Location-Specific Cyber Risk

Lincoln Kaffenerger
Cyber Threat Intelligence Officer
IMF Information Security Group

John Kupcinski
Director, Cyber Security
KPMG
Agenda

- Why assess the cyber risks by a physical location
- Overview of the Cyber Risk Location Framework and Methodology
  - Methodology
  - Threat Assessment
• The views expressed herein are those of the speaker and should not be attributed to KPMG, the IMF, its Executive Board, or its management.
Who are these guys?

- Lincoln (@LincolnKberger): Threat Intelligence Officer with the International Monetary Fund.
  - Background: ~10yrs in U.S. Army doing Military Intelligence

- John (@Kupcinski): Cyber Security Director with KPMG
  - Background: ~10 years providing a range of cyber and physical security for public and private clients
WHY ASSESS THE CYBER RISKS BY PHYSICAL LOCATION?

If I’m connected to the internet, aren’t the risks all the same regardless of where I am?
Examples of Threats

The Darkhotel APT
A threat actor possessing a seemingly inconsistent and contradictory set of characteristics, some advanced and not fairly rudimentary. Inconsistently operating, the threat actor is currently

APTs

Insiders

Government

Criminals

Hacktivists

Examples of Threats
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government Monitoring Communications</td>
<td>Ability of the host-nation government to monitor telephone and internet communications inside its physical borders.</td>
<td>Gain political advantage through espionage</td>
</tr>
<tr>
<td>Advance Persistent Threats (APT)</td>
<td>Technically sophisticated, well-resourced, hacker group that continues to attack their target until they achieve their objectives.</td>
<td>Gain political advantage through espionage or attack</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>Criminals that use illegal means to access people or organizations’ networks. May or may not be targeted.</td>
<td>Financial gain</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>Online protesters – often decentralized and limited in resources, but are unpredictable.</td>
<td>Advancing an ideological or political cause</td>
</tr>
<tr>
<td>Insider</td>
<td>Person with privileged access who is self-motivated to carry out an attack against his/her organization</td>
<td>Revenge or to see their project receive “due” notoriety</td>
</tr>
</tbody>
</table>

Categories are not mutually exclusive.
FRAMEWORK AND METHODOLOGY

A consistent, standardized, empirical method for assessing cyber threats and determining information risk.
Cyber Risk Assessment Overview

- Situational Awareness
- Threat Assessment
- Risk Scenarios
- Risk Assessment
- Mitigate Risks

Source: based off of modified version of UN's Department of Safety and Security's Security Level System
1. Monitor country situation and establish information security context

Cyber Risk Assessment Overview: Situational Awareness

- Political Situation
- Economic Situation
- Sociological Situation
- Infrastructure State
- Natural Hazards
- Security Forces
- Threat Actors
2. Measure the threat level based on actor intent and capability.
### Cyber Threat Assessment

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Indicators</th>
<th>Intent</th>
<th>Capability</th>
<th>Inhibiting context*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gov Coms Monitoring</td>
<td></td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>APTs</td>
<td></td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Hacktivist</td>
<td></td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Cyber crime</td>
<td></td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td>1</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

**Overall Threat Rating:** High
<table>
<thead>
<tr>
<th>Type</th>
<th>Indicators</th>
<th>Intent</th>
<th>Capability</th>
<th>Inhibiting context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gov Coms Monitoring</td>
<td>Indicators</td>
<td>Intent</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capability</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inhibiting context*</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>APTs</td>
<td>Indicators</td>
<td>Intent</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capability</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inhibiting context</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>Indicators</td>
<td>Intent</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capability</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inhibiting context</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>Cyber crime</td>
<td>Indicators</td>
<td>Intent</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capability</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inhibiting context</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Indicators</td>
<td>Intent</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capability</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inhibiting context</td>
<td>5</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Intent Description</th>
<th>Capability Description</th>
<th>Inhibiting context Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Groups call for change</td>
<td>Communication; no hacking capability</td>
<td>Strong law enforcement capability to track down or prosecute hacktivist attacks</td>
</tr>
<tr>
<td>2</td>
<td>Groups call for peaceful demonstrations</td>
<td>Ability limited to conducting largely ineffective DDoS attacks against undefended websites</td>
<td>Moderate law enforcement capability to track down or prosecute hacktivist attacks</td>
</tr>
<tr>
<td>3</td>
<td>Groups call for protests</td>
<td>Ability limited to conducting DDoS and website defacement</td>
<td>Some law enforcement capability to track down or prosecute hacktivist attacks</td>
</tr>
<tr>
<td>4</td>
<td>Groups call for mass demonstrations to demonstrate grievances</td>
<td>Ability to conduct moderate to large DDoS attacks; some ability to gain unauthorized access to specific individuals’ accounts or devices</td>
<td>Minimal law enforcement capability to track down or prosecute hacktivist attacks</td>
</tr>
<tr>
<td>5</td>
<td>Groups call for overthrow of current establishment; call for immediate online action</td>
<td>Ability to gain unauthorized access to specific individuals’ accounts or devices</td>
<td>No law enforcement capability to track down or prosecute hacktivist attacks</td>
</tr>
</tbody>
</table>
Factors that cause an attacker to self-restrain his intent/capabilities outside of victim’s controls

Examples:

High Inhibiting Context: Strong Law Enforcement capabilities; Cultural stigma against hacking

Low Inhibiting Context: Weak/no Law Enforcement capability; Culture rewards/praises hacking
3. Formulate organization information security risk scenarios

Risk Assessment

Risk Scenarios

Threat Assessment

Situational Awareness

Mitigate Risks

External Data
- Country asmt.
- Threat asmt.

Internal Data
- Questionnaire
- Assets in loc.
- Vulnerabilities

+ = Risk Scenario

Example: Hacktivists target organization member in country and publicly disclose (dox) his personal emails.
4. Measure the likelihood and impact of all information security risk scenarios.
Plotting likelihood and impact scores for each risk scenario on a risk matrix results in an overview of organization-specific risks in a given location. Overall risk score assessed by the HIGHEST risk event.

EXAMPLE:
G1 - APT breaches org member email in country and publicly disclose (dox) the emails; results in riots and org reputation damage.

Very High Risk
5. Apply mitigating measures to reduce residual risk

**Technology Controls**
- Security monitoring
- Loaner devices
- Check and wipe devices on return

**Process Controls**
- Reduce access to sensitive info
- Only secure communications allowed
- Don’t go to location

**Will help with prioritizing:**
- Investments/procurements
- Logging/monitoring
- Technology deployments
- User awareness/training
- Triage after incident response
Results

- Conducted risk assessments of 3 locations
- Briefed travelers and remote offices on the threats and risks
- Found:
  - 1/3rd of people briefed didn’t know about a secure communications solution we had – improved adoption
  - Users now concerned about security and asking for it
  - Users now reporting security incidents in ways they weren’t before
Closing

- Methodology is a work in progress.
- Feedback and critiques are welcome.

Resources:
- [https://drive.google.com/drive/folders/0By1YzfeyTgkYV1dRYkRYSIRSSUU?usp=sharing](https://drive.google.com/drive/folders/0By1YzfeyTgkYV1dRYkRYSIRSSUU?usp=sharing)
  - CAVEAT – *Inside Threat is still under development.*
  - Has spreadsheet of resources for each type of threat
  - Has questionnaire for travelers and for remote offices
  - Can provide additional methodology upon request
Questions?