Bridging the Gap Between Threat Intelligence and Risk Management

Wade Baker
VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker
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?
Risk Management
“There’s way too much uncertainty around her. I live & die in binary world.”

“I beat adversaries with STIX & 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, bro! Need I say anything more?”

“He’s intolerable. I assess he needs to be treated & transferred to a 3rd 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>75%</td>
<td>1%</td>
<td>8%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>10%</td>
<td>1%</td>
<td>4%</td>
</tr>
<tr>
<td>Administrative</td>
<td>8%</td>
<td>27%</td>
<td>12%</td>
<td>43%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>13%</td>
<td>7%</td>
</tr>
<tr>
<td>Construction</td>
<td>7%</td>
<td>13%</td>
<td>13%</td>
<td>7%</td>
<td>33%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>&lt;1%</td>
<td>6%</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>7%</td>
<td>22%</td>
<td>10%</td>
<td>7%</td>
<td>12%</td>
<td>2%</td>
<td>2%</td>
<td>32%</td>
<td></td>
<td>5%</td>
</tr>
<tr>
<td>Finance</td>
<td>&lt;1%</td>
<td>27%</td>
<td>7%</td>
<td>3%</td>
<td>5%</td>
<td>4%</td>
<td>22%</td>
<td>26%</td>
<td>&lt;1%</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
<td>3%</td>
<td>15%</td>
<td>46%</td>
<td>12%</td>
<td>3%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Information</td>
<td>&lt;1%</td>
<td>41%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>31%</td>
<td>&lt;1%</td>
<td>9%</td>
<td>1%</td>
<td>16%</td>
</tr>
<tr>
<td>Management</td>
<td>11%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td></td>
<td>11%</td>
<td>44%</td>
<td>11%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>14%</td>
<td>8%</td>
<td>4%</td>
<td>2%</td>
<td>9%</td>
<td></td>
<td>24%</td>
<td>30%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Mining</td>
<td>25%</td>
<td>10%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>40%</td>
<td>5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>&lt;1%</td>
<td>9%</td>
<td>6%</td>
<td>4%</td>
<td>3%</td>
<td>3%</td>
<td>37%</td>
<td>29%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>&lt;1%</td>
<td>24%</td>
<td>19%</td>
<td>34%</td>
<td>21%</td>
<td></td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td>10%</td>
<td>37%</td>
<td>13%</td>
<td>20%</td>
<td>7%</td>
<td></td>
<td>3%</td>
<td>10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>31%</td>
<td>10%</td>
<td>4%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>6%</td>
<td>33%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Figure from Verizon 2014 DBIR
Bridging Risk and IR in the DBIR

The Intelligence Gap

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

Breach discovery methods over time

"Intel Stop-gap"

"Intelligence Gap"

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

1) Victim discovers malware

2) Malware contains C2 domain

3) C2 domain resolves 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

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

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

Respond: addresses what organizations choose to do once risk has been assessed and determined.
Risk management process (ISO 27005)

- "Frame"
- "Assess"
- "Respond"
- "Monitor"
Finding Common Ground
<table>
<thead>
<tr>
<th>Question</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>What types of threats exist?</td>
<td>Could we detect those attacks?</td>
</tr>
<tr>
<td>Which threats have occurred?</td>
<td>Are we vulnerable to those attacks?</td>
</tr>
<tr>
<td>How often do they occur?</td>
<td>Do our controls mitigate that vulnerability?</td>
</tr>
<tr>
<td>How is this changing over time?</td>
<td>Are we sure controls are properly configured?</td>
</tr>
<tr>
<td>What threats affect my peers?</td>
<td>What happens if controls do fail?</td>
</tr>
<tr>
<td>Which threats could affect us?</td>
<td>Would we know if controls failed?</td>
</tr>
<tr>
<td>Are we already a victim?</td>
<td>How would those failures impact the business?</td>
</tr>
<tr>
<td>Who’s behind these attacks?</td>
<td>Are we prepared to mitigate those impacts?</td>
</tr>
<tr>
<td>Would/could they attack us?</td>
<td>What’s the best course of action?</td>
</tr>
<tr>
<td>Why would they attack us?</td>
<td>Were these actions effective?</td>
</tr>
<tr>
<td>Are we a target of choice?</td>
<td>Will these actions remain effective?</td>
</tr>
<tr>
<td>How would they attack us?</td>
<td></td>
</tr>
</tbody>
</table>
Intel in the risk management process

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

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

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

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)

Source: https://stixproject.github.io/
Finding some common ground
A FAIR-ly intelligence approach

Threat Intel (STIX)

Risk Analysis (FAIR)

- Behavior
- Sophistication
- Kill_Chain_Phases
- Exploit_Target
- Observed_TTPs

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

Scenarios → FAIR Factors → Expert Estimation → PERT → Monte Carlo engine → Risk

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

**SOCIO-POLITICAL AXIS**
- Intent: High
- Target Geo: US, RU
- Target Sector: FinSrv
- Timeline: 2014 to present

**TECHNICAL AXIS (TTPS)**
- Spear phishing, CSRF, SQLi, DNS hijack, Parameter tampering
- A&M withdrawals

**CAPABILITIES**
- Files: 6773a8354a[...]
- VIRLOCK
  - Exploits: CVE-2012-2539, CVE-2012-0158
  - Tools: Mimikatz, MBR Eraser, Network Scanner, Cain & Abel, SSHD backdoor, Amyny Admin, Team Viewer

**ADVERSARY**
- Group: Anunak/Carbanak
- Type: eCrime
- Motive: Financial or economic
- Origin: Russia

**INFRASTRUCTURE**
- IPs: 78.128.92[]117, 176.31.157[]62
- Hosts: log.n.collegefan[]org, log.n.log.ntol[]me, img.in.travelusa[]com

**VICTIM**
- Organizations: Acme Corp (that's us), 50 Russian banks, British bank
- Assets: Endpoints, servers, ATMs, SWIFT network

Known to rent adversary infr
Example risk assessment project

Example intelligence-driven threat community profile...OVER TIME

Manufacturing (31) 12.2%
Information (51) 10.4%
Food Services (722) 9.9%
Professional (54) 9.9%
Unknown 8.4%
Finance (52) 8.1%
Transportation (48) 6.1%
Public (92) 3.5%
Other Services (81) 2.3%
Utilities (22) 1.7%
Administrative (56) 1.4%
Educational (61) 1.2%
Healthcare (62) 0.9%
Wholesale Trade (42) 0.9%
Accommodation (721) 0.6%
Construction (23) 0.6%
Real Estate (53) 0.3%

Financial
Espionage
Activism

Server
Network
User
Media
People

Financial (n=458)
Espionage (n=120)

Malware
Hacking
Social
Misuse
Physical
Error
Env
Crossing the Divide
Making it work in your organization

1. Initiate communication between intel & risk teams
2. Orient intel processes & products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines & procedures for risk assessment projects
5. Encourage ongoing coordination & collaboration
   • Create centralized tools/repositories
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**.
SESSION ID: GRC-T09R

Bridging the Gap Between Threat Intelligence and Risk Management

THANK YOU!!

Wade Baker
VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker