MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
FIELD GUIDE WHITEPAPER

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

Jamie Collier, Shanyn Ronis, Kelli Vanderlee, John Doyle, Neil Karan, and Andrew Close

# Contents

# Executive Summary

- This paper discusses the mutual benefits of integrating cyber threat intelligence (CTI) and risk management disciplines. This fosters a more synchronized cyber defense posture that has an accurate and timely understanding of relevant threats. In doing so, we provide practical advice on how CTI and risk professionals can engage with each other.
- Several factors can undermine CTI-risk cooperation, including the unique lexicons used in each discipline, misperceptions about the role each team serves, and cultural differences. However, both CTI and cyber risk professionals ultimately strive to reduce cyber risk exposure. This shared mission provides exciting and natural opportunities for collaboration.
- Both CTI and risk management functions are dedicated career paths that require specialist knowledge and skill sets. Collaboration between the two capabilities, therefore, requires both CTI and risk management professionals to possess a baseline understanding of each other's roles, responsibilities, and concepts.
- Common CTI concepts covered in this paper include stakeholder analysis, intelligence requirements, and a cyber threat profile. A threat profile can be used to develop a threat model, which can then be used by risk management teams to determine whether proper cyber security controls are in place to address potential risk exposure.
- Common risk management concepts covered include risk analysis, mitigation processes, and risk registers. In our experience, most CTI practitioners are unaware of these risk management constructs. Building awareness will help to build collaborative workflows informed by each team's unique perspective.
- Transcending cyber risk-intelligence silos not only creates a more synchronized cyber defense organization, but also enables both processes to thrive as they support larger strategic initiatives within an organization.

# Introduction

**Cyber threat intelligence (CTI) and risk management have emerged as two traditionally separate areas to help organizations understand their risk exposure. Often treated as distinct disciplines, there is a growing appetite for coordinating workflows and sharing knowledge between CTI and risk management teams. This enables more focused and aligned efforts to manage cyber risks.**

The overarching goal for both risk practitioners and CTI analysts is to inform the decision-making process within an organization. Both approaches seek to achieve this through providing high-quality insight related to some of the most pressing challenges facing an organization. Risk and CTI teams may approach this challenge from different vantage points, yet their underlying shared mission means there is ample common ground and exciting opportunities for collaboration.

Cyber risk represents one component of overall enterprise risk management and an input to operational risk. It is ultimately designed to help business leaders develop a collective understanding of their organization's risk exposure. Risk professionals bring diverse information together to help leaders understand issues such as their top risks, how business objectives are impacted by external events, and the impact of geopolitical trends on key organizational priorities.

The evolving cyber threat landscape continuously increases the need for high-fidelity and timely data to support an understanding of cyber-related threats and how they may influence risk assessments and ultimately enrich the understanding of organizational risk. As a result, the level of specialist skills within both CTI and cyber risk makes it difficult for individuals to master both disciplines. This is why collaboration between teams is essential.

The overarching goal of this paper is to enable CTI teams and risk practitioners to work more closely to achieve key organizational outcomes. We explore how CTI programs can become informed and active contributors to the cyber risk process through three essential steps.

## Building Intelligence-Risk Collaboration

1

**Build mutual understanding.** CTI professionals do not need to master the topic of cyber risk or vice versa. However, gaining a baseline understanding of the other discipline identifies overlap points and sets the foundation for long-term collaboration.

2

**Identify how foundational elements of CTI can be applied to cyber risk.** Understanding how key CTI products and foundational cyber threat elements relate to cyber risk will help CTI programs engage risk practitioners in a more meaningful manner, allowing them to tailor insights and product delivery based on risk management's intelligence needs. CTI foundational elements include conducting stakeholder analysis, gathering intelligence requirements, and building a threat profile.

3

**Build collaborative workflows.** Once mutual understanding is achieved, cyber risk and CTI teams can work in tandem to create joint analysis that is collectively informed by each team's unique perspective. Examples of this include threat modeling and the development of a responsibility matrix. These concepts are explored in depth below.

# Building Mutual Understanding

To help CTI and cyber risk professionals build mutual understanding, we provide a brief overview of core competencies, methodologies, and approaches for each discipline. This should assist each respective team in identifying collaboration points. The following Venn diagram provides examples of overlaps between the two approaches (Figure 1).

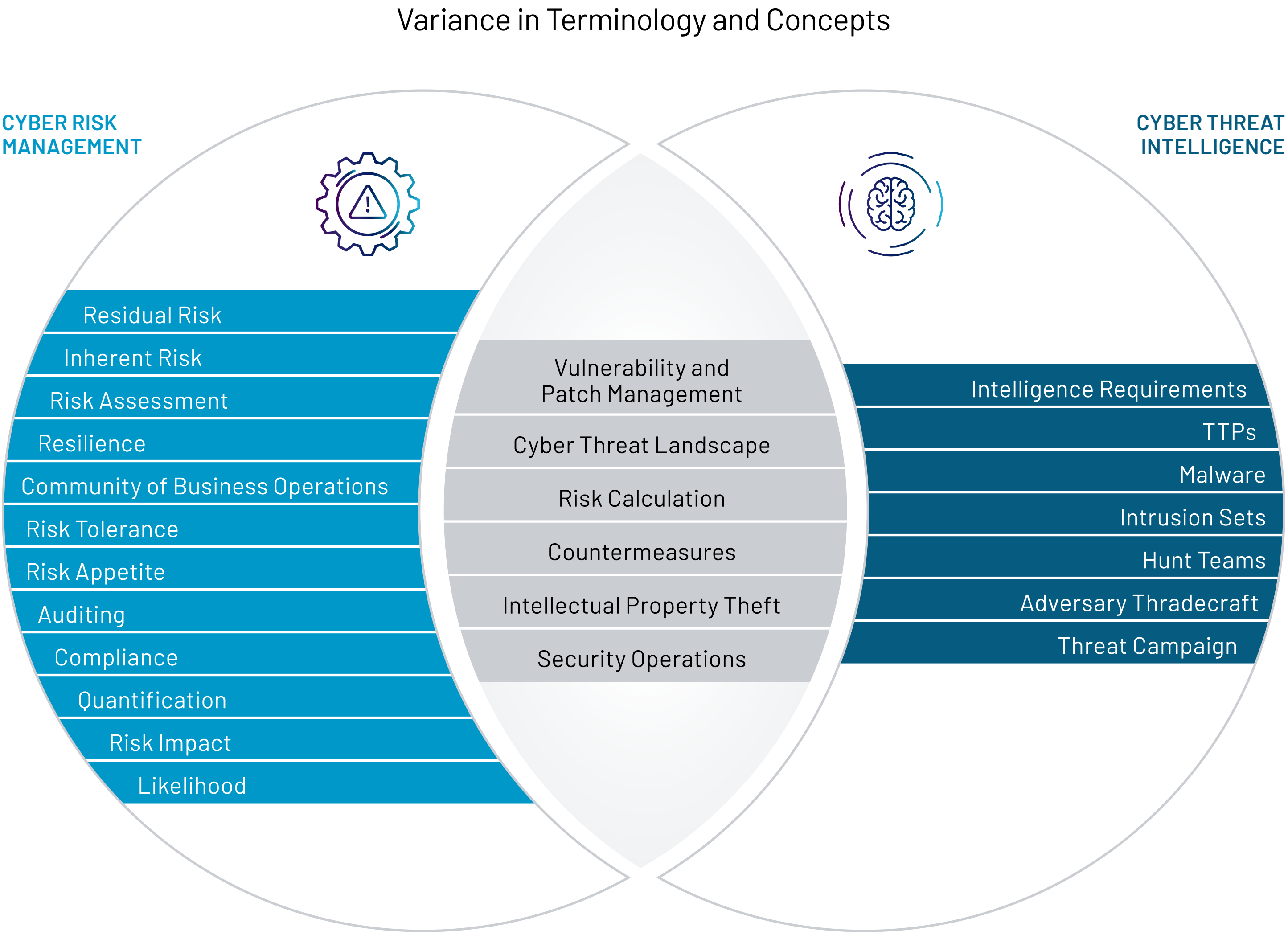


**FIGURE 1.** Overlap and differences within risk management and CTI

# Risk Management Overview for CTI Professionals

Cyber risk is a growing concern for organizations of all sizes. The ever-evolving nature of cyber threats means that organizations must constantly maintain situational awareness to identify relevant changes. By design, Enterprise Risk Management (ERM) helps decision makers create directional strategies in a deliberate and responsible manner that balance systemic uncertainty against organizational priorities. Not dissimilar to threat intelligence, risk management focuses on identifying, assessing, and communicating risks to an organization.

The goal of a cyber risk management program is to support organizational resilience, minimize potential losses, and continue operations in a way that is consistent with an organization's mission, vision, and goals. Cyber risk is a component of operational risk within ERM focused on identifying the likelihood and impact of a cyber incident occurring.  Internal and external decisions can affect this likelihood. For instance, this could include a change in the organization's strategic direction or shifts in the geopolitical climate.

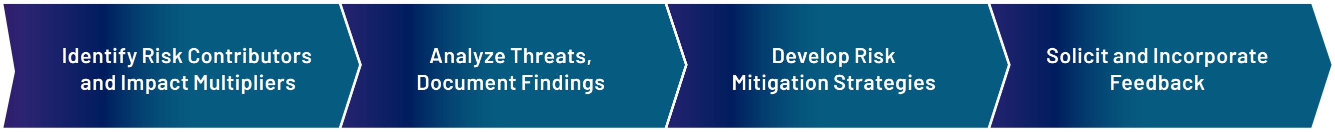

Identify Risk Contributors and Impact Multipliers
Analyze Threats, Document Findings
Develop Risk Mitigation Strategies
Solicit and Incorporate Feedback

**FIGURE 2:** Traditional cyber risk analysis workflow

Modeling organizational threats helps key decision makers identify the impact of potential cyber incidents. Cyber risk analysis therefore seeks to improve decision making around the choice and implementation of safeguards (i.e. cyber security controls) to protect the confidentiality, integrity, and availability of information as it is processed, stored, and transmitted.

As a discipline, cyber risk practitioners use various frameworks and analytical techniques to bring together observational threat data. Similar to CTI, the risk management process can be viewed as an iterative cycle.

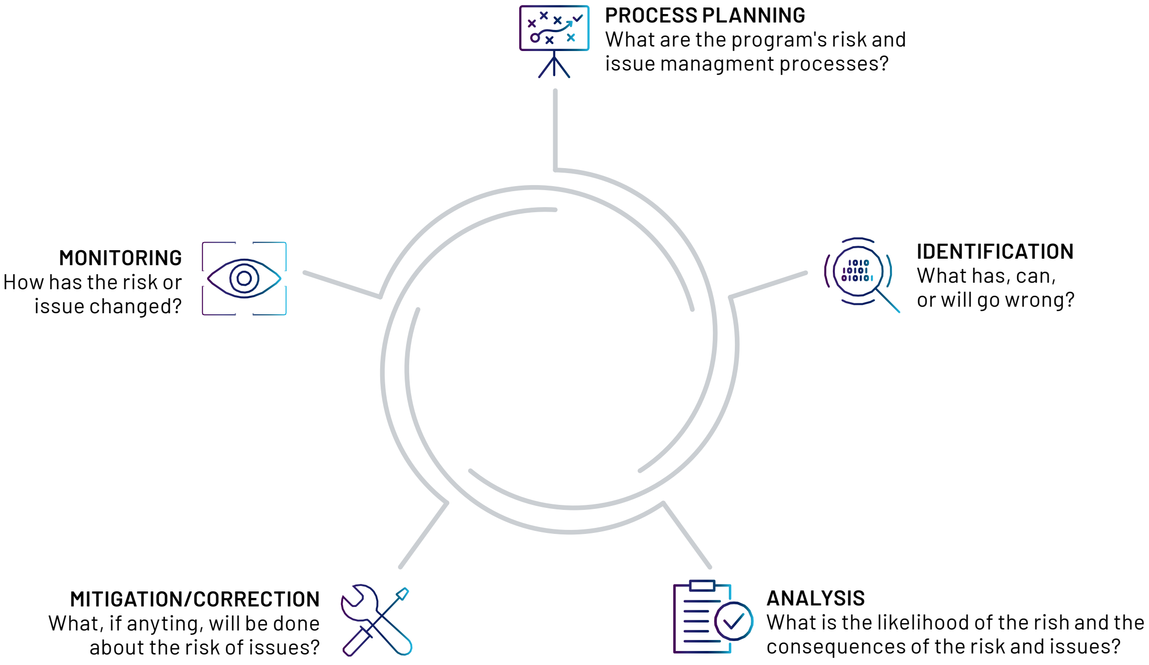

PROCESS PLANNING
What are the program's risk and issue managment processes?
IDENTIFICATION
What has, can, or will go wrong?
ANALYSIS
What is the likelihood of the rish and the consequences of the risk and issues?
MITIGATION/CORRECTION
What, if anyting, will be done about the risk of issues?
MONITORING
How has the risk or issue changed?

**FIGURE 3:** Risk management lifecycle

Organizations can take steps to protect themselves against potential risks, provided they understand the threats they face. To enable the monitoring of risk on a continuous basis, risk teams will typically manage a risk register. This is a repository for all risks identified within an organization. Risk practitioners track risks over time through this register to maintain a dynamic ledger where organization leadership can make informed decisions about how to allocate resources and take steps to mitigate potential threats. A risk register can provide invaluable intelligence about where an organization needs to direct effort to enhance resiliency.

Risk teams provide organizational leaders with the insight required to make informed decisions about how to address risk, often through four avenues:

- Mitigate: Reduce vulnerability through changes to people, processes, or technologies.
- Avoid: Choose to remove exposed risk factors.
- Accept: Acknowledge and document the risk, monitor for potential incidents.
- Transfer: Explore options to shift some responsibility for adverse outcomes through insurance or third-party providers.

**TABLE 1.** Example risk register housed in a GRC system

| Rank | Business Risk | Category | Likelihood | Impact | Inherent Risk | Controls | Residual Risk | Overall Risk | Business Areas |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Data Center Outage | Operational Risk | Possible | Extreme | 15 | Mostly Ineffective | 12 | Very High | • Information Technology<br>• Board Risk<br>• Data Protection<br>• External Audit<br>• Emerging Risk<br>• Earnings |
| 2 | Internet Rates Rise on Variable Debt | Financial Risk | Possible | Major | 12 | None | 12 | Medium | • Board Risk<br>• Treasury<br>• Finance<br>• Legal<br>• Critical Risks |
| 3 | Supplier Risk - Beatsource Components Supply | Operational Risk | Likely | Major | 16 | Mostly Ineffective | 12 |  | • Manufacturing<br>• Earnings<br>• Board Risk |
| 4 | Opportunity - Changing Customer Preferences Leading to a Decrease in Market Size | Strategic Risk | Almost Certain | Major | 20 | Mostly Ineffective | 15 | Low | • Emerging<br>• Board Risk<br>• Emerging Risk |

More recently, organizations have honed their focus by performing asset-centric analysis to identify organizational "crown jewels." This helps an organization understand the impact of cyber threats on key assets. These assessments usually focus on the following high-level categories to group and categorize impact: financial, operational, brand, and regulatory damage.

Several best practice documents issued by the U.S. National Institute of Science and Technology (NIST) on cyber risk topics expand on the areas discussed above in further detail:

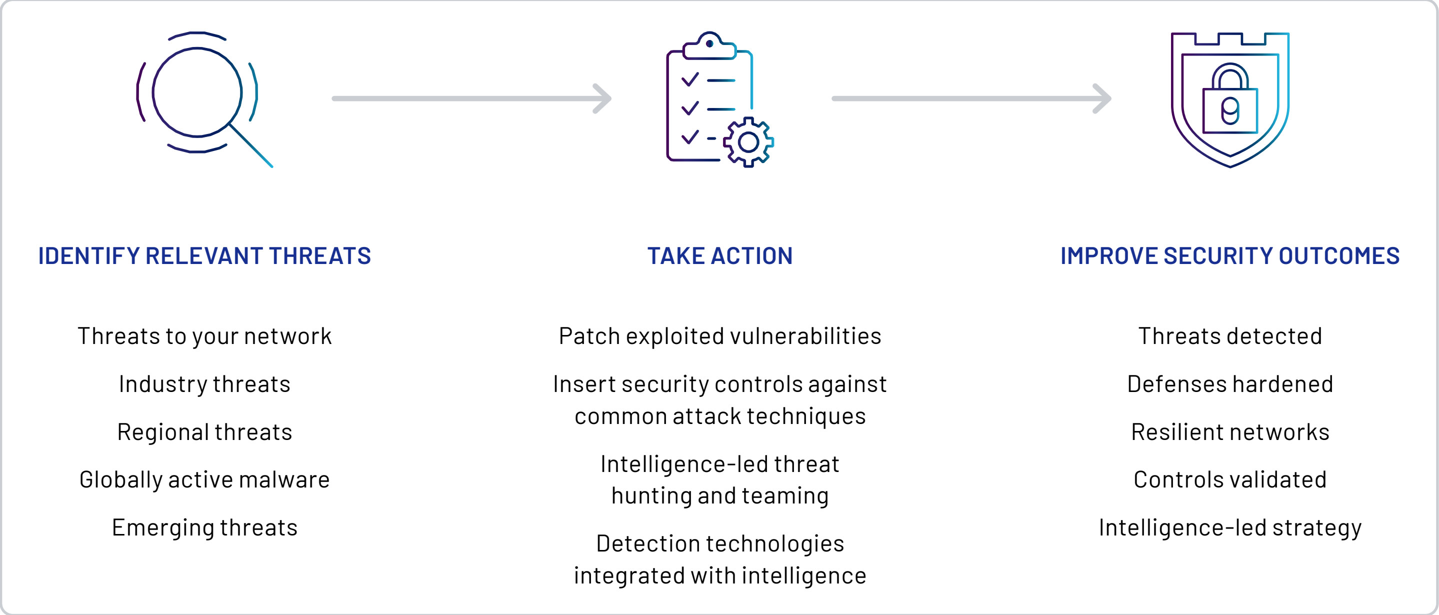
- The NIST Risk Management Framework
- ISO 31000: "Risk Management"
- Special Publication 800-139: "Managing Information Security Risk: Organization, Mission, and Information System View"
- Special Publication 800-30: "Guide for Conducting Risk Assessments"

# CTI Overview for Risk Professionals

CTI provides visibility into current and emerging threats to inform cyber security decisions across people, processes, and technologies. CTI is ultimately used to reduce risk exposure (whether in the form of preventing incidents, improving threat detection efforts, and speeding up response time).

Gartner provides a reasonable definition of CTI as "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."

In short, threat intelligence helps security practitioners to improve security outcomes by taking action on the back of identifying relevant threats.



**IDENTIFY RELEVANT THREATS**

Threats to your network

Industry threats

Regional threats

Globally active malware

Emerging threats

**TAKE ACTION**

Patch exploited vulnerabilities

Insert security controls against common attack techniques

Intelligence-led threat hunting and teaming

Detection technologies integrated with intelligence

**IMPROVE SECURITY OUTCOMES**

Threats detected

Defenses hardened

Resilient networks

Controls validated

Intelligence-led strategy

**FIGURE 4:** How understanding threats can drive improved security outcomes

CTI teams work with a range of internal stakeholders to identify their needs in the form of intelligence requirements. These guide CTI focus areas, whether that be data collected, the types of intelligence products developed, or the topics addressed.

CTI analysts are also often tasked with developing highly strategic products that support business decisions and contain clear overlap with cyber risk. For example, country and industry threat profiles outline the key threats associated with operating in a particular geography or industry. This would be a product that could actively inform various risk assessments, for example, a review into the key risks of entering into a new market.

CTI teams are therefore a supporting function and often work closely with various strategic customers such as boards, the C-suite, and risk management functions. CTI helps these stakeholders understand the level of threat exposure that exists and where to focus efforts within a security function. CTI also enables cyber defense functions to quickly identify, detect, and contextualize cyber incidents that occur.

TABLE 2. The value of CTI across different security roles

| Audience | Strategic | Operational | Tactical |
|---|---|---|---|
| **Security Roles** | • Chief Executive Officer<br>• Chief Information Security Officer<br>• Security Management<br>• Risk Management | • Incident Response Team<br>• Forensics Team<br>• Red Team/Pen Testing<br>• Purple Team | • Security Operations Center<br>• Network Operations Center<br>• Vulnerability Management Team |
| **Tasks** | • Allocate resources<br>• Communicate with executives | • Determine attack vectors<br>• Remediate<br>• Hunt for breaches | • Indicators to security tools<br>• Patch systems<br>• Monitor, escalate alerts (triage) |
| **Problems** | • No clear investment priorities<br>• Executives are not technical | • Event reconstruction resource intensive<br>• Difficult to identify damage | • False positives<br>• Difficult to prioritize patches<br>• Alert overload |
| **Value of CTI** | • Demystify threats<br>• Prioritize based on business risk | • Add context to reconstruction<br>• Focus in on potential targets | • Validate and prioritize indicators<br>• Prioritize patches<br>• Prioritize alerts |

CTI teams adapt their communication style (i.e. medium, lexicon, message, and production cadence) based on their audience. This can range from strategic, executive-level staff to highly technical practitioners (such as detection engineers and security architects).

Regardless of the stakeholder, CTI strives to convey what are often complex messages in a straightforward and accessible manner well-aligned to its intended audience. Examples of CTI products include:

- Developing adversary playbooks and hunt guides using MITRE ATT&CK mapping.
- Illustrating organizational threat models within a Cyber Threat Profile. This would often involve integrating with other frameworks including Factor Analysis of Information Risk (FAIR) or Vocabulary for Event Recording and Incident Sharing (VERIS).
- Visualizing overlap across an adversary's tools, infrastructures, personas, and suspected affiliation through link analysis tools such as Maltego or MISP.
- Fostering understanding between CTI and cyber risk teams is essential for collaboration. Once each team understands the other's roles and responsibilities, it becomes much easier for a cyber risk practice to be served as an intelligence stakeholder.

# Applying Foundational Elements of CTI to Cyber Risk

Any successful CTI program should actively identify relevant stakeholders in their organization, gather their intelligence requirements, and have a cyber threat profile in place to aid these discussions. These steps set up an intelligence function for long-term, sustainable success.

Having these foundations in place is essential for any CTI function planning to engage with risk management teams. Using an ad hoc or piecemeal approach to these foundational CTI elements can quickly undermine the credibility and utility of CTI among risk management teams, especially given the importance of repeatable and reliable measurements in risk assessments.

## Stakeholder Analysis and Gathering Intelligence Requirements

Intelligence programs will add value to cyber risk processes by identifying the teams involved in risk management, understanding their challenges, and building intelligence requirements to address these challenges. Engaging cyber risk practitioners will also provide an opportunity to raise awareness on the different ways intelligence can potentially support risk analysis. All this makes both conducting stakeholder analysis and gathering intelligence requirements essential.

Cyber risk can comprise a variety of definitions, frameworks, and processes. As such, there is no one right way for an organization to conduct cyber risk assessments. Understanding cyber risk stakeholders and their requirements will therefore help an intelligence function to better understand the specific way that cyber risk management is approached within their organization.

Practical advice on both conducting stakeholder analysis and gathering intelligence requirements can be found in our previous whitepaper, A Requirements Driven Approach to Cyber Threat Intelligence.

## Building a Cyber Threat Profile

A cyber threat profile leverages CTI to produce a holistic view of the external cyber threats relevant to a specific organization. It is a critical component of developing an intelligence-led approach to cyber risk by providing the key data needed to properly scope, prioritize, and describe cyber threats.

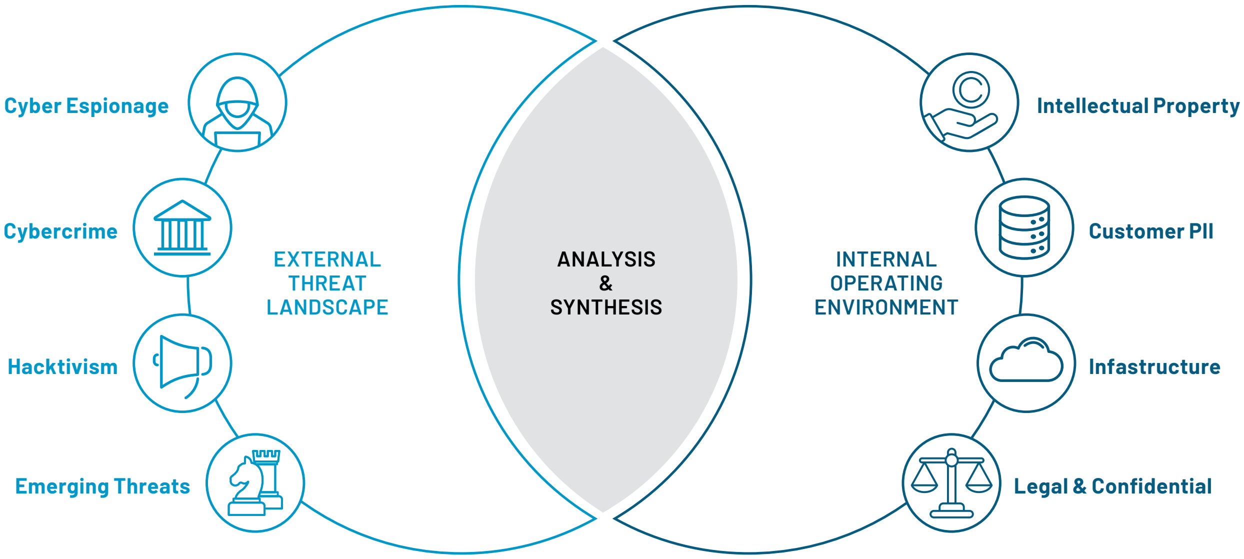
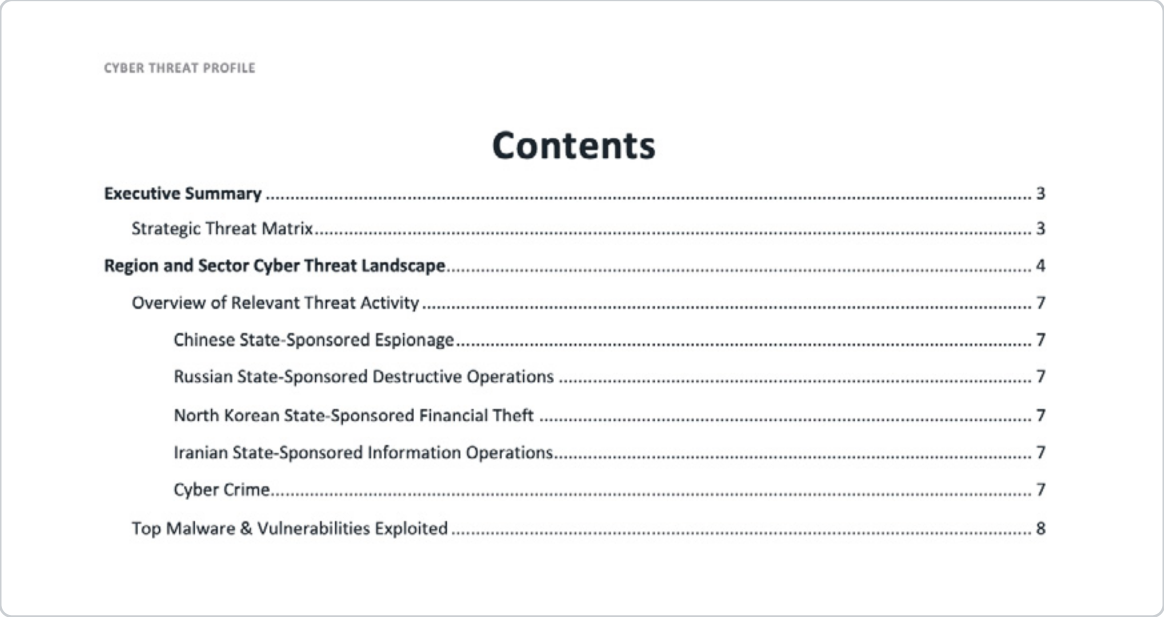


**FIGURE 5:** Cyber threat profile components

A cyber threat profile combines the externally facing threat landscape with a more introspective review of an organization's internal operating environment (i.e. their people, processes, and technology). Once the pool of all cyber threats is narrowed down to those who have probable reasoning and motivation, a high-level dossier is created on recent operations as well as the tactics, techniques, and procedures (TTPs) used by relevant threat actors.

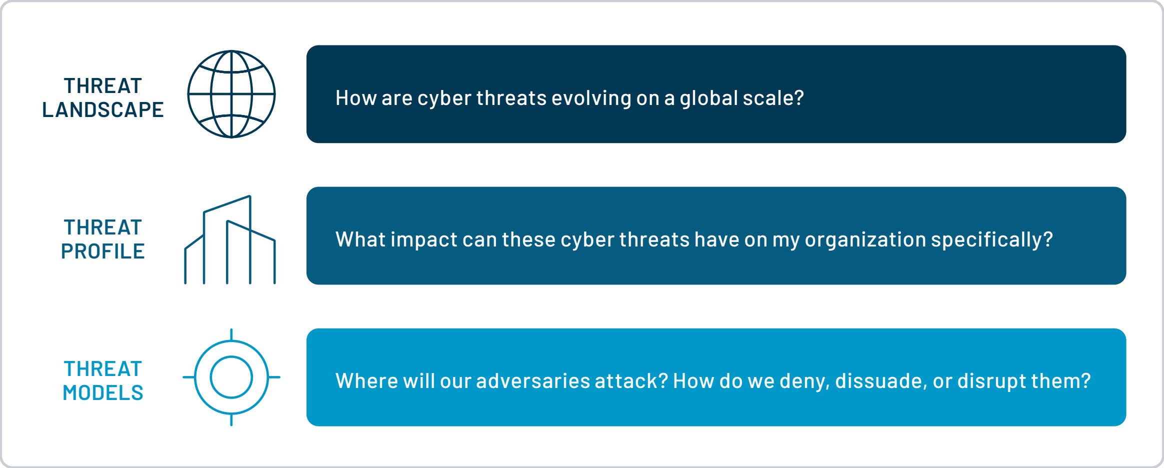


CYBER THREAT PROFILE

Contents

**FIGURE 6:** Example threat profile structure

Beyond being a key reference point for intelligence analysts, a threat profile can also serve as a catalyst for a series of cascading activities that help organizations measure and mitigate cyber risk. This creates clear impetus for cyber risk and CTI teams to work together.



THREAT LANDSCAPE

How are cyber threats evolving on a global scale?

THREAT PROFILE

What impact can these cyber threats have on my organization specifically?

THREAT MODELS

Where will our adversaries attack? How do we deny, dissuade, or disrupt them?

**FIGURE 7:** A threat profile drives additional activities, including threat modeling

# Building Collaborative Workflows Between Cyber Risk and Threat Intelligence

The overlapping perspective on threats shared between the CTI team and teams managing cyber risk provides a range of collaboration opportunities. Once CTI professionals understand the core principles of cyber risk management and how intelligence products can assist, they are in a much stronger position to work together.

Partnership between risk and CTI teams can play out in various ways and can depend on an organization's unique context. Typical examples of collaboration include crown jewel asset mapping, threat modeling, and feeding threat data into risk matrices.

## Threat Modeling

Threat modeling represents one of the most obvious and fruitful collaborative opportunities between CTI and risk management teams. It is the practice of evaluating organizational security controls to reveal unknown risks and vulnerabilities within systems. Threat modeling provides insight into the types of cyber threat actors an organization faces and their potential impacts. It is also a  key part of several frameworks including FAIR or VERIS.

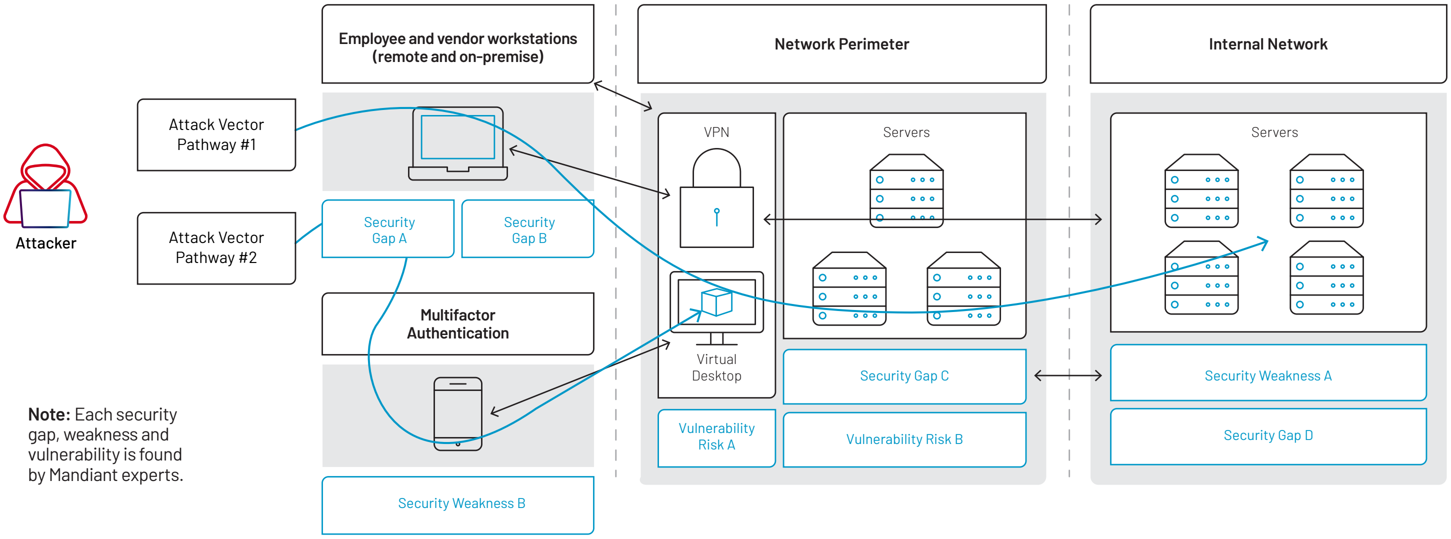
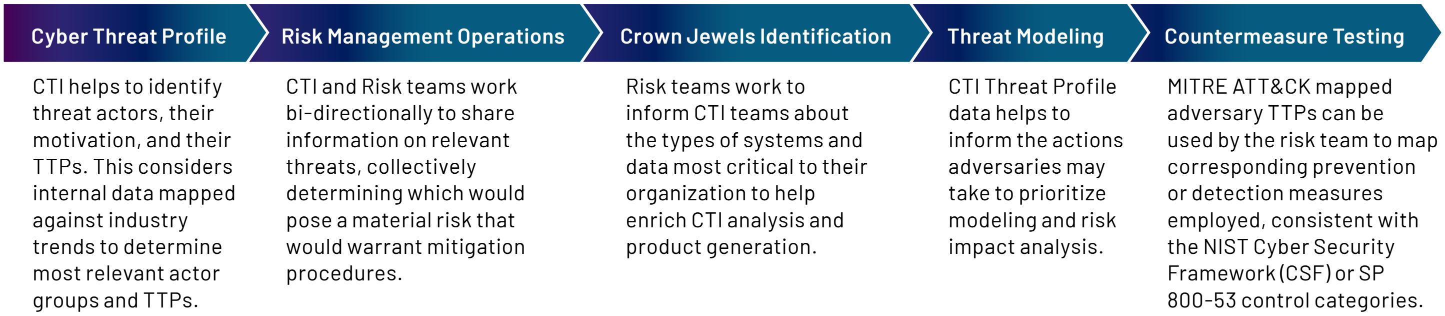


**FIGURE 8:** Example threat modeling depiction

Collaborative threat modeling often starts with a cyber threat profile as this contains details on an adversary's modus operandi. This insight helps to assess the validity and likelihood of a cyber event. This goes further than just considering a given threat's likelihood and impact and considers variables including attack initiation and sophistication.

Figure 10 outlines one way a cyber threat profile could  instigate an integrated workflow alongside risk practitioners.



**Cyber Threat Profile**

CTI helps to identify threat actors, their motivation, and their TTPs. This considers internal data mapped against industry trends to determine most relevant actor groups and TTPs.

**Risk Management Operations**

CTI and Risk teams work bi-directionally to share information on relevant threats, collectively determining which would pose a material risk that would warrant mitigation procedures.

**Crown Jewels Identification**

Risk teams work to inform CTI teams about the types of systems and data most critical to their organization to help enrich CTI analysis and product generation.

**Threat Modeling**

CTI Threat Profile data helps to inform the actions adversaries may take to prioritize modeling and risk impact analysis.

**Countermeasure Testing**

MITRE ATT&CK mapped adversary TTPs can be used by the risk team to map corresponding prevention or detection measures employed, consistent with the NIST Cyber Security Framework (CSF) or SP 800-53 control categories.

**FIGURE 9:** Collaborative workflows between risk management and CTI

## Develop a Combined Intelligence-Risk Responsibility Assignment Matrix

A responsibility assignment (RACI) matrix documents responsibility and accountability within an organization. It outlines different business activities and documents who is responsible for them, the personnel accountable, and other stakeholders that need to be consulted or informed.

An intelligence-risk RACI matrix clarifies the involvement and ownership of different risk-related issues within an organization. Given the vast potential overlap between the two functions, building a RACI matrix represents a positive opportunity to streamline and enhance the effectiveness around process integration by clarifying roles.

**TABLE 3.** An example of an intelligence-risk RACI matrix

| Activity | Responsible | Accountable | Consulted | Informed |
|---|---|---|---|---|
| Identify and document cyber threat factors | CTI | CTI | IT leadership | Risk |
| Lead cyber risk assessments | Risk | Risk | CTI | IT leadership |
| Develop threat models | IT security | IT security | Risk and CTI | IT leadership |
| Validate cyber threats to crown jewels | CTI or red team | Risk | Risk | IT leadership |

# Cyber Risk Informed by CTI

> Once a CTI and cyber risk team have built mutual understanding on how their two approaches can be combined, a collaborative framework can be applied to a variety of cyber security challenges.

Given that so much of CTI-cyber risk collaboration is dependent on the specific risk frameworks and context of a particular organization, there is no one correct way to implement this. Rather than prescribe a formalized and rigid approach to collaboration, we outline several case studies below. These are intended to serve as inspiration and highlight the range of opportunities available. Organizations can then adapt and amend this underlying collaborative approach in ways that suit their own unique context.

## Case Study One: Assessing the Risk of a 'High Severity' Vulnerability

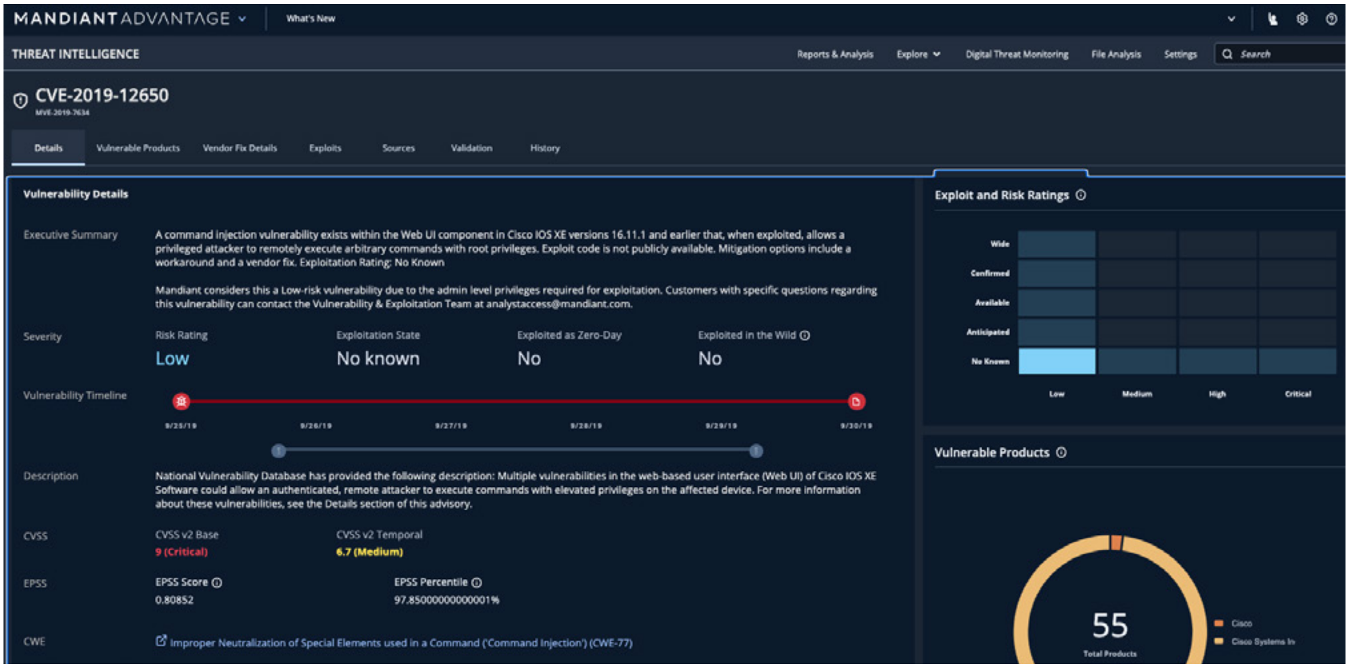
Vulnerability management represents one of the most fruitful yet underutilized opportunities to combine cyber risk and CTI perspectives. Traditional approaches to vulnerability management have typically focused on vulnerability severity—i.e. the impact of a vulnerability on an organization if it were to be exploited.  This is a useful metric but lacks context on its own.

With its connection to the threat landscape, CTI can complement this approach by also informing vulnerability management stakeholders on an equally important metric: vulnerability exploitability. Vulnerability exploitability refers to both how easy a vulnerability is to exploit and whether it has actually been exploited. This helps network defenders to determine the likelihood of a vulnerability being exploited in the future.

### Case Study Context

Cisco has released 13 bugs and corresponding patches. A CTI team can use external data sources to contextualize the severity of the vulnerabilities. In this case, we are using Mandiant Advantage's system, which provides both a description of the vulnerability and the potential for an adversary to exploit it. Exploitation activity could be further graded and contextualized by examining how relevant an exploit is to an organization or its crown jewels.

Here, we can see that it is characterized as a remote code execution vulnerability, which could allow an adversary to execute arbitrary commands with root privileges. Although this would merit a high severity rating inw isolation, the privileges required to exploit CVE-2019-12650 alongside the lack of exploitation in the wild mean that its overall risk is low.



CVE-2019-12650
MVE-2019-7634

Vulnerability Details

Executive Summary: A command injection vulnerability exists within the Web UI component in Cisco IOS XE versions 16.11.1 and earlier that, when exploited, allows a privileged attacker to remotely execute arbitrary commands with root privileges. Exploit code is not publicly available. Mitigation options include a workaround and a vendor fix. Exploitation Rating: No Known

Mandiant considers this a Low-risk vulnerability due to the admin level privileges required for exploitation. Customers with specific questions regarding this vulnerability can contact the Vulnerability & Exploitation Team at analystaccess@mandiant.com.

Severity: Risk Rating: Low; Exploitation State: No known; Exploited as Zero-Day: No; Exploited in the Wild: No

Vulnerability Timeline

Description: National Vulnerability Database has provided the following description: Multiple vulnerabilities in the web-based user interface (Web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands with elevated privileges on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.

CVSS: CVSS v2 Base: 9 (Critical); CVSS v2 Temporal: 6.7 (Medium)

EPSS: EPSS Score: 0.80852; EPSS Percentile: 97.850000000000001%

CWE: Improper Neutralization of Special Elements used in a Command ('Command Injection') (CWE-77)

**FIGURE 10:** CVE-2019-12650 threat intelligence available in the Mandiant Advantage portal

The CTI team can provide inputs to the risk management team through various means. One example of this would be a joint template like the one below.

**TABLE 4:** Example CTI-risk joint assessment template

| Situation Requiring Assessment | CTI Contribution | Simple Risk Assessment | Crown Jewel Impact |
|---|---|---|---|
| A command injection vulnerability exists in the Web UI component of Cisco IOS XE versions 16.11.1 and earlier that, when exploited, allows a privileged attacker to remotely execute arbitrary commands with root privileges (CVE-2019-12650). NVD rated this vulnerability to be "high" risk. | Mandiant rated it as low risk because it requires the highest level of privileges—level 15 admin privileges—to exploit. Because this level of access should be quite limited in enterprise environments, we believe that it is unlikely attackers would be able to leverage this vulnerability as easily as others. There is no known exploitation of this activity. | • Frequency = No known; future exploitation unlikely<br>• Severity = High | No |
| Recommended risk management strategies: Mitigate the risk through patching, and accept the risk until the patch is implemented. The patching schedule likely does not need to be accelerated in this case given low likelihood of exploitation. | | | |

## Case Study Two: Executive Leadership Consider Supply Chain Risks Associated with Developer Environments

An alternative case where CTI teams and risk professionals might collaborate is around strategic decision making. This could apply to a range of contexts such as the risks associated with entering a new market, proceeding with a digital transformation project, or collaboration with third parties.

### Case Study Context

An organization is planning to build a large software development team from scratch. Before they go ahead, the executive leadership team first wants to understand any associated risks. The prominent use of open-source tools and software dependencies in developer environments makes supply chain security a key issue in understanding relevant risks.

CTI and Risk professionals can contribute to supply chain risk assessments in the following ways:

- Provide an assessment of the current supply chain threats posed to an organization.
- Assist security teams in identifying incidents affecting peers and third-party providers to demonstrate the relevance of threats to their organization, sector, and region.
- Support ongoing defensive efforts by providing up-to-date information about the TTPs associated with supply chain compromise and the targeting of developer environments and the range of potential post-compromise scenarios.
- Assist in building resiliency measures, by identifying strategies that have been successful for other organizations.

A CTI team can contribute to broader risk assessments by producing intelligence related to historical incidents of supply chain compromise, developer tools, and software dependencies.

Based on Mandiant's own analysis, 2021 was the first time we identified more supply chain compromises involving developer tools or software dependencies (T1195.001) than compromises affecting final software products (T1195.002).

These incidents frequently involved resources from open-source or collaborative communities, such as libraries and other code packages from PyPI or npm, Docker virtualization images, and WordPress plugins and themes.

Many of these open-source tools are used extensively across a range of sectors and regions, meaning that a successful supply chain compromise incident can be far-reaching. This was showcased by the critical Log4shell vulnerability (CVE-2021-44228) in the widely used logging tool Log4j, which was exploited by a variety of threat actors and targeted a variety of technologies that had incorporated Log4j.

Frequent post-compromise activity related to supply chain compromise of developer environments included credential theft, collecting codesigning certificates, and deploying coin miners. We also noted examples of actors abusing open-source repositories to spread protest messages.

Using the same template as above, both the CTI team and risk team can fill in their respective portions.

**TABLE 5:** Example CTI-risk joint assessment template

| Situation Requiring Assessment | CTI Contribution | Simple Risk Assessment | Crown Jewel Impact |
|---|---|---|---|
| Supply chain risks associated with developer environments | 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. | • Frequency = Moderate and increasing<br>• Severity = High | High Probability |

Recommended risk management strategies include mitigation steps, for example:

- Utilize Software Bill of Materials (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. This could include a centralized IT or IT security managed process for downloading, testing, and pushing updates out to users.
- Use an advanced endpoint security solution, such as an endpoint detection and response, to detect malicious behavior if a tainted software package is downloaded 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.

## Case Study Three: Executive Leadership Consider Transferring Ransomware Risk via Insurance

CTI can also play an equally important role in helping a cyber risk team understand the implications of how they address risk—i.e. whether a risk is mitigated, avoided, accepted, or transferred.

### Case Study Context

An executive leadership team is considering insurance policies as a means to transfer the risk of a potential ransomware attack against their organization.

In the event of a ransomware deployment, cyber insurance can theoretically facilitate the release of funds for recovery efforts, ransom payment, and/or legal fees, subject to the policy terms and legality of extortion payments within a given jurisdiction.

However, ransomware insurance policies should ideally only represent one component of an organization's ransomware risk management strategy. Rather than being the primary strategy for dealing with ransomware risk, it should be viewed as a last resort mechanism in the event of a worst-case scenario occurring.

The ideal outcome (to reduce both cost and business impact) is for organizations to avoid a ransomware incident altogether through improving defenses and detecting and containing an initial compromise before data is stolen or ransomware encryption is deployed. Here, CTI and risk teams can make several contributions in building ransomware risk assessments that ultimately lead to more effective security strategies.

CTI and risk teams can contribute to ransomware risk assessments in the following ways:

- Provide an assessment of the current ransomware threat posed to an organization.
- Assist security teams in identifying incidents affecting peers and third-party providers to demonstrate the relevance of threats to their organization, sector, and region.
- Support ongoing defensive efforts by providing up to date information about the TTPs ransomware operators are employing to gain initial access to victim networks, as well as the range of potential post-compromise scenarios.
- Assist in building resiliency measures, by identifying strategies that have been successful for other organizations. This could include using offsite backups, conducting tabletop exercises, and planning for how to respond to intrusions taking place out of traditional working hours.[1]

Using the same template as above, both the CTI team and risk team can fill in their respective portions.

**TABLE 6:** Example CTI-risk joint assessment template

| Situation Requiring Assessment | CTI Contribution | Simple Risk Assessment | Crown Jewel Impact |
|---|---|---|---|
| Ransomware and multifaceted extortion | Since 2017 ransomware operations have grown significantly in both frequency and severity. Observed ransomware operations have affected both small and large organizations in nearly every sector and region. During this time, threat actors have continually improved their compromise tactics and tools as well as strategies for increasing leverage against victims. | • Frequency = High<br>• Severity = High | High Probability |
| Recommended risk management strategies:<br>• Mitigate the organization's vulnerability to ransomware TTPs, including initial infection vectors and malware or pivoting tactics that frequently precede data theft and ransomware encryption deployment.<br>• Institute and test backup and after hours incident response plans to enhance the organization's resiliency in the event of a compromise.<br>• Explore cyber insurance options for transferring some risk. | | | |

As the case studies above have shown, CTI can make a significant contribution across a range of risk management use cases. This highlights the opportunity to leverage  CTI as organizations build comprehensive mitigation and risk management strategies.

[1] For comprehensive recommendations for addressing ransomware, please refer to our blog: Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment and the linked white paper.

# Conclusion

Both cyber risk and CTI confer benefits to organizations independently. Yet the value of what are often siloed and disparate functions multiplies when brought together. An approach to cyber risk deeply connected to developments in the threat landscape enables decision makers to adopt a genuinely evidence-led approach to confronting their most pressing and complex challenges.

When combined, risk assessment frameworks and CTI empower decisionmakers to consider and triage new threats or challenges more efficiently and accurately. The language and logic of risk assessments help security staff to communicate the potential danger associated with a threat development or a business decision in terms that business owners and executives understand.

Based on a risk assessment, stakeholders across an organization can suggest strategies for mitigating, avoiding, accepting, and/or transferring risk and assist business owners to make well-informed plans for the organization's future success.

Cyber risk and CTI are both growing fields and ones that increasingly require specialist skills. This means cyber risk and CTI professionals can understandably feel detached from each other's process. Yet, it is not necessary for each discipline to master the other's skills and knowledge base in order to engage. Instead, as this paper has demonstrated, there are plenty and fruitful opportunities for an intelligence function to become a meaningful contributor to cyber risk.

# Mandiant Cyber Risk Services

Mandiant offers a range of services to help organizations pinpoint the cyber risks that are relevant to your specific organization and understand the potential harm they pose against your business. Advance your business approach to cyber risk management for effective decision-making and risk mitigation.

**Services include:**

- Intelligence Capability Development: Build best practices for the consumption, analysis and practical application of CTI.
- Crown Jewels Security Assessment: Identify, protect and defend your most critical business assets from harmful compromise.
- Threat Modeling Security Service: Discover unidentified business and security risks through effective, dynamic system analysis.
- Cyber Risk Management Operations Service: Identify and manage relevant cyber risks to enable effective, risk-based decision making.
- Cyber Security Program Assessment: Evaluate your security program to prioritize investments, increase resiliency and reduce risk.
- Threat and Vulnerability Management: Improve and stabilize your vulnerability management processes with proven risk-based security strategies.
- Cyber Security Due Diligence Service: Realize and mitigate inherited cyber risks associated with business transactions, relationships and systems out of direct control.

## Mandiant Threat Intelligence

Mandiant Threat Intelligence gives security practitioners unparalleled visibility and expertise into threats that matter to their business right now. This can be applied to CTI-cyber risk collaboration across a range of use cases.

Our threat intelligence is compiled by over 500 threat intelligence analysts across 30 countries, researching actors via undercover adversarial pursuits, incident forensics, malicious infrastructure reconstructions and actor identification processes that comprise the deep knowledge embedded in the Mandiant Intel Grid. Threat Intelligence can be delivered as a technology, operated side-by-side with your team, or fully managed by Mandiant experts.

**Mandiant**
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

**About Mandiant**
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.
GRAF-2131