Building an Effective Corporate Cyber Threat Intelligence Practice

Greg Rattray, CEO
Delta Risk LLC
10 Feb 2014
Our Path Today

- Corporate Cyber Threat Intelligence
- Value of Corporate Threat Intelligence Practice
- Initiating a Threat Intelligence Practice
- Maturing a Threat Intelligence Practice
- What to do Yourself & Getting Help

Questions and Discussion
Corporate Cyber Threat Intelligence

Definition: Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard (Gartner; 2013)

“If you know the enemy and know yourself you need not fear the results of a hundred battles” (SunTzu)

Purpose: Enable risk reduction

Three Levels:
- Tactical – Improve defense against today’s attacks
- Operational – Focus security engineering and resiliency
- Strategic – Improve corporate risk decisions going forward
Value of Corporate Threat Intelligence Practice

- **Tactical:** Improve the ability of NOC/SOC and other corporate security personnel to anticipate prevent & mitigate cyber attacks across a wide spectrum
  - Including amateurs, fraud, APT, DDOS and insiders
  - Will involve activities that reaches across security functions

- **Operational:** Improve ability of CISO, CIO, CTO to evolve use of IT / Cyber for both protection and response
  - Understand threat to improve security engineering
  - Improve training/exercise programs – improve people

- **Strategic:** Improve CRO, CEO and Board decisions about cyber risk
  - Inform decision about where to operate facilities and people
  - Improve security management of vendors and supply chain
Taking a Holistic Approach

**Noted Best Practices...**
- Risk-driven approach
- Well-defined, centrally managed function
- Enterprise Integration
- Continuous threat understanding
- Automation of threat tracking
- Actionable reporting for multiple audiences

**Guide functional areas...**
- Mission
- Management and Resourcing
- Identifying & Managing Sources
- Intelligence Gathering
- Conducting Fusion and Analysis
- Strategic Activities and Processes
- Reporting

**Lead to...**
- **Tactical Intel**
  - Example: Granular technical indicators (i.e. hash, IP, callback domains)
  - Example: Short-term, technical fix actions (i.e. change technical settings of a firewall)
- **Engineering Solutions**
  - Example: Long-term solution recommendation (i.e. modify implementation of email)
- **Strategic Intel**
  - Example: Business decision support (i.e. active threats in specific geographic location)
- **Strategic Situational Awareness**
Initiating a Threat Intelligence Practice

- Understanding Your Adversaries and Risks
- Establish the Level of Corporate Commitment
  - Mission & Responsibilities -> Resources
- Management
  - Who’s in Charge & Organization
  - Concept of Operation -> Implementation Plan
- Skilled People
  - Ninjas plus Positions
- Sources of Information
  - Internal and External
- Tools and Technical Processes
  - Development of an Analytical Engine

Understand Mission > Assess Current Capabilities > Plan
Be Leery of Heroes
Evolve from Organic to Strategic
<table>
<thead>
<tr>
<th>Risk</th>
<th>Potential Adversary</th>
<th>Description &amp; Intent</th>
<th>Example</th>
<th>Applicability</th>
</tr>
</thead>
</table>
| High      | Organized crime                                 | Independent or collective hackers that collect information that can be sold for a profit or used directly for fraud and extortion; may be for hire for non-state actors | • 2011 Unknown criminal syndicate (Fidelity Information Service)  
• 2013 Eastern European criminals (World Health Organization) | Seek access to client data; target organization to hold data hostage in order to make money |
| Med.      | Hacktivist/ advocacy groups                     | Decentralized group that targets sectors of interest to disrupt productivity and cause reputational damage or advance specific causes through information gathering | • 2007 Albert Gonzalez (Heartland Payment Systems, others)  
• 2010 Anonymous (HBGary, OWS, etc.) | Expose confidential info, inject misinformation into news stream, use website to send a message |
|           | Disgruntled Employees/ Contractor Access         | (may be used by other adversaries) Trying to damage the company/make money             | • 2007-9 Samarth Agrawal (SocGen)  
• 2009-11 Chunlai Yang (Chicago Mercantile Exchange)  
• 2010 Rodney Reed Caverly (Bank of America) | Provide code to others – enable disruption to use as intellectual property; emplace software bugs to cause major systems disruption |
|           | State sponsored entity                           | Well resourced, operational teams with goals to damage competitor interests/impact critical infrastructure operations/track dissidents | • 2006- China (comprehensive)  
• 2007- Russia (Estonia, Georgia)  
• 2009- US/Israel (Iran)  
• 2012- Iran (financial services) | Disrupt ability to provide accurate trading data to shut down markets; get at news investigators |
| Low       | Corporate competitors                            | Other corporate entities that want to understand inner workings of others or steal intellectual property for internal use | • 2008, Starwood sues Hilton for theft of thousands of pages of company data, $75M in damages | Competition for various tools or tradecraft might be of value to competitors, likely to hire ex-employees to get this data |
|           | Opportunists                                     | Unaffiliated hackers (usually young) looking for bragging rights and hacker community recognitions, and may target information could be of value to sell or use | • 1998 Kazakh nationals (Michael R. Bloomberg)  
• 2013 Syrian Group (Associated Press Twitter) | Unaffiliated parties take advantage of security gaps, able to dig around to find information, or other actions |
## Analyze YOUR Potential Attack Vectors

<table>
<thead>
<tr>
<th>Threat Vectors</th>
<th>Description</th>
<th>Example</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider - Access, Control, Knowledge</td>
<td>has legitimate access to networks, systems, code and data</td>
<td>2011, Citigroup employee steals $750k over 8 years by subverting monitoring and audit capabilities</td>
<td>Disgruntled employee accesses customer databases and sells them to competitors; steals payment capabilities</td>
</tr>
<tr>
<td>Cloud-based, Mobile Assets &amp; Social Media</td>
<td>Compromise data stored outside the corporate network, and potentially outside corporate security monitoring</td>
<td>DROPBOX Social Media Mobile Attacks</td>
<td>Information stolen quietly over time; potential lack of clarity on who is responsible for incident response</td>
</tr>
<tr>
<td>System Compromise and Control</td>
<td>Take over specific cyber assets and able to control them; used to exfiltrate data or disrupt operations</td>
<td>2008-present, counterfeit router gear from China presents access risk to infrastructure</td>
<td>Footholds introduced into the environment without traditional infiltration forensic log data</td>
</tr>
<tr>
<td>Supply Chain Corruption</td>
<td>Compromised hardware/software that allows for attacker access – could be foothold</td>
<td>2010, Night Dragon report of Chinese APT targeting financial docs related to oil/gas and bids</td>
<td>Footholds introduced into the environment without traditional infiltration forensic log data</td>
</tr>
<tr>
<td>Social Engineering/Spear Phishing</td>
<td>Through human action gain access/foothold &amp; may lead to targeted exploit; top APT vector</td>
<td>2013, Syrian Electronic Army socially engineers The Onion to take over its Twitter accounts</td>
<td>Attacker gets help desk/HR to open malware; Tangential risk of subsidiaries and other third-party vendor networks</td>
</tr>
<tr>
<td>Disruptive Malware</td>
<td>Malware leveraging access to disrupt/destroy data integrity and/or access to systems</td>
<td>Aramco and 30,000 computers wiped; threats of recce on US energy industry</td>
<td>Custom virus written and implanted to erase systems/corrupt customer databases</td>
</tr>
<tr>
<td>DDoS</td>
<td>Disrupt Internet/public facing services</td>
<td>2013, MasterCard, Paypal and others targeted in a major DDoS attack requiring active responses</td>
<td>Attack against egress points, denying users/field personnel access to corporate information</td>
</tr>
<tr>
<td>Drive-by Malware/rogue USB device</td>
<td>User inadvertently installs; attacker gains foothold; e.g., criminals harvesting PII for fraud or resale</td>
<td>Fake AV and other variants trick users into providing information or allowing hackers to access system</td>
<td>Employee finds USB device and inserts it, or visits drive-by web site, causing system infection</td>
</tr>
</tbody>
</table>

**Note:** The table above outlines various attack vectors and provides examples along with the implications of each.
## Assess Potential Consequences to YOUR Corporation

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputational Damage</td>
<td>Negative perception by customers, media, public due to publicized issues</td>
<td>Organization could experience negative publicity, lose customers, revenue, confidence and potentially be targeted by other cyber adversaries</td>
</tr>
<tr>
<td>Reduction of competitive edge with direct competitors</td>
<td>Theft of intellectual property (e.g. corporate processes, customer databases, privileged communications)</td>
<td>Customers could be contacted by competitors and entice with slightly better deals, tradecraft could be analyzed allowing competitors to improve upon it</td>
</tr>
<tr>
<td>Loss of data or systems</td>
<td>Destruction of data, systems, or access to systems through willing or accidental means; physical loss of mobile devices</td>
<td>Adversaries could alter or destroy data in databases, making it very difficult or impossible for operations to work and requiring incident response/data recovery functions to be enacted</td>
</tr>
<tr>
<td>Data breach disclosure</td>
<td>Compromise of internal integrity and public disclosure of privileged communications or customer data</td>
<td>Posting of sensitive information (e.g. communications, PII, payment information) publicly can not only damage an organization, but create a problem for customers and partners</td>
</tr>
<tr>
<td>Loss of customers</td>
<td>Customer’s loss of confidence in services offered</td>
<td>Customers might simply leave the company for another, regardless of cost, in order to distance themselves from fallout from a catastrophic cyber incident</td>
</tr>
<tr>
<td>Threat Adversary</td>
<td>Threat Vector</td>
<td>Consequence</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disgruntled Employees /</td>
<td>Insider - Access, Control, Knowledge</td>
<td>Customer data or systems corrupted via CLIENT</td>
</tr>
<tr>
<td>Contractors</td>
<td>System Compromise and Control</td>
<td>Loss of sensitive data – customer or corporate</td>
</tr>
<tr>
<td>State sponsored</td>
<td>Supply Chain Corruption</td>
<td>Destruction/disruption of internal data, systems, or access to systems</td>
</tr>
<tr>
<td>entity</td>
<td>Social Engineering/Spear Phishing</td>
<td></td>
</tr>
<tr>
<td>Hacktivist / advocacy</td>
<td>Disruptive Malware</td>
<td>External/Internet connectivity disrupted to enterprise systems</td>
</tr>
<tr>
<td>groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organized crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate competitors</td>
<td>DDoS</td>
<td></td>
</tr>
<tr>
<td>Opportunists</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Maturing a Threat Intelligence Practice

### Focus on Key Functional Areas

<table>
<thead>
<tr>
<th>Functions of Threat Intelligence</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Management and Resourcing</td>
<td>Ensure clear direction to the team, establish a focal point for prioritization, allocate resources and integrate with security, and confirm incident response and other organizational functions</td>
</tr>
<tr>
<td>Identifying and Managing Sources of Threat Intelligence</td>
<td>Provide the intelligence team with the understanding of where intelligence comes from</td>
</tr>
<tr>
<td>Intelligence Gathering</td>
<td>Identify the processes needed for collecting information from intelligence sources</td>
</tr>
<tr>
<td>Conducting Fusion and Analysis</td>
<td>Understand the need to analyze and develop actionable reporting for operations</td>
</tr>
<tr>
<td>Strategic Activities and Processes</td>
<td>Comprehend issues with tracking emerging and geographically based threats</td>
</tr>
<tr>
<td>Reporting</td>
<td>Describes the various types of reporting the team should consider and how to develop the reports</td>
</tr>
</tbody>
</table>

- Establish metrics to drive impact and improvement meaningful to executives
  - How to activities improve decisions and actions?
- Integrate threat intelligence processes and products into corporate risk management
## Example Maturity Evaluation Framework: Identifying & Managing Sources of Threat Intel

<table>
<thead>
<tr>
<th>Requirements</th>
<th>ML1</th>
<th>ML2</th>
<th>ML3</th>
<th>ML4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2. Identifying &amp; Managing Sources of Threat Intel</strong></td>
<td>- Threat intelligence team &amp; employees</td>
<td>Personnel: Minimal if any threat intelligence experience &amp; training</td>
<td>Personnel: Some threat intelligence experience &amp; training; disparate disciplines that may or may not overlap</td>
<td>Personnel: Advanced threat intelligence experience &amp; training, react well to current threats, and can proactively define and document future threats; can inform threat intelligence personnel at similar organizations</td>
</tr>
<tr>
<td></td>
<td>Process: No processes exist for adding new sources. New sources are disparate and may not integrate.</td>
<td>Process: Informal, single person initiated, processes exist for managing TI sources.</td>
<td>Process: Structured process to vet and add new TI sources. New sources integrate with few troubles into existing system.</td>
<td>Process: Well documented processes that vet and manage new sources, and discourage overlapping sources. Integration with existing TI system is always a consideration, and occurs at all levels.</td>
</tr>
<tr>
<td></td>
<td>Tools/Tech: Basic understanding of current threat intelligence tools and capability providers; minimal ability for staff to leverage basic tools</td>
<td>Tools/Tech: Moderate understanding of TI tools &amp; capability providers; ability for staff to leverage basic tools, some ability for intermediate/advanced tools</td>
<td>Tools/Tech: Deep understanding of current threat intelligence tools and capability providers; staff can thoroughly leverage basic tools, improved ability for intermediate/advanced tools</td>
<td>Tools/Tech: Advanced understanding of current threat intelligence tools and capability providers; staff can intuitively leverage basic tools, strong ability to leverage and customize intermediate/advanced tools</td>
</tr>
</tbody>
</table>
Sample Analytic Engine

Database

Indexer

Correlation

APT Profile Database

SOC/CERT Analyst

Visualization

Trends & Metrics

Internal Data Feeds, Logs, Forensics Data, Alerts, etc

Domain Tools

VirusTotal

Mailing Lists

ISAC

Other Inputs

Alerts

Correlation

INFO

OUTPUTS

Recommended Tactical Action

Situational Awareness & Reporting

Authorize Automated Blocks

Business Management

Feedback
Establishing Operational Level Analysis

- Drive proactive changes to IT Infrastructure and net defense posture through understanding adversary, TTP and rhythms

- Drive training, exercise and range environments based on realistic adversary replication – people are your greatest asset
Establishing Strategic Level Analysis

- **Adversary Evolution**
  - Improved Capability of Cyber Guerilla Forces
  - Emergence of Cyber Weapons focus on RF access & disruption

- **Geo-Cyber Risk Analysis**
  - Exposures to facilities, people, data flows

- **Business Evolution, Mergers & Acquisitions**
  - Cyber security posture of new business operations

- **Supply Chain and Vendors**
  - Increasing the threat vector of sophisticated attackers
  - Integrate into vendor management process

- **Technology Evolution**
The Meaning of Geocytber Risk

Despite the Internet’s global presence, cyber threats occur within localized environments. Companies with global operations face diverse cyber threats depending on where the company operates. By tailoring operational security to in-country risk, companies can efficiently allocate resources and prioritize protection of its most vulnerable operational centers.

Examples of Geocytber Risk

• **Human Enabled Cyber Activities**
  - Device access (Cell phones, Laptops, USBs, etc) – theft or spyware infection
  - Physical access to networks, infrastructure, other opportunities
  - Origins of spear phishing attacks – email spoofing targeted at specific individuals or organizations

• **Activity of Specific Actors enabled by Proximity**
  - Patriot hackers such as the Honker's Union of China and mercenaries like Hidden Lynx
  - Government-run groups such as Unit 61398 aka APT

• **Poor Cyber Hygiene in Operating Environment**
  - High amount of pirated software and Operating Systems; pirates wary of system updates due to chance of being locked out of own pirated software
  - Poor operating/security practices of local businesses
  - High malware infection rate

• **Governmental Climate**
  - Permissive industrial and intelligence service espionage or cyber dissents
  - Policies that exacerbate poor hygiene, environmental & supply chain conditions
Benchmark Program & Establish Improvement Goals

Our Rating of the Recommended Goals

1. Mission Management & Resourcing
2. Identifying & Managing Sources of Threat Intel
3. Intelligence Gathering
4. Conducting Fusion & Analysis
5. Strategic Activities and Processes
6. Reporting

Maturity Level: 0 1 2 3 4

Delta Risk LLC © 2013
Example Metrics for Cyber Threat Intel Practice

More Qualitative

- **Strategic:** CRO determinations of corporate risk are impacted based upon threat intelligence outputs
  - Indicative of a well informed CRO, fed by information gleaned at all stages of threat intelligence.

- **Operational:** Time to respond to a known high severity intrusion
  - Indicative of change in capability (people/process/technology) in intrusion response.
  - Time should be from detection to containment of intrusion.

- **Tactical:** Number of threats detected in a given month
  - Indicative of the quality of detection capability within an organization.
  - Similar metrics exist for prevention, and response.

More Quantitative
What to do Yourself & Getting Help

- Driven by desired capability as well as corporate culture
  - Fully mature capabilities require wide range of skills and tools
  - Wide range of capabilities are appropriate
  - Corporate cultures differ regarding use of outside help

- Minimum to-dos for a practice
  - Organize – establish who is in charge of the practice, duties for personnel related to threat intelligence & reporting requirements
    - Document to avoid “hit by a bus” scenario
  - Plan – forecast for future fiscal years, ask for budget lines to organize or equip better, use previous threat intel data to help make the case
  - Equip – ensure management and technical personnel are armed with the right tools (and the right data)

- Analyze what’s available to reach desired level of capability
  - Lots of options; it’s a complex task
Fast Increasing Field of Threat Intel Providers

- Red Sky Alliance
- CrowdStrike
- RSA Security
- IBM
- Mandiant
- General Dynamics
- iSIGHT Partners
- Looking Glass
- Invincea
- Team CyMru
- Cyveillance
- McAfee
- Vigilant by Deloitte
- Trustwave
- FireEye
- Dell SecureWorks
Threat Intel Providers – Criteria & Metrics

Criteria to help rate providers

1) What’s Advertised
2) What’s Really offered
3) Hands on assessment
4) Strengths
5) Weaknesses
6) Business line categorization
7) Primary threats tracked Intent
8) TTPs
9) Intent
10) Forums
11) Portal
12) Ease of use
13) Automated Data source
14) Data
15) Presentation
16) Content
17) Output
18) Usability
19) Integration
Parting Shots

➢ Technology Drives Risks

➢ Take a Global Perspective

➢ Collaboration

➢ Learning
Questions?

Greg Rattray
grat tray@delta-risk.net