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code of Conduct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extra legal minor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extra legal major</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Club</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills (max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adept</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective (1 or more)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destroy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All of the Above/Don't Care</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility (min)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clandestine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multipurpose/Don't Care</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Intel IT Threat Assessment Group, 2007

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)
- **Visibility**: Overt, Covert, Clandestine, Don’t Care

**HOW**

- **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)**
- **Visibility**: Overt, Covert, Clandestine, Don’t Care

**HOW**
- **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

Threat Actor Categories:
- Nation State
- Hacktivist
- Organised Crime
- Terrorists
- Trusted Insider
Threat Actor Analysis

- Organised Crime
- Trusted Insider
- Hacktivist Group
- Terrorist
- Nation State
Threat Actor Analysis

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

- **Trusted Insider**

- **Nation State**

- **Terrorist**

- **Hacktivist Group**
Threat Actor Analysis

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

- Terrorist

- Trusted Insider

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

- Hacktivist Group
Threat Actor Analysis

- **Terrorist**
- **Trusted Insider**
- **Nation State**
- **Organised Crime**
- **Hacktivist Group**

**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

- **Hacktivist Group**
- **Organised Crime**
- **Trusted Insider**
- **Nation State**
- **Terrorist**

**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

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

<table>
<thead>
<tr>
<th>Threat Actor Analysis</th>
<th>Impact Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outcome</strong></td>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Acquisition / Theft</td>
<td>Copy</td>
</tr>
<tr>
<td>Business Advantage</td>
<td>Destroy</td>
</tr>
<tr>
<td>Technical Advantage</td>
<td>Injure</td>
</tr>
<tr>
<td>Damage</td>
<td>Take</td>
</tr>
<tr>
<td>Embarrassment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Scenario Selection

<table>
<thead>
<tr>
<th>Threat Actor Analysis</th>
<th>Impact Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outcome</strong></td>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Acquisition / Theft</td>
<td>Copy</td>
</tr>
<tr>
<td>Business Advantage</td>
<td></td>
</tr>
<tr>
<td>Technical Advantage</td>
<td></td>
</tr>
<tr>
<td>Damage</td>
<td></td>
</tr>
<tr>
<td>Embarrassment</td>
<td></td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Objective</th>
<th>Value at Risk</th>
<th>Potential Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition / Theft</td>
<td>Copy</td>
<td>Customer Funds</td>
<td>Customer Service / Operational</td>
</tr>
<tr>
<td>Business Advantage</td>
<td></td>
<td></td>
<td>Financial</td>
</tr>
<tr>
<td>Technical Advantage</td>
<td></td>
<td></td>
<td>Reputational / Brand</td>
</tr>
<tr>
<td>Damage</td>
<td></td>
<td></td>
<td>Legal / Regulatory Compliance</td>
</tr>
<tr>
<td>Embarrassment</td>
<td></td>
<td></td>
<td>Customers</td>
</tr>
</tbody>
</table>

### Hacktivist Group

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

## Impact Analysis

- Availability of banking systems
- Employee health and safety
- Legal / Regulatory Compliance

### Scenario

Socio-political group performs prolonged denial-of-service attack causing sustained outages.
## Is it “Extreme”?

<table>
<thead>
<tr>
<th>Impact</th>
<th>Financial</th>
<th>Customer Service &amp; Operations</th>
<th>Reputation / Brand</th>
<th>Legal / Regulatory Compliance</th>
<th>People</th>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;$50m</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>1</td>
<td>&lt;$50m</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>2</td>
<td>&lt;$50m</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>3</td>
<td>$50m-$200m</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>4</td>
<td>$200m-$500m</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>5</td>
<td>&gt;$500m</td>
<td>Significant loss of customers due to extensive interruption to service capability</td>
<td>Substantial damage to brands resulting from extensive negative national publicity</td>
<td>Loss of license, loss of public listing or substantial penalties on Directors</td>
<td>Death or severe injury to employees</td>
<td>Serious financial impact to all customers</td>
</tr>
<tr>
<td>Likelihood</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>VH</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>VH</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>I</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>VH</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>I</td>
<td>L</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>I</td>
<td>I</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

Scenarios on Risk Matrix
## Scenario Selection

<table>
<thead>
<tr>
<th>Organised Crime</th>
<th>Hacktivist Group</th>
<th>Nation State</th>
<th>Terrorist</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Gain</strong></td>
<td>1. Large scale targeting of bank customers using malware to steal funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. High value fraud conducted against backend payment system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Theft / Exposure</strong></td>
<td>4. Exfiltrate and disclose large sets of corporate data to embarrass or discredit the bank.</td>
<td>6. Exfiltrate corporate intellectual property for strategic, commercial or political gain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Compromise bank IT systems and exfiltrate large sets of customer data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sabotage / Operations Impact</strong></td>
<td>3. Targeted, prolonged DDoS against multiple Internet facing systems.</td>
<td></td>
<td>7. Destructive cyber-attack against multiple bank data centres.</td>
</tr>
</tbody>
</table>
Aim: Develop detailed attack trees for each extreme scenario
Attack Tree Analysis

Steal Car

Unlock Door
- Smash Window
- Pick lock

Start Engine
- Hot wire
- Screwdriver in ignition
Attack Tree Analysis

“How”?

Steal Car

AND

Unlock Door
Smash Window
Pick lock

Start Engine
Hot wire
Screwdriver in ignition
Attack Tree Analysis

Steal Car

Unlock Door
- Smash Window
- Pick lock

Start Engine
- Hot wire
- Screwdriver in ignition

“And then”?
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.
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
- NIST Special Publication 800-53
- SANS 20 Critical Controls for Effective Cyber Defense
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:

► Status of control:

► Potential to mitigate:

► Cost of control:
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.
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

Threat Actor Analysis

Scenario Selection

Impact Analysis

For each scenario

Attack Tree Development

Remediation

Response Planning

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

► Join “Extreme Cyber Scenario Planning” on LinkedIn
Information shared using the traffic light protocol:

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

- Private
  - Commitment to contribute to knowledge base
- Restricted
  - Verified members of IT security community
- Vetted
- Public

- Full attack trees with control mapping and effectiveness
- Full attack trees without control effectiveness
- Generic attack trees
  - Control taxonomy
  - Threat actor library
- Methodology only
Questions?

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