Bridging the Gap Between Threat Intelligence and Risk Management

Toni Gidwani
Director of Research Operations

ThreatConnect
@ThreatConnect
Underlying assumption

Good **intelligence** makes smarter **models**; Smarter models inform **decisions**; Informed decisions drive better **practice**; Better practice improves **risk** posture; which, done efficiently, Makes a successful security **program**.
Does your security program look like this?
Threat Intelligence
Risk Management
They have some issues dividing them...

**Threat Intelligence**

- “There’s way too much uncertainty around her. I live and die in a binary world.”
- “I beat adversaries with STIX and detonate their remains. She plays with numbers.”
- “People say she’s ‘stochastic.’ That explains a lot; she needs serious help.”
- “She doesn’t even cyber! Need I say anything more?”

**Risk Management**

- “He’s intolerable. I assess he needs to be treated and transferred to a third party.”
- “One look at his laptop makes me panic. It’s a giant audit finding with a keyboard.”
- “He never shares with coworkers. I swear, if he TLP-Red’s us one more time...”
- “What’s his deal with China, anyway? It’s an HR liability if you ask me.”
... but they’d make such a great team.
Agenda

- Bridging risk & IR in Verizon’s DBIR
- Building understanding
- Finding common ground
- Bridging the gap
- Crossing the divide (apply)
Bridging Risk and IR in Verizon’s DBIR
## Bridging risk and IR in the DBIR

### Frequency of incident classification patterns per victim industry

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>POS INTRUSION</th>
<th>WEB APP ATTACK</th>
<th>INSIDER MISUSE</th>
<th>THEFT/LOSS</th>
<th>MISC. ERROR</th>
<th>CRIMeware</th>
<th>PAYMENT CARD SKIMMER</th>
<th>DENIAL OF SERVICE</th>
<th>CYBER ESPIONAGE</th>
<th>EVERYTHING ELSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>74%</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>20%</td>
<td>&lt;1%</td>
<td>1%</td>
</tr>
<tr>
<td>Administrative</td>
<td>4%</td>
<td>11%</td>
<td>22%</td>
<td>2%</td>
<td>56%</td>
<td>4%</td>
<td>81%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Education</td>
<td>&lt;1%</td>
<td>19%</td>
<td>8%</td>
<td>15%</td>
<td>20%</td>
<td>6%</td>
<td>99%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment</td>
<td>1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>&lt;1%</td>
<td>48%</td>
<td>3%</td>
<td>&lt;1%</td>
<td>1%</td>
<td>2%</td>
<td>6%</td>
<td>34%</td>
<td>&lt;1%</td>
<td>5%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5%</td>
<td>4%</td>
<td>23%</td>
<td>32%</td>
<td>18%</td>
<td>4%</td>
<td>2%</td>
<td>11%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>&lt;1%</td>
<td>12%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>11%</td>
<td>4%</td>
<td>46%</td>
<td>3%</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1%</td>
<td>6%</td>
<td>6%</td>
<td>1%</td>
<td>5%</td>
<td>&lt;1%</td>
<td>33%</td>
<td>16%</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>90%</td>
<td>2%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>22%</td>
<td>20%</td>
<td>24%</td>
<td>16%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>32%</td>
<td>13%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>45%</td>
<td>2%</td>
<td>16%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td>35%</td>
<td>6%</td>
<td>6%</td>
<td>10%</td>
<td>26%</td>
<td>16%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: 2016 Verizon DBIR
Bridging risk and IR in the DBIR

The Intelligence Gap

Percent of breaches where time to compromise (red)/time to discovery (blue) was day or less

Breach discovery methods over time

**All Figures from Verizon DBIR**
Building Understanding
What is threat intelligence?

“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_

“The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence’s primary purpose is to inform business decisions regarding the risks and implications associated with threats.”

_FORRESTER_
Classic intelligence cycle

DIRECTION

COLLECTION

ANALYSIS

PROCESSING

Distribute finished intel products
Evaluate, integrate, and interpret intel
Process intel for exploitation
Collect intel in support requirements
Plan intel requirements to meet objectives
Threat intelligence process
The Diamond Model of Intrusion Analysis
Threat intelligence process

1) Victim discovers malware
2) Malware contains C2 domain
3) C2 domain services to IP address
4) Firewall logs reveal more comms to C2 IP
5) IP address ownership details reveal adversary
What is risk?

“The probable frequency and probable magnitude of future loss.”

– Factor Analysis of Information Risk (FAIR)
Risk management process (NIST 800-39)

Frame: establishes the context for risk-based decisions and strategy for execution

Monitor: verifies proper implementation, measures ongoing effectiveness, tracks changes that impact effectiveness or risk, etc.

Assess: encompasses everything done to analyze and determine the level of risk to the organization

Respond: addresses what organizations choose to do once risk has been assessed and determined
Risk management process

(ISO 27005)
Finding Common Ground
Risky questions needing intelligence answers

- What types of threats exist?
- Which threats have occurred?
- How often do they occur?
- How is this changing over time?
- What threats affect my peers?
- Which threats could affect us?
- Are we already a victim?
- Who’s behind these attacks?
- Would/could they attack us?
- Why would they attack us?
- Are we a target of choice?
- How would they attack us?

- Could we detect those attacks?
- Are we vulnerable to those attacks?
- Do our controls mitigate that vulnerability?
- Are we sure controls are properly configured?
- What happens if controls do fail?
- Would we know if controls failed?
- How would those failures impact the business?
- Are we prepared to mitigate those impacts?
- What’s the best course of action?
- Were these actions effective?
- Will these actions remain effective?
Intel in the risk management process

Frame: adjust intelligence direction and ops to meet the needs of risk management

Monitor: intelligence tracks threat changes that warrant system and control changes

Assess:
1. Select asset(s) at risk
2. Identify risk scenarios
3. Estimate risk factors
4. Determine risk level

Respond: intelligence supports evaluation and implementation of courses of action
Finding some common ground

Factor Analysis of Information Risk (FAIR)
Finding some common ground

Structured Threat Information eXpression (STIX)
Finding some common ground

A FAIR-ly intelligent approach

**Threat Intel (STIX)**

- Campaign
- Indicator
- Threat Actor
- Target
- Course of Action
- Incident

**Risk Analysis (FAIR)**

- Risk
  - Loss Event Frequency
  - Vulnerability
  - Threat Event Frequency
  - Probability of Action
  - Threat Capability
  - Resistance Strength
  - Secondary LEF
  - Secondary LM

- Type
- Sophistication
- Planning and Support
- Intended Effect
- Observed TTPs

*Initial map: threatconnect.com/threat-intelligence-driven-risk-analysis/*
Finding some common ground

A FAIR-ly intelligent approach

Threat Intel (STIX)

Risk Analysis (FAIR)

- Behavior
- Resources
- Kill Chain Phases
- Exploit Target

* Initial map: threatconnect.com/threat-intelligence-driven-risk-analysis/
Bridging the Gap
“During a recent audit, it was discovered that there were active accounts in a customer service application with inappropriate access privileges. These accounts were for employees who still worked in the organization, but whose job responsibilities no longer required access to this information. Internal audit labeled this a high risk finding.”

From: Measuring and Managing Information Risk by Jack Freund and Jack Jones (p. 123)
Example risk assessment project

FAIR analysis process flow

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 93)
Example risk assessment project

Scenarios associated with inappropriate access privileges

<table>
<thead>
<tr>
<th>Asset at Risk</th>
<th>Threat Community</th>
<th>Threat Type</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer PII</td>
<td>Privileged insiders</td>
<td>Malicious</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Customer PII</td>
<td>Privileged insiders</td>
<td>Snooping</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Customer PII</td>
<td>Privileged insiders</td>
<td>Malicious</td>
<td>Integrity</td>
</tr>
<tr>
<td>Customer PII</td>
<td>Cyber criminals</td>
<td>Malicious</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

FAIR estimations relevant to the cyber criminal scenario

<table>
<thead>
<tr>
<th>TEF Min</th>
<th>TEF M/L</th>
<th>TEF Max</th>
<th>TCap Min</th>
<th>TCap M/L</th>
<th>TCap Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5 / year</td>
<td>2 / year</td>
<td>12 / year</td>
<td>70</td>
<td>85</td>
<td>95</td>
</tr>
</tbody>
</table>

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 127)
**Example risk assessment project**

**Standard cyber criminal threat profile**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motive</td>
<td>Financial, intermediary.</td>
</tr>
<tr>
<td>Primary intent</td>
<td>Engage in activities legal or illegal to maximize their profit.</td>
</tr>
<tr>
<td>Sponsorship</td>
<td>Non-state sponsored or recognized organizations (illegal organizations or gangs).</td>
</tr>
<tr>
<td>Targets</td>
<td>Financial services and retail organizations.</td>
</tr>
<tr>
<td>Capability</td>
<td>Professional hackers. Well-funded, trained, and skilled.</td>
</tr>
<tr>
<td>Risk Tolerance</td>
<td>Relatively high; however, willing to abandon efforts that might expose them. Prefer to keep their identities hidden.</td>
</tr>
<tr>
<td>Methods</td>
<td>Malware, stealth attacks, and Botnet networks.</td>
</tr>
</tbody>
</table>

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 54)
Example risk assessment project
Example intelligence-driven adversary profile

**ADVERSARY**

**GROUP:** Anunak/carbanak, **TYPE:** eCrime
**MOTIVE:** Financial or economic, **ORIGIN:** Russia

**CAPABILITIES**

**VIRLOCK**

**EXPLOITS**
CVE-2012-2539, CVE-2012-0158

**TOOLS**
Mimikatz, MBR Eraser, Network Scanner, Cain & Abel, SSHD backdoor, Ammy Admin, Team Viewer

**INFRASTRUCTURE**

**IPS**
128.92.31.17
176.31.127.162

**HOSTS**
login.collegefanta[.]org
login.loginto[.]me
img.in-travelusa[.]com

**KNOWN TO RENT ADVERSARY INFRA**

**ORGANIZATIONS:** Acme Corp (that’s us), 50 Russian banks, British bank
**ASSETS:** Endpoints, servers, ATMs, SWIFT network

**TECHNICAL AXIS**

1. **CAPABILITIES**
   - Spear phishing, CSRF, SQLi
   - DNS hijack, parameter tampering
   - ATM withdrawals

2. **FILES VIRLOCK**
   - CVE-2012-2539, CVE-2012-0158

**SOCIOPOLITICAL AXIS**

1. **Intent:** High
   **Target Geo:** US, RU
   **Target Sector:** FinSrv
   **Timeline:** 2014 to present

2. **TECHNICAL AXIS**
   - Spear phishing, CSRF, SQLi
   - DNS hijack, parameter tampering
   - ATM withdrawals

3. **INFRASTRUCTURE**
   - **IPS**
     - 128.92.31.17
     - 176.31.127.162
   - **HOSTS**
     - login.collegefanta[.]org
     - login.loginto[.]me
     - img.in-travelusa[.]com
   - **KNOWN TO RENT ADVERSARY INFRA**
   - **ORGANIZATIONS:** Acme Corp (that’s us), 50 Russian banks, British bank
   - **ASSETS:** Endpoints, servers, ATMs, SWIFT network

© 2016 ThreatConnect, Inc. All Rights Reserved | All material confidential and proprietary
Example risk assessment project

Example intelligence-driven threat community profile .... OVER TIME
Crossing the Divide
Making it work in your organization

1. Initiate communication between intel and risk teams
2. Orient intel processes and products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines and procedures for risk assessment projects
5. Encourage ongoing coordination and collaboration
   - Create centralized tools/repositoriess
Underlying assumption

Motivating conviction

Good intelligence makes smarter models;
Smarter models inform decisions;
Informed decisions drive better practice;
Better practice improves risk posture;
which, done efficiently,
Makes a successful security program.
THANK YOU!
Bridging the Gap Between Threat Intelligence and Risk Management

Toni Gidwani
Director of Research Operations

ThreatConnect
@ThreatConnect