Cyber Security Concepts

for Chilean Financial Services

David Livingstone

- Former Serviceman (land, sea and air)
  - Including 2 years as Director of IT for Naval Air Command
- Member - Government Cabinet Committee on Information Warfare
  - COBR staff officer
- Cyber Security Adviser – Scottish Government
- Overseas Missions - Ministry of Foreign Affairs
- Architect – 2 x Virtual Task Forces
- Author – UK Police Cyber Crime Strategy
- Business Case (CLP 55MM) author – UK National Cybercrime Unit
- Adviser on Cyber Security Policy – National Audit Office
- UK Parliament Inquiries
- Applied Research for Chatham House Think Tank:
  - National Risk Management in Electronic Threats
  - Serious and Organised Crime strategy
  - Cyber Security of Critical National Infrastructure
  - Cyber and Civil Nuclear Industry
  - Cyber and Space Supply Chain

NAPIER MERIDIAN

David Livingstone

- Former Serviceman (land, sea and air)
  - Including 2 years as Director of IT for Naval Air Command
- Member - Government Cabinet Committee on Information Warfare
  - COBR staff officer
- Cyber Security Adviser – Scottish Government
- Overseas Missions - Ministry of Foreign Affairs
- Architect – 2 x Virtual Task Forces
- Author – UK Police Cyber Crime Strategy
- Business Case (CLP 55MM) author – UK National Cybercrime Unit
- Adviser on Cyber Security Policy – National Audit Office
- UK Parliament Inquiries
- Applied Research for Chatham House Think Tank:
  - National Risk Management in Electronic Threats
  - Serious and Organised Crime strategy
  - Cyber Security of Critical National Infrastructure
  - Cyber and Civil Nuclear Industry
  - Cyber and Space Supply Chain

NAPIER MERIDIAN

This Symposium

- Two way dialogue of the cyber domain in financial services
- Plenty of time for discussion
- No requirement for exchange of sensitive information
- Proposal - Chatham House Rule
  - nobody is an absolute expert!

- Focus on national financial services requirements to counter the threat
- Start at high level to set common understanding of the challenges we face
- Response to specific questions at the end

- Develop a plan for further discussion and information exchange between parties
- Identify what can be done and how quickly

NAPIER MERIDIAN

CyberSpace - Threat Summary

- Nation States
- Organised Criminal Gangs
- Terrorists
- Individual Hackers

And mixtures of all above – proxies.

NAPIER MERIDIAN

The Nature of Cyber

- Dynamic
- Fast moving
- Agile
- Unpredictable growth in applications
- Difficult to regulate
- Requires specialists to understand it, but needs everyone to become part of the response

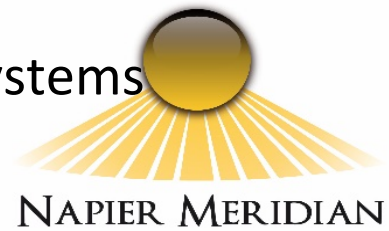
NAPIER MERIDIAN

The Internet

- International / cross jurisdictions
- Attribution is difficult
- Future characteristics uncertain
- Driven by profit
    - Security becomes a secondary consideration
- Proliferation of applications

The Nature of Attacks

- Difficult to detect
- Swift
- No or little warning
- Rehearsal in one sector – main attack in another
- Unattributable
- Executable by an inferior party
- Can be executed via complex access paths including human direct access to systems



The Nature of Losses

- Money
- National secrets, such as in defence
- Intellectual Property
- Reputation
- Identities
- Potentially – physical harm from software corruption
  - eg SCADA systems - Hamoon / Stuxnet

Response

- Cannot be centrally controlled – too slow
- Cannot be technology driven
- Risk management – cannot defend everything
- Communicate the simple things and get the basics right
  - 80% / 19% / 1%
  - firewalls / anti-virus / automatic patching
- Opportunity to ‘deflect’ the threat
  - Bad people do business planning too!

NAPIER MERIDIAN

Increasing Tempo and Agility

- Have to try and match the pace of the Threats
- Cannot be resource intensive
- Flatten the organisation
- Create a better understanding of best practice through collaboration
- Improve knowledge of the domain throughout workforces
- Rely on better coordination to make the fastest strategic progress

NAPIER MERIDIAN

Lessons Learned from UK

- It is more about organisation than just technology
- Don’t invent anything new
- Start small, but keep in mind the big picture
- Use risk management principles
- Do not have an isolated system, create partnerships as wide as you are able
- Use whatever you have available to create an immediate response
- Educate the user communities
- Exercise regularly – all the way to Ministers!

NAPIER MERIDIAN

Things still to do

- Common International understanding of cyber security
- Common lexicon
- Common approaches
- Educate our leaders
- Understand our adversaries better
- Find the disruptive technologies
- Better communications techniques
- Increase collaboration

NAPIER MERIDIAN

Summary

- Create a better understanding
- Agile systems and disruptive technologies
- Find the correct role for Government and Regulators
- Communications and messaging
- Coordination
- Don’t relearn anything!
- Need a better way of sharing sensitive and sometimes embarrassing information

NAPIER MERIDIAN

Potential Mitigation

Financial Services take ‘cyber’ off the competitive agenda

In 2009 the UK formed a national Financial Services VTF consisting of major financial institutions

A VTF is:

- Voluntary
- A trusted environment
- Not regulated
- Involves regulator and law enforcement but only as needed
- Minimal costs

NAPIER MERIDIAN

Virtual Task Forces

Implication

Chilean Financial Services may be harmed by cyber threats thus reducing confidence in the financial services industry. Potentially, a reduction in economic growth may also follow

A Proposal

The Chilean financial services replicates the UK and works together in an unregulated but trusted environment via a VTF system. The VTF collaborates with the regulator, police and intelligence agencies working together to mitigate cyber threats by gathering threat information, coordinating responses and also sharing best practice.

NAPIER MERIDIAN

How a VTF Works

- A trust based relationship to share information
- Use of information not generally permitted outside of VTF
- Regulator and police are ‘invited guests’ for some parts of the agenda
- Chatham House Rule in force – attendees and attribution
- Policy Group of senior executives
  - Meeting quarterly initially
  - Tactical Group of leaders of response teams
  - Weekly telcons
  - Monthly meetings
  - Immediate response coordination

NAPIER MERIDIAN

Benefits

Enterprise Level

- Considerable increase in cyber capability at minimal cost
- The Chilean Financial Services are seen to be responsible in times of increased pressures on economic growth
- Threat actors are ‘displaced’ as they see Chilean financial infrastructure as increasingly hostile

Operational Level

- Better intelligence
- Early warning of developing threats
- Increased resilience
- Reduced response times
- Better level of understanding with police services (PDI etc)

NAPIER MERIDIAN

The Results!

Operation POPLIN

- POPLIN was the first VTF operation and was an Intelligence led covert action executed to minimise the impact of a particular Trojan virus on financial institutions.

- 13 suspects were arrested and prosecuted. The banking sector estimated a loss of £725,000 over 50 calendar days; however, the organised crime network (OCN) had access to a further £18.5M through compromised accounts.

- In addition, data was recovered identifying 50,000 compromised accounts in the USA. The principal received 4.5 years imprisonment

NAPIER MERIDIAN

Operation PAGODE

- PAGODE was a VTF started by an investigation into an OCN running a ZeuS Botnet. The OCN was also hosting the largest global English speaking criminal forum, which allowed the 8500 members to trade compromised credit cards, malicious software etc.

- The harm created through criminal activity linked to the forum was estimated to be in excess of £20million.

- Five UK individuals were arrested and charged, all submitting guilty pleas, including intentionally / encouraging an Offence under the Serious Crime Act 2007.

NAPIER MERIDIAN

Operation DYNAMOPHONE

- DYNAMOPHONE was a proactive cyber crime investigation instigated following the discovery of a number of virtual identities, which had been set up to perpetrate a global online phishing scam.

- The police, with assistance of VTF members, was able to evidence that the relevant OCN obtained £3million through their fraudulent activity.

- Covert police methods established the real identities of the subjects and evidentially linked them to their online virtual identities. The police arrested three subjects with fraud offences.

NAPIER MERIDIAN

Operation LATH

- LATH was started through the VTF following a report from a member that its online banking customers were being attacked by the ZeuS BotNet.
- A major international enquiry incorporating the FBI and Secret Service, and unprecedented cooperation with Eastern European Law.
- The investigation team identified an OCN based in Eastern Europe with a UK arm that was involved in both the online theft and then coordinated 'cashing out' of the stolen money. The OCN was identified as a globally recognised Internet Criminal Organisation responsible for a multitude of attacks on worldwide financial institutions with thousands of victims.
- During a 90 day investigative period, 315 UK accounts were discovered as compromised and evidential losses were discovered to be in excess of £3million. A further potential loss of £125M was identified.

NAPIER MERIDIAN

VTF Development – Cross Sector - CiSP

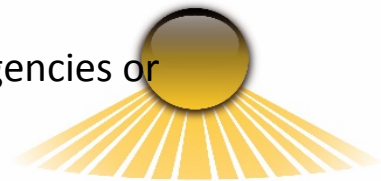
A joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business

- Engagement with industry and government counterparts in a secure environment
- Early warning of cyber threats
- Ability to learn from experiences, mistakes, successes of other users and seek advice
- An improved ability to protect their company network
- Access to free network monitoring reports tailored to your organisations' requirements

NAPIER MERIDIAN

Cyber Security Best Practice Checklist – UK Bank

- Cyber is a risk-management exercise and falls in the top three board-level concerns.
- There is broad accountability for cyber issues, and it is on the agenda of senior management.
- Service-level agreements with utilities and other critical business relationships have been identified.
- Cyber security policy falls under the umbrella of traditional security arrangements rather than being an adjunct to them.
- Extensive due diligence is conducted with IT, procurement and finance as well as critical third parties, and over the past decade the high-risk scenarios that could affect business have been considered.
- The board is involved in walk-throughs for contingency planning, and the effect that a cyber attack would have on the company has been tested.
- Training is conducted from the board level to the shop floor, and includes involvement of directors in scenario-based training for cyber attacks such as ‘denial of service’.
- The organization is working on more age-specific cyber security education for the younger elements of its workforce.
- It monitors online sources of information such as Twitter for brand awareness as well as for attacks on its reputation, and passes intelligence back to the appropriate authorities.
- A system is in place to distribute notices quickly, such as via SMS and office monitors, for a variety of emergencies or incidents including cyber attacks.



We just sat down and thought about it