SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL INFORMATION SECURITY DECISIONS

Upping Your Intel Game

Leveraging Intelligence to Improve Information Security

Nick Selby
Trident Risk Management

Agenda

- One minute of propaganda
- Data *v* Information *v* Intelligence *v* Knowledge
- Types of Information and Intelligence feeds available
- Some Obvious Examples
- Forming an Intelligence Strategy
- The Lifecycle

One Minute of Propaganda

- Managing Director of Trident Risk Management
- Consultant to local and federal LE
- Consultant to banks, F1000 companies
- Founded 451 Group security practice (2005)
- IANS Faculty

I’m Not Here To Tell You How To Suck Eggs, But…

- “Intelligence” is a FUD-, Sales- and Marketing-exploited word and concept
- Defining it is tough
- So the following is to define terms for *this* presentation. Your mileage may vary, check with your doctor, consult an attorney, etc etc.

Things I hear…

"We've got intelligence – we subscribe to Symantec's DeepSight and Cyveillance. We're looking to add to these capabilities."

"We're getting really serious about building out our intelligence operations. Can you tell me about Palantir?"

- These two statements and sentiments are common in mid- to large financial institutions.
- They're not "wrong" but they indicate a piecemeal approach to intelligence operations that can lead to frustration and failure.
- Intelligence is not something you can buy, and there's no box that can deliver it.

Definitions

“ The successful intelligence process converts acquired information into clear, comprehensible intelligence and delivers it to the President, policymakers, and military commanders in a form they can utilize to make educated policy decisions.

-Intelligence.gov

“Intelligence is the process by which specific types of information …are requested, collected, analyzed and provided…”

Mark Lowenthal, *The Intelligence Edge*

“The Intelligence Process: Planning & Direction. Collection. Processing & Exploitation. Analysis & Production. Dissemination.”

-CIA *Consumer’s Handbook to Intelligence*

A Working Definition

In the private sector, “Intelligence” is the process by which a commercial organization gathers data, analyzes it, and produces actionable information in a form that can be accessed and understood by executives - who use it to inform their tactical and strategic decisions. It’s also used as a noun to describe the product of this process.

-Selby

“Knowledge is what you’re after. Information is the raw material you use. Intelligence is what finds and processes information.”

-George Friedman

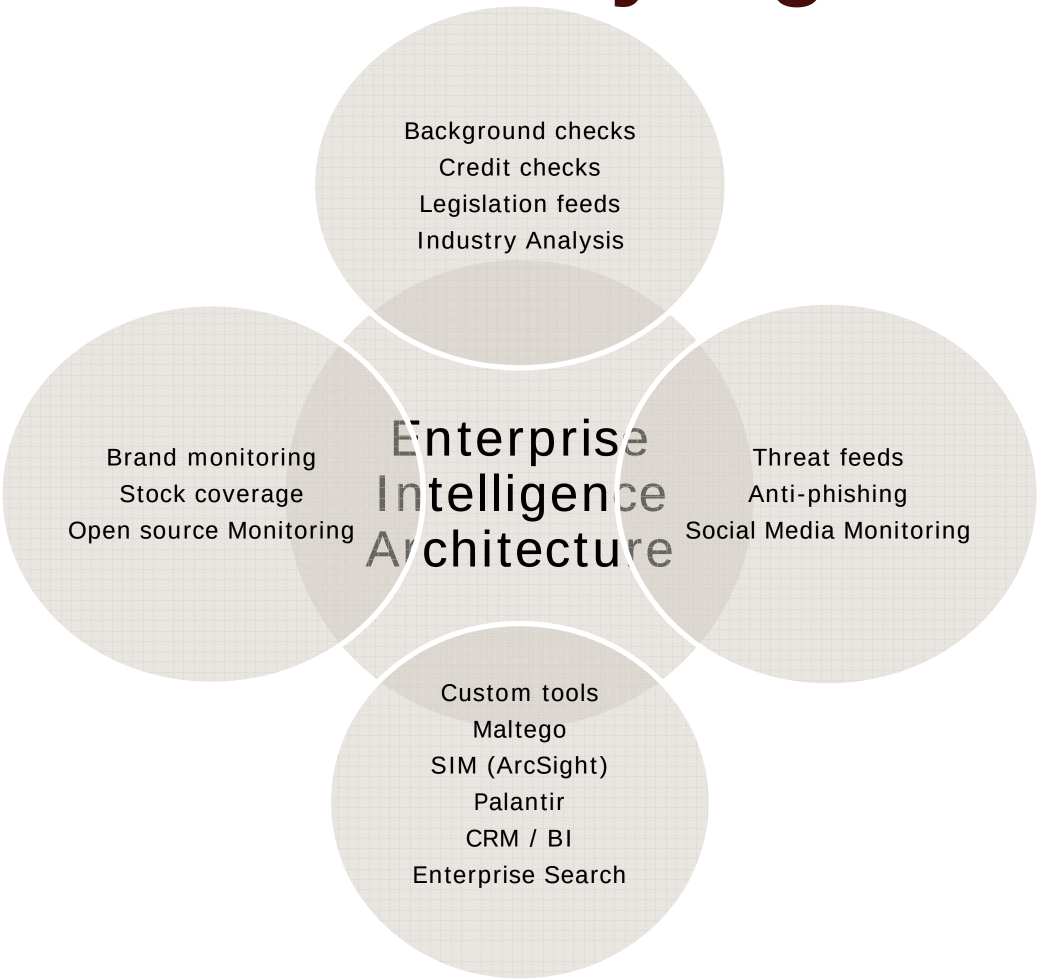
Sources of Information

- Proprietary
  - Stuff you get internally (BI, CRM, HR, legal, etc)
  - Stuff collected by 3rd parties for you (RSA, Cyveillance, MarkMonitor, Radian6 etc etc)
  - Industry analyst reports
  - Industrial espionage
- Open Source (OSINT) – by far the most voluminous
  - Every newspaper and industry rag
  - Social media monitoring
  - Blogs, aggregation sites, etc
  - Tools like Maltego and other link/matching/relationship web software
- Government/Classified

What Are You Paying For Now?

Background and Credit Checks
Legislation Feeds, Industry Analysis, Stock Coverage
Threat Feeds, Brand Monitoring
Anti-Phishing, Open Source Monitoring
Social Media Monitoring
Custom dashboards and Tools
Maltego
ArcSight, Q1, Nitro or other SIM
Palantir
CRM, BI, Enterprise Search Tools

What Are You Paying For Now?



Background checks
Credit checks
Legislation feeds
Industry Analysis

Brand monitoring
Stock coverage
Open source Monitoring

Enterprise
Intelligence
Architecture

Threat feeds
Anti-phishing
Social Media Monitoring

Custom tools
Maltego
SIM (ArcSight)
Palantir
CRM / BI
Enterprise Search

Obvious Example #1

- Legal hears that, of the 60 some-odd pieces of legislation pending in Washington, we might be particularly concerned about the Defending Industrial Computing from Heinous Electronic Attacks and Denial of Service act of 2010;
- Industry Analyst reports discuss the expense of PCI compliance, noting that it is taking increasing portions of security budgets;
- Compliance and CTO's office report progress in the matrix of overlapping regulatory directives;
- Industry press reports that PCI is becoming the "best practices" list;
- Mainstream press reports show payment card industry executives lobbying or testifying in Washington;
- Sharing these datapoints might lead to an inference that PCI and DICHEADS are aligned.

Obvious Example #2

- ATMs in retail branches are getting hit with Skimmer attacks;
- Information about these attacks is coming in from branches to loss prevention, information security, facilities
- Security and hacker blogs start describing the value chain of the skimmer business
- US Secret Service, regional fusion centers, regional retail-law enforcement lists issue warnings describing attack methodology from various regions in the country; DHS Critical Infrastructure Daily lists news reports from around the country
- Intel creates an alert for all branch managers and assistant managers to be aware, seek signs of skimmers, and action plan when one is discovered
- This alert can be shared with other banks to encourage information sharing on issues of mutual concern

Obvious Example #3

- Executive protection observes surveillance of facilities, executives in South Asia;
- Information security sees raised levels of recon-probing and network attacks in South Asia;
- Mainstream press shows growing local disenchantment with US banks, bankers due to their support of blah blah blah.
- Sharing these datapoints might lead to an inference that the threats against executives and facilities and increased threats against networks and systems are not isolated from one another.

FUD: Your Competitors

- The worst damage is done to you by the competitor who understands the intelligence advantage.

To Get This To Work…

- Intelligence must be a defined, funded strategic undertaking
- This does not mean it must be expensive, merely that it must be defined and agreed upon.
- There must be a plan beyond aggregation of information. Intelligence must add value to the information it processes, not just be a collection point.
- An intelligence lifecycle is essential. It will take time. It will be worth it.
- In the legislation example, each party felt they *saw* the big picture and wouldn't necessarily seek outside correlation.
- "Dot connecting" only works when a concerted effort to connect dots meets executive desire, cross-stovepipe authority and application of technical and analytical resources.

Common Barriers

- Executive Buy-In
- Metrics for Success
- Stovepipes ("Cylinders of Excellence")
- Lack of planning
- Lack of analysis; shortcomings in the analytical process or failure to analyze
- Dissemination (in a way that people will actually convert the information to knowledge).

Plan

- What do you want intelligence to do? Are you staying ahead of fraud by keeping up to date with tactics? Legislation? Malware?
- Think strategically about what you want, articulate the strategy clearly
- Give someone responsibility for *and authority to* run an intel shop. Get someone who's done it for the military to be that someone*.
- *They needn't have been an officer – this needn't cost the world
- Articulate the strategy, provide the resources to develop the tactical
- *Leverage, leverage, leverage*

Gather

- You already are gathering, you’re just not working with what you have
- People looking at good, solid, actionable intelligence and not sharing:
  - Marketing
  - HR
  - Legal
  - Executive Protection
  - Traders
  - Logistics and Facilities
  - Information Security
- Think about the kinds of things these folks look at, and how it feeds your intel strategy.

Analyze

- Empower analysts. Get them the tools they need (these need not be expensive) to aggregate the intelligence and look at it
- Encourage and Train. Analysts need to understand the limitations of the collection methods, and see the big picture – and how the information they get informs their understanding
- Ex-military or government analysts are great. So are writers, storytellers, private investigators, police detectives….

Disseminate

- That empowered guy with the authority and responsibility? She’s got to be the voice of the intel department. Solid analysis, stating clearly where data don’t support conclusions and where they do, presented soberly by a responsible person.
- Aim small, miss small. Build on early success. You’re not looking to solve Mideast Peace, but to empower decision makers.
- This is not espionage: you’re connecting dots and adding value by delivering actionable information.

Review

- Nothing new here; basic lifecycle management
- Regularly review your finished intelligence products and measure against the plan and the metrics
- Tweak the metrics, hammer the tactics etc
- Regularly review your feeds, especially the commercial ones, to find synergies, expose those not being used or not serving their purpose etc.

Some Available Feeds

- OSINT: Social Network Monitoring, website-watching, compendiums, searching etc
  - DHS Daily Critical Infrastructure
  - KGS NightWatch, Stratfor
  - Whostalkin.com
  - Securosis, DailyDave, Krebs, Attrition, Shostack….
- Commercial: Threat intelligence feeds
  - McAfee, Symantec, Sophos, Prevx, other AV folks
  - Customized phishing/fraud feeds eg Cyveillance
  - NCFTE and other sources of threat aggregation
- Classified: Government (local, state, federal)
  - If you've got clearance/reason*
  - Critical infrastructure (eg banking)
    - *Caution: Creating open source information from classified sources is not something to try at home

Conclusions

- Leverage what you have
  - Find what you have
  - Remove redundancies, find synergies
- Have a plan
  - Be clear in your strategy and the tactics will sort themselves out
- Give the plan the best shot at success
  - Get/empower good people
  - Define metrics for success
  - Make certain to build on early success

Questions?

Nick Selby
nick.selby@tridentrm.com