Translating Intelligence for the Business

Tiernan Connolly

3 Traditional Tracts of Threat Intel

Strategic Intelligence:

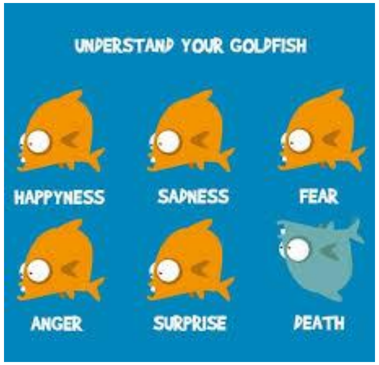
Educate ; create a continued awareness ; enable senior management to make key decisions around business strategy and investments

***Audience:** C-Suite, Board, all levels of management*

Tactical Intelligence

Contextualised , tailored intel to improve resilience, défenses, governance, incident response etc

***Audience**: IR/SOC, CISO, InfoSec Mgt, cyber teams*



Operational Intelligence:

Technical data for detection & prevention (i.e. monitoring)

***Audience:** automated technical feeds, cybersecurity teams*

Frameworking It

Intel Tract	Outputs	Audience	Value
Tactical and Strategic	• Strategic threat reports • Situational awareness updates • Trending & analytics • Business-focused cyber risk contextualisation • Campaign, threat, incident analysis/assessments • Threat actor/group profiles	• *C-Suite* • *Board* • *CISO/CIO* • *InfoSec Mgt* • *Business Mgt* • *ITSec teams*	• *Cyber threats with business perspective e.g. in context of regulatory risks* • *Tailored reports*
Holistic / Program	• Development of a Threat Intel program • Improvement or maturation of existing program • Co-sourcing options for on-site support • Threat Landscape Assessments • Cyber Economics / Business alignment	• *Holistic* • *InfoSec functions*	• *Function guided by an understanding of environment, critical assets and threat landscape*
Operational	• Technical data for detection and prevention (i.e. monitoring systems) • Indicators of Compromise (IOCs) - attributes cross-correlated with other IOCs • Malware/attacks/vuln signatures & patterns • Malicious IP addresses/domain blacklists	• *Monitoring appliances* • *Aggregator (SIEM)* • *IR / SOC* • *Vuln Mgt*	• *Sifting, analysis, cross-correlation and enrichment of technical intel from multiple prominent intel vendors*

←Improve→

←Assess→

←Build→

←Operate→

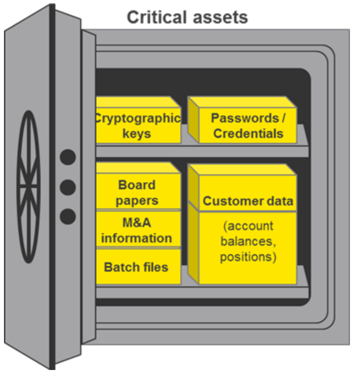
Binding the priorities and actions of the SOC, CISO and executives

1

What is unique to your business?
What is of most interest to adversaries?

How may they want to hurt you?

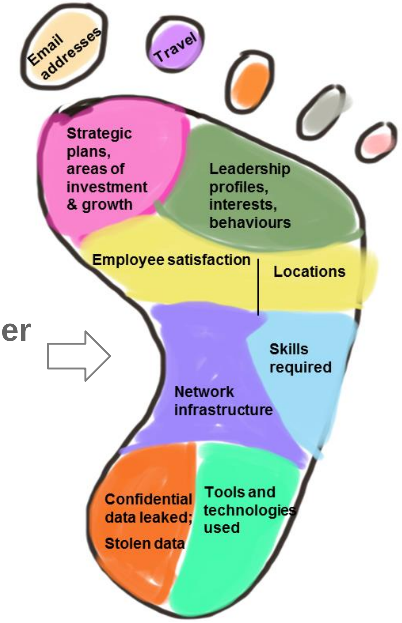
Define the business strategy/priorities



2

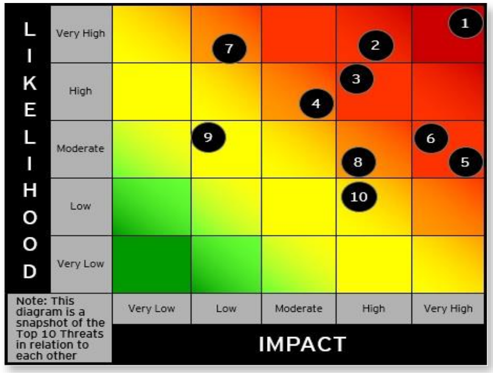
How are you helping them target you?

Understand Cyber Footprint


Email addresses
Travel
Strategic plans, areas of investment & growth
Leadership profiles, interests, behaviours
Employee satisfaction
Locations
Skills required
Network infrastructure
Confidential data leaked;
Stolen data
Tools and technologies used

3

Threat Landscape

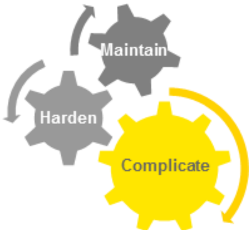


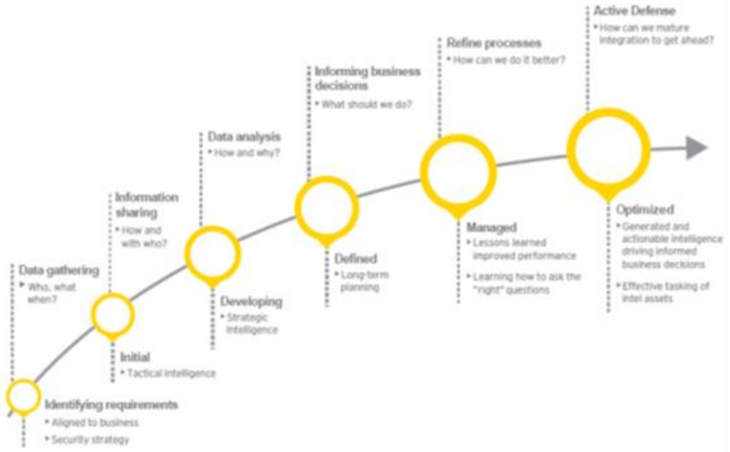
How are the attackers most likely to be successful (threat scenarios)?

What impact will this have on the organisation's strategy, value, customers?

4

What are the appropriate priorities and countermeasures to put in place?





5

Longer term a programme build integrates TI from top to bottom in a virtuous cycle

Common CTI Values & Benefits

Cyber threat intelligence can help **security operators** answer questions like:

- Is our team/technologies equipped to identify the threat early in the adversary life cycle?
- Is our team/technologies mature enough to integrate threat intelligence?
- What are the tactics, techniques, and procedures of current threat actors?
- How can we take threat data and incorporate it into security operations and technologies to get ahead of the threat?

? GREY AREA ?

Cyber threat intelligence can help **decision makers** answer questions like:

- What cyber threats target my industry? My business? And how is this relevant to me?
- Is my business taking these into account for strategy, planning, operations etc.?
- What is the risk of inaction?
- How should I prioritize security solutions, countermeasures, and resource planning?
- How can I show the effectiveness of measures my business has put/will put into place?
- How can we better manage vulnerabilities?

Converting Grey to Gold

Use CTI to carve out a direct channel to the most important people in your organization

educate *influence*

- What threats target my industry/business (awareness)? How is this relevant to me?
- How is the InfoSec/Cyber function protecting me from these threats (marketing)?
- What programs and initiatives need support/money (CISO Agenda/budget)?
- What bad things could happen if I don't support InfoSec/Cyber function (value-teaching/propaganda)?
- How we can all work together to protect the organization (collaboration)?

Value

Impact

Awareness

Agenda

Support

Example Business-Focused Products

Products/ reports	Description	Audience
Monthly Bulletins	Business-focused thought-leadership-style briefing looking at recent cybersecurity issues, emerging trends and relevant events, contextualising them in relation to clients and their industries - to create awareness and educate management on relevant risks and their repercussions in a non-technical, risk-orientated, language	• *C-Suite* • *Board* • *InfoSec Mgt* • *Business Mgt* • *Op/Tech Risk functions* • *Key ITSec teams / individuals* • *Corporate Security*
Trend/Event Analysis Reports	A retrospective in-depth analysis of malware, internal data over time, a large incident, threat, or trend. Presented to clients in case-study style reports.	
Event Updates (non-technical)	Timely (POV style) situational awareness reports on recent significant events, issues, trends (e.g. a large data breach), advising your function can/does react and protect (in light of the, or to similar, attacks or breaches)	
Daily cybersecurity News Digest	Daily roundup of client/industry-relevant cybersecurity stories selected from a wide range of sources/feeds, presenting in a style that allows for quick and easy consumption, helping maintain their 'situational awareness' of current events and issues.	
Event/Threat Updates (technical)	Timely, event-driven situational awareness reports on recent significant events, issues, trends - e.g. campaign, threat and incident analysis/assessments, Threat actor/group profiles - including IOCs where necessary	• *InfoSec Mgt* ○ *Business Mgt* ○ *Corp Sec* ○ *SOC/IR* ○ *Vuln Mgt*
Flash Updates	Very brief updates conveying time-sensitive information about highly specific/relevant threats to clients (typically followed up with larger, more in-depth, Threat Updates.	
Country Risk Profiles	Country-specific reports detailing information security and cyber risk levels and threats, travel advice etc (this could be created in conjunction with other internal teams e.g. Risk Management).	• *Various* • *InfoSec Mgt* • *Business Mgt* • *Corp sec*
Bespoke Intelligence Requests	Tailored intelligence/analysis carried out on request e.g. RFIs, target/problem profiles, strategic/tactical/risk assessments.	• *Request-specific*

How-To Summary

- Establish and sustain a capability to obtain a business-orientated understanding of relevant Cyber Security threats, trends, security concepts (i.e. attackers, techniques and motivations), mitigations and controls.
- Use and showcase your security function's unique insight and access to knowledge and intelligence from peers, vendors, industry and government sources.
- Develop products (i.e. reports) that translate and contextualise tactical and strategic intelligence into non-technical, business-focused and risk-oriented language
- Focus on educating management and keeping them informed.
- Advertise and promote your Information/cyber security departments/projects /initiatives
- Create awareness of the need for continual expenditure in this space.
- Understand and explain why the security measures currently in place are sufficiently effective (or not) to defend against the threats facing your industry.
- Focus on all aspects of Cyber Security i.e. the human factor along with technology, in order to raise employee awareness and promote security best practices.

MAKE IT RELEVANT
MAKE IT PERSONAL
MAKE IT ENGAGING