Intelligence Led Corporate Security Programs
Why a Business Needs to Setup a Cyber Threat Analysis Unit

Ian Cook

16th Annual Computer Security Incident Handling Conference
Budapest, Hungary
June 13-18, 2004
How Much Security?

• The most critical question that security managers ask is how should they allocate the limited resources.
  • Where are the threats?
  • How much security is needed?
  • How much residual risk?
  • Where is the balance?

• A Cyber Intelligence Program based on proven Government Intelligence processes can help answer these questions
Cyberspace is rapidly growing and has become part of the way we conduct our lives. Accelerating number of new threats and vulnerabilities that appear faster than vendors can fix and patches can be deployed. There is no Perimeter.

Technologies have grown increasing complex so that all the ways systems could be compromised by an attacker cannot be predicted.

Networks, business requirements and risks continuously change and degrade security. Behavior banned today is promoted tomorrow.

Daily volume of security information and intelligence is greater than most organizations can effectively process and analyze.

Few companies have the necessary in-house security expertise. The enemy has become more sophisticated, organized and better resourced.
Time in Which to Make Decisions Decreasing

- Vulnerabilities Increasing
- Patches proliferating
- Days between Alert and exploit decreasing
  - Nimda 331 Days
  - Blaster 21 Days
  - Witty 36 Hours
- Time to Propagate decreasing
  - Code Red 5+ Days
  - Slammer 87 Minutes
  - Witty 45 Minutes
- Exploits are more sophisticated
- Speed of attacks results in widespread damage in little time

Source: CERT
Intelligence Led Decision Making

• Those making security related decisions have often been taking an uncoordinated, uninformed, and unplanned approach to security
• It’s difficult to manage what you don’t know about or understand. (Most Organizations spend less than $250 for every $1 million revenue on security.)
• Security Decisions should be based on facts, not intuition
• An Intelligence Program will:
  – Identify the need for action
  – Provide the insight and context for deciding among courses of action (value added analysis)
  – Provide information/assessment on the effectiveness of pursuing the selected course of action
Intelligence Led Decision Making: Phishing

- Phishing Attack Stages

Monitor

- New Domains including Company name
- Sites containing Company name and requesting ID & Password
- Phishing emails containing Company name
- Seed fake sites with account details and monitor accounts
Anti Phishing Tool Workflow

define rules per client

Cogen Analyser

Alert and Report

Client acts on alert to neutralise threat

Inform company at threat

Inform company at threat

Base threat ruleset (not client specific)

General Alert monitor

Ignore

no threat

possible threat

possible threat

given threat rating

follow links

Email

PDF

SMS

pre-process isolate key characteristics and components

our spam collection + customers + 3rd party spam list

Monitoring Domain registration

(input domain query)

Monitoring Usenet IRC, chatrooms

(spying for early warnings)

email processes

domain processes

newsgroup processes

common processes

Information in four dimensions
Prototype Email Phishing Threat Analyzer
Intelligence Defined

• Intelligence is the product that results or the knowledge that is derived from cyclical processing of information
  United States Intelligence – An Encyclopaedia

• Cyber Intelligence is the systematic and broad-scale examination of Internet activity to assess, predict and understand current and prospective behaviors on the Internet.
Tenets of Intelligence

Intelligence must be:

- **Timely** - Late intelligence is as useless as no intelligence.
- **Accurate** – Must be unbiased and based on fact
- **Usable** – Understandable and specific to current need.
- **Complete** - Must identify all the adversary’s capabilities, identify all available courses of action and forecast future adversary actions and intentions.
- **Relevant** - Must focus on current need.
Questions Decision Makers Ask

- Where are our weaknesses and vulnerabilities
- What threats/adversaries exist
- What tools/capabilities attackers have
- Who’s targeting us and does it matter
- Which potential threats may be imminent
  - Are we vulnerable?
  - Are we an attractive Target
  - What impact might an attack have
- How do our Threats compare to those of our competitors
- What are our competitors doing
- What's being said about us and by whom
- What safeguards / countermeasures can we deploy
- What actions we should take

A Cyber Intelligence Program based on proven Government Intelligence processes can help answer these questions.
Situational Awareness

- Decision Makers need to understand the “big picture” of their Security posture
- Having the right information helps Decision Makers take actions that balance security and cost.

Situational Awareness Requires:
- Perception – What’s Happening Now
- Comprehension – Is it Important
- Projection – What could happen Next

Intelligence Output Requires:
- Right Content
- Right Time
- Right Place and People
- Right Form
Understand Information Needs

- Get a clear understanding of Decision Makers information needs/timescales.
- **What** decisions need to be made?
- **Why** do the decisions need to be made?
- **When** do the decisions need to be made?
- **Who** will be using the intelligence to make the decisions?
- Is the intelligence **nice to know or need to know**?
The Six Stage Intelligence Cycle

Direction for current and future intelligence gathering activities is established.

Collect information from known sources. Identify & collect information from new sources of information.

Intelligence personnel assess how well each phase of the cycle is performed.

Intelligence is delivered to and used by the consumer.

Raw information is converted to forms readily used by analysts.

All available processed information is integrated, analysed, evaluated and interpreted.
Analysis

• Analysis is really the application of common sense and experience to raw information
  

• Turns information into actionable intelligence that leads to informed decisions and actions.
Basic Analysis Steps

• Read all previously processed information.
• Concentrate on the reliable data.
• Recognize gaps in information
• Read between the lines
• Look for patterns
• Organize the information
• Develop a number of possible scenarios.
• Develop long-term and short-term responses for each scenario.
• Know when to quit! *(Know Your Business Drivers)*
Potential Sources of Intelligence Information

- Web Sites
- Search Engines and Tools
- News Feeds
- FTP Sites
- Printed Material
- Vulnerability Alerts
- Professional Associations
- Government Sources
- Vendors
- Industry Organizations
- Media Organizations
- Hacker Organizations
- In House Technical experts

- Periodicals
- Subscription Services
- Newsgroups
- Chat (IRC)
- Information Exchange Partners
- Human Sources
  - Industry experts
  - Underground
  - Law Enforcement
  - Govt. Intelligence Agencies

- Public Record Databases
- Bulletin Boards
- Proprietary Sources
- Etc.
Search Engines

- Google
  http://www.google.com
- AllTheWeb.com
  http://www.alltheweb.com
- Yahoo
  http://www.yahoo.com
- HotBot
  http://www.hotbot.com

- List of Search Engines
Personalized Web Search Updates

Welcome to Google News Alerts

Google News Alerts are sent by email when news articles appear online that match the topics you specify.

Some handy uses of Google News Alerts include:
- monitoring a developing news story
- keeping current on a competitor or industry
- getting the latest on a celebrity or event
- keeping tabs on your favorite sports teams

Create your News Alerts with the form on the right.

Create a Google News Alert

Enter the topic you wish to monitor.

News search:

How often: once a day

Your email:

Create News Alert

Google will not sell or share your email address.
Meta Search Engines

- Meta Search Engines return best results from leading search engines

www.vivisimo.com
www.dogpile.com
www.metacrawler.com
Copernic Agent Professional
(meta-search engine)

- Power-search the Web
- Advanced Management of Searches and Results
- Analyze Search Results
- Summarize Search Results
- Track Changes in Web Pages Contents
- Track New Search Results
- Access Hidden Information
- Create Custom Search Categories
- Automate Result Analysis
- Integration with Internet Explorer and Office

WebSite Watcher

- Monitors Web pages and notifies you when they change

http://www.aignes.com/
The big news last week (and possibly this, depending on what happens) is the massive attack of W32/MyDoom.A-mm (also known as W32/MyMail.R and W32/Myworm), on the e-mail world. According to antivirus vendors, MyDoom started on the Kazaa file sharing network, and spread to e-mail networks. With the sheer multiplication potential of harvesting e-mail addresses from a victim's machine, it didn't take long before MyDoom was infecting 1 in 12 e-mail messages on the Internet. According to MessageLabs, in two days MyDoom broke the Sobig/F worm's previous record from last August of 1 in 17 messages.


Using sophisticated statistical and linguistic algorithms, it pinpoints the key concepts and gives summary of any document.
Net Snippets

- Allows saving selected information on web page
- Information can be edited
- Add comments
- Automatically captures and saves bibliography information
- Automated bibliography reports
- Snippets stored in HTML format so you can later use them in MS Word etc

www.netsnippets.com
The Information Explosion

• The Potential Sources of Intelligence Information are increasing:
  – The size of the world-wide web is doubling every 12-months and this rate is increasing
  – Annual publication rates > 800mb person/annum for every person on the planet
  – Disk space usage in organisations increasing 50-70% per annum
  – The ‘Deep’ or ‘Hidden’ web includes databases of information from businesses, universities, government agencies which search engines can’t spider
  – The Hidden’ web is up to 50 times larger than the visible web (Sherman – Search Engine Watch Newsletter)
The High Cost of Not Finding Information

  - Knowledge workers spend from 15 to 30% of their time searching for information
  - Searchers find what they look for only 50% of the time or less
  - 40% of corporate users report they can’t find the information they need to do their jobs on their intranets
  - The average enterprise wastes at least $1.6 to $2.3m per year searching for non-existent information, failing to find existing information and recreating information that can’t be found
  - The Fortune 1000 stands to waste at least $2.5 billion per year due to an inability to locate and retrieve information.
Intelligence Tool Requirements

- Single point of access to multiple sources:
  - Search engines
  - Subscription sites
  - Specialised portals
  - User defined web sites
  - Bulletin Boards
  - Newsfeeds
  - Newsgroups
  - IRC
  - Etc.

- Collect Information from parts of web not indexed by search engines (Hidden Web)
- Support multiple data formats
- Log-in search source capability
- Automate the search process with ‘human’ like abilities to translate, analyze and intelligently discover content
- Intelligently rank results and summarise content using statistical and linguistic algorithms
- Link analysis for visualizing associations and interactions
Cogenta Research Director

- Single point of access to multiple data sources
- Central Data Repository
- Share results with co-workers – distributed analysis.
- Intelligent agents search hidden web
- Finds new sources
- Searches dynamically created web pages
- Documents ranked using computational linguistic algorithms
- Summarises documents
Behavioral Profiling Techniques

The same data mining technologies used by marketers can be used by Cyber Intelligence Analysts:

• **Data warehousing** for accessing multiple and diverse sources of information and demographics
• **Link analysis** for visualizing criminal associations and interactions
• **Intelligent Software agents** for retrieving, monitoring, organizing, analyzing and acting on information
• **Text mining** for sorting through gigabytes of documents, web pages, public records and e-mails in search of concepts and key words
• **Data mining** for predicting the probability of crimes and extracting profiles of perpetrators
Cyber Intelligence Program Enables You to:

- Facilitate more informed security related business decisions by providing situational awareness
- Predict, understand and give advance warning of imminent or emerging threats, and cyber attacks
- Prevent and effectively respond to potential or actual threats
- Understand how your threats compare to those of your competitors
- Identify whether any actions taken by you or news regarding the company may make you a target, and
- In a world of unlimited threats focus limited resources effectively
Questions?

- www.cogenta.com
- Ian.cook@cogenta.com
- Tel: +44 (0)1252 725478

“Someone else may decide if you will be a target - but you decide whether or not you will be a victim.”

~ Gavin De Becker