Solving CISO Headaches

How to Align CTI and Risk Management

Dr Jamie Collier
Principal Threat Intelligence Advisor

John Doyle
Applied Intelligence Mentorship Program Lead

7th November 2023
Introduction

- CTI and Risk Management have emerged as separate areas. This talk explores how we can bridge the gap.
- Transcending cyber risk-intelligence silos creates more synchronized defense organizations, enabling larger strategic initiatives.
- But, aligning the two is not always an easy task...
Challenges in Risk-Intelligence Integration

1. Role misperceptions
   - CTI often perceived as highly tactical
   - Risk can become detached from network defence

2. Unique lexicons
   - Risk frameworks rarely used in CTI
   - Many CTI processes detached from cyber risk

3. Cultural differences
   - Intelligence overwhelmingly threat-led
   - Different workflows

4. Dedicated career paths
   - Specialist skill sets required for each discipline
Why a CTI Team Benefits

- Build influence with executive audiences.
- Contribute to highly strategic initiatives beyond the security function.
- Make use of existing work and improve visibility of the internal organization.
- Mutual benefit vs. zero-sum game.
Risk and Intelligence: How to Play Nice

1. Build mutual understanding
   A baseline understanding of the other discipline sets the foundation for long-term collaboration.

2. Identify foundational overlap
   Understanding how key CTI products and processes relate to cyber risk will help CTI programs engage risk practitioners.

3. Build collaborative workflows
   Cyber risk and CTI teams can work in tandem to create joint analysis that is collectively informed by each team’s unique perspective.
Build Mutual Understanding

Cyber Risk
- Risk assessments
- Backup strategy
- Continuity of business operations
- Auditing
- Compliance Resilience
- Disaster recovery strategy

Threat Intelligence
- Cyber threat landscape
- Risk calculation
- Vulnerability and patch management
- Threat modelling
- Countermeasures
- IP theft

Attacker techniques
- TTPs
- Hunt teams
- Malware analysis
- Adversary campaigns
- Intrusion sets
- Adversary tradecraft

Compliance Resilience
- Risk assessments
- Auditing
- Compliance Resilience
- Disaster recovery strategy
Secret Sauce vs CTI Fundamentals

Stakeholder analysis vs. Use cases

Intelligence requirements
WHEN CTI ANALYSTS

REALISE THEY'RE NOT THE MAIN CHARACTER
Advice on Engaging with Risk Stakeholders

- Embrace role as an **educator**.
- Start **simple**.
- Focus on what you can **control and manage**.
- Don’t be afraid to **push back**.
Focus on What You Can Control

The shared goal is risk reduction

Threats are an input into overall risk.

Organizations can only control 1 of these variables, but...

A reduction in any of the three drives down overall threat and provides a more scoped focus for risk management decisions.
Each Discipline Has Separate Processes

CTI LOOP

- Plan
- Collect Process
- Share Feedback
- Produce
- Analyze Exploit

RISK LOOP

- Plan
- Monitor Adjust
- Identify
- Respond Mitigate
- Analyze Quantify Prioritize

Proprietary + Confidential
Each Discipline Leverages Separate Mental Models

**Cyber Security and CTI**
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK
- Lockheed Martin's Cyber Kill Chain
- The Mandiant Targeted Attack Lifecycle
- The Unified Cyber Kill Chain

**Factor Analysis of Information Risk (FAIR)**
- Cyber Risk Quantification Model
- Vocabulary for Event Recording and Incident Sharing (VERIS)
- ISF Quantitative Techniques in Information Risk Analysis
- OWASP’s Risk Rating Methodology

**Risk Management**
- NIST Risk Management Framework
- NIST Risk Framework Profiles
Yet Multiple Integration Opportunities Exist

Understand the threats associated with the industry and to the organization, taking informed decisions as appropriate to the risk posed to the organization.
Build Collaborative Workflows

**Threat profile**
CTI team identifies key external threats

**Risk management**
CTI & risk collaborate to determine which threats pose a material risk

**Crown jewels**
Risk teams inform CTI teams about the most critical data and systems

**Threat modelling**
Threat profile informs actions adversaries take to inform modelling & impact analysis

**Countermeasure testing**
Adversary techniques used by risk team to map prevention & detection measures
A cyber threat profile is arguably the most important document for any cyber intelligence program.
# Responsible, Accountable, Consulted and Informed (RACI) Matrix

Clarifies which individuals or groups are responsible for a project’s successful completion, and the roles that each will play throughout the project.

<table>
<thead>
<tr>
<th>ACTIVITY</th>
<th>RESPONSIBLE</th>
<th>ACCOUNTABLE</th>
<th>CONSULTED</th>
<th>INFORMED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and document cyber threat factors</td>
<td>CTI</td>
<td>CTI</td>
<td>IT Leadership</td>
<td>Risk</td>
</tr>
<tr>
<td>Lead cyber risk assessments</td>
<td>Risk</td>
<td>Risk</td>
<td>CTI</td>
<td>IT Leadership</td>
</tr>
<tr>
<td>Develop threat models</td>
<td>IT Security</td>
<td>IT Security</td>
<td>Risk, CTI</td>
<td>IT Leadership</td>
</tr>
<tr>
<td>Validate cyber threats to crown jewels</td>
<td>CTI (or red team)</td>
<td>Risk</td>
<td>Risk</td>
<td>IT Leadership</td>
</tr>
</tbody>
</table>
CASE STUDY

SUPPLY CHAIN RISKS & DEVELOPER ENVIRONMENTS

Building a Software Team from 0
- Exec team wants to understand risks
- Prominent use of open-source tools and software dependencies makes supply chain security a key issue

CTI & Risk Actions
- Provide Supply Chain Risk assessment
- Help identify peer and third party incidents to demonstrate org, sector, regional threat relevance
- Support defense with up-to-date TTPs
- Recommend and build successful resiliency measures
CASE STUDY

SUPPLY CHAIN RISKS & DEVELOPER ENVIRONMENTS

<table>
<thead>
<tr>
<th>SITUATION REQUIRING ASSESSMENT</th>
<th>CTI CONTRIBUTION</th>
<th>SIMPLE RISK ASSESSMENT</th>
<th>CROWN JEWEL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply chain risks associated with developer environments and interest in developing software team</td>
<td>Since 2013 supply chain risks associated with developer environments have grown significantly in both frequency and severity. This includes targeting of both open-source libraries and developer tools across a range of sectors and regions. During this period, threat actors have continually improved their compromise tactics and tools. Typical post-compromise activity includes credential theft and the deployment of cryptominers.</td>
<td>Frequency - Moderate and increasing Severity - High</td>
<td>HIGH PROBABILITY</td>
</tr>
</tbody>
</table>

Recommendations include mitigation steps, for example:

- Utilize SBOM methods to document, understand, and track build components associated with application development.
- Establish a change control process and board for all enterprise hardware and software changes. (E.g. centralized IT or IT security managed process for downloading, testing, and pushing updates out to users.)
- Use an advanced endpoint security solution, such as EDR, to detect malicious behavior if a tainted software package is DLed and executed.
- Security assessments and audits should be an integral part of the software development lifecycle or continuous integration and deployment (CI/CD) pipeline for any internally developed software that is customer facing or integral to internal functions of the organization.
Both cyber risk and CTI operate better together.

The value of what are often siloed and disparate functions multiplies when brought together.

Combining CTI and risk management is easier than you think!

A lot of the work comes down to the foundational elements of CTI (stakeholder analysis, intelligence requirements, and a threat profile).

Combing CTI and risk management increases the relevance and effectiveness of both parts of the organization.

- Better Together: The Benefits of Integrating Cyber Threat Intelligence and Risk Management
Conclusion

Everyone has intrinsic drivers. Identify and leverage them!

Organizational constructs run on KPIs

Share the spotlight, give praise and glory

Feedback drives relationships and outcomes

Champion, advocate, woo, and win hearts and minds to best position ourselves for success
Bonus Ask

bit.ly/ctisurvey23
Get In Touch

JOHN DOYLE
@_John_Doyle
in/john-doyle-a02bab10/

JAMIE COLLIER
@TheCollierJam
in/collierjs

GRACE CHI
@euphoricfall
in/graceschi
grace@pulsedive.com