What has changed in Information Assurance in the Age of Austerity?

John Doody, Director
Interlocutor Services Limited
Is it possible to demonstrate a Return on Investment from Security spend?

Edd Hardy, Head of Operations
CNS Hut3
Security is seen as a cost.

- It does not generate revenue.
- You are trying to protect yourself from bad people.
- It is a constant cost, every year, security wants and needs more money.
- We only hear about it when it goes wrong (when did you last hear a bank tell you they had a major attack but they defeated it (possibly because they don’t know!))
- If you were the CEO, and you had a cost, that kept going up, but you still get attacked and hacked, it generates no return (or rather you can’t prove it), would you spend anything other than the minimum?
The approaches to security spend and ROI

• 1 – Spend after your attacked
• 2 – Spend what you are obliged to (e.g PCI, CoCo)
• 3 – Hide it (don’t use the word security, bundle it in with general IT Spend)
• 4 – Fight for Every Penny
• 5 – Invest, and prove it adds value and we are getting better
1. Spend when you are attacked.

- The consultancy or kit you have been asking for will help secure the organisation.
- But it costs £20,000
- Your request is refused because it offers no benefit to the organisation, it doesn't make things faster, more efficient or better (non techies struggle to see secure = better)
- You get hacked and it costs you £100k in fines.
- Your request for the consultancy or kit is rapidly approved, because they can now see that 20K is cheaper than 100K and bad things happen to good organisations.
- Its now cost you 120k to buy a 20k firewall.
2. Spend when you are obliged to.

- Standards like PCI and CoCo and ISO 27001, are good for security consultancies like us.
- The board can understand that this standard is a requirement, if you want to take credit cards, it’s a cost of doing business.
- It is easy to see a ROI, PCI Costs us £100k but we can process £5 Mill a year in cards.
- But, as with all standards, they focus on what they want to focus on (e.g. PCI cares about card data, it doesn’t care about your medical data)
- It helps with security, but it is selfish security, not across the board.
3. Hide It (the traditional approach)

- Security is a dirty, expensive word.
- Bundle the costs into individual projects
- E.g. a PenTest can be tucked away in the project development costs.
- The firewall with an IDS module is a replacement for the EOL firewall without one.
- Very traditional, we see it in a lot of Government organisations.
- Means there is no organisation wide security posture, its about individuals who care, fighting for money and doing the best they can (whilst not ideal, we admire them very much for doing so)
4. Fight for Every Penny.

- There is usually a CISO or someone with security as a responsibility.
- Standards exist, risk management exists, compliance exists.
- Usually in regulated areas like Finance and Gov.
- The CISO spends far more time arguing for money, manipulating budgets and trying to pinch money from projects, than actually CISOing.
- Virtually impossible to prove value for money, ROI, or that things are actually getting better.
5. Invest and Prove it Adds Value

• Very tricky to do.
• Your network is constantly changing.
• The attacks are evolving.
• Nobody sees your successes
• Everybody sees your failures (even though they didn’t invest its still your fault)
• For Example:
Penetration Testing.

- It should be done regularly (at least Annually).
- We give you a huge report full of critical and high issues.
- You spend money on the test and then money + time fixing the issues.
- Next year we come along and find lots of critical and high issues.

- **We** know that new issues come along, things have changed and you have put a lot of work in.
- For the Management, its hard to understand and see the ROI.
  - Year 1 = Test 20K + 100K time/kit Fixing stuff = £120k
  - Year 2 = Test 20K + 100K time/kit Fixing stuff = £120k but we still have bad reports
Penetration Testing.

Client

- Harder to get budget
- Harder to justify the time
- End up fire fighting the issues not the causes. Treading water
- No ROI

CNS

- Harder to get spend on High Quality Testing
- Repetitive when problems not fixed
- We want to make things more secure and focus on challenging issues
Our Solution.

Next Generation Penetration Testing

- **Rate Assets** - all assets are equal – you rate them by importance
- **Rate Risks** - All risks are not created equal – you rate which risks are worse for you.
- **Assign Fixes** – Fixes are complex, multiple people and teams might be involved.
- **Track Progress** and fixes.
- Get continual **support and verification** from us.
- Most importantly – **Track overall risk** and demonstrate progress
- Testing and security advisory has to be seen as continuous and multiyear, this is not a one off project.
Our Solution.

• If we can mark how good or bad you are
• If we can mark how quickly you fix things
• If we can mark how much risk you have overall.
• If we can compare to previous assessment and show improvement.
• If we can bring in relevant risk data.
• If we can bring in relevant intelligence.
• We can actually show the board, what the spend has bought them.
• Instead of we have to spend 100k and we’re not sure.
• We can say we spent 100k and improved by the amount.
Solution.

Next Generation Penetration Testing

• Yes we want you to buy it, but we genuinely want to fix stuff and make it better.
• We want to help you:
  • Spend your limited budget in the most effective way to increase security.
  • Get things done as quickly as possible.
  • Fix the things that matter to you not me.
• Demonstrate that things are getting better and that you are delivering value for money to the organisation.
Replacing the GPMS with the GSCP

the original business drivers, how the new scheme has been implemented, what we’ve learned, and what more is still to be done

Peter Drissell, Head of InfoSec
Civil Aviation Authority (CAA)
Cyber Security in the time of Austerity

Shannon Simpson, CCO
CNS Group
The Austerity Agenda

1. Budgets are being cut.
2. Budgets are harder to compete for.
3. Cyber Security ROI is often hard to demonstrate (to people who don’t get Information Assurance)
4. Or Cyber Security is coming out of existing budgets.
Cyber Security Trends

• Attackers are becoming more capable and the attack types much more sophisticated.
• Day Zero attacks and Advanced Persistent Threats are on the increase.
• Knowing what to look for is becoming more difficult
• More controls are being mandated (Zero Tolerance on PSN compliance)
  • Protective Monitoring
The Challenge

How do we address the increasing cyber threat on a decreasing budget?
## Approaches to Cyber Security Services

<table>
<thead>
<tr>
<th>Approach</th>
<th>+ives</th>
<th>-ives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud/Appliance</td>
<td>Cost, compliance, easy deployment</td>
<td>Inflexible, lacks context or integrated process, does not fit all</td>
</tr>
<tr>
<td>IT Outsourcer</td>
<td>AOI service, in budget,</td>
<td>Cost, not specialist, conflict of interest, poor SLAs</td>
</tr>
<tr>
<td>MSSP</td>
<td>Cost, specialist, continuity, focus, objective, integrated</td>
<td>Opex, vendor lock-in</td>
</tr>
<tr>
<td>In-house</td>
<td>Control, integration, technology choice, data privacy</td>
<td>Cost, skills retention, lacks global visibility, brain drain, maintenance</td>
</tr>
</tbody>
</table>
What to look for?


A supplier should be able to provide:

• Clearances, accreditation and ability to work within the relevant environments
• Relevant understanding of business and technical environments (vertical specific)
• Experience in dealing with cyber security events
• Fast and effective investigation and response
• Collaboration with law enforcement, CERTs and Government
• Not JUST SIEM (Protective Monitoring)
• Quality, tailored and integrated services
What do we offer?

CNS Mosaic COMPLY & SECURE offer:

- Multiple Security functions (controls) in platform
- Single Platform with a Universal View
- UK Sovereignty
- Simple Deployment
- PSN Accreditation & SC Cleared SOC
- 24x365 Cyber Security monitoring service

Making it a:

Cost effective, real-time detective and re-active service to protect your data against cyber threat.
Multiple Controls in a Single Platform?

- Protective Monitoring
- SIEM
- Threat & Malware Detection
- Intrusion Detection
- Vulnerability Management
- Behavioural Analysis (Netflow)
- Asset Discovery
- Threat Intelligence
- Compliance Monitoring

Unified Security Management Platform
Single Platform – Universal View

Unlimited Assets
Multiple Locations
Complete UK data Sovereignty
Cloud or CPE deployment
24x365 Security Ops Centre
PSN Accredited
SC Cleared Staff
Compliance Management
CERT / Incident Response

Unified Security Management Platform

COMPLY&SECURE
Cyber Security-as-a-Service
UK Sovereignty

Camberley Data Centre
Tier 1 Primary
Tier 2 Back-up

Enfield Data Centre
Tier 2 Primary
Tier 1 Back-up

Camberley SOC

London NOC

UK Security Operating Centres
2 x UK Datacentres (NO offshoring – Mandatory HMG Requirement
Resilient WAN and PSN connectivity
Simple deployment
(Federated Model)
PSNSP Accreditation

- **ANY** 3rd party SERVICE PROVIDER wishing to do business with HMG MUST be accredited to PSN standards and have PSN lines installed.

- CNS has now achieved compliance and is able to be called a PSN Service Provider (PSNSP) – SRV_0220

- Controls ensure that CNS able to routinely sell services to a large number of HMG entities
Information & Reports

- Latest SIEM vs Logger Events
- SIEM: Top 10 Events by Product Type
- Threat Level
- SIEM: Events by Sensor/Data Source

Graphs and charts showing various data and trends.
Information & Reports
Types of alarms we see in the SOC
(Accredited Environment)

- **Environmental Awareness — COMPLIANCE EVENT** - Policy changed, logs cleared, configuration changed or privileges escalated
- **Delivery & Attack — Bruteforce Authentication** — COMPLIANCE EVENT - Firewall Access Failure
- **Bruteforce Authentication** — COMPLIANCE EVENT - Switch Management Access Failure
- **Environmental Awareness — Unauthorized Access** - Firewall Management Access Failure
- **Environmental Awareness — Network Anomaly**
- **E.g. Someone attempting to guess the password on a device (trying lots of different passwords). Dictionary attack**
- **E.g. Someone attempting to gain access to a switch without proper privileges**
- **E.g. Someone attempting to gain access to a firewall without proper privileges**
- **E.g. Someone making a change to a switch or firewall, or logs into a server and escalates their privileges or clears security logs on an AD Server**
Types of alarms we see in the SOC
Non-Accredited Environment

- Delivery & Attack — Bruteforce
- Authentication — Boundary Firewall Detected Malicious Activity
- Environmental Awareness — Network Anomaly — COMPLIANCE EVENT — System error or failed connection
- Environmental Awareness — Configuration Changed — COMPLIANCE EVENT — Policy changed, logs cleared, configuration, changed or privileges escalated
- Environmental Awareness — Network Anomaly

80%

6%

11%

3%
How we give you more?
Access to information and data

• **Staff retention and Empowerment:** we automate the mundane keeping them focussed on the interesting information to provide power to the elbow!

• **Ongoing and Easy Compliance:** no longer a drawn out affair to achieve annual compliance accreditation.
How do we give you more?

Deployment and Integration

- **Single system** for multiple controls
- **Quick Deployment**: 60 days to live service, 30 days tuning
- **Quick Answers** e.g. Is that malware an exposure to me?
- **Shorter Remediation**: time and quicker fixes, better use of internal resources.
How do we give you more?
Flexibility and Price

• **Measuring your Budget:** look beyond the “noise” and see where your budget and time is going

• **Cost & Procurement:** flexible per asset per month contracts via G-Cloud or RM1058

• **Quicker ROI**
Examples
SSH brute force attack

- SOC reported continuous brute force attacks on switch from IP’s originating from Shanghai
- Customer stated that switch on internal network ONLY and stated therefore not real attack not real!!
- Analyst showed that it was “exposed” to the internet and source attempting to gain access to sensitive data
- Totally insecure switch
- Switch swiftly removed.
Examples

Poodle Attack (SSL Vulnerability)

- SOC sustained SSL poodle attacks against client web servers
- Escalated to CNS Hut3 SOC Level 3
- Within 11mins customer informed that 111 servers exposed. These were identified and patched
Examples
Existing Customers

• UK Police Forces
• PSN Private Cloud Providers
• Central Government Applications
• Local Government Applications
• Home Office Applications
• MOJ Service Providers (HMP)
Conclusions

• It doesn’t have to take a year to implement a Cyber (Protective) Monitoring Solution
• You can have the assurance, intelligence, information and compliance you need in one service
• You can justify the spend within 3 months
• You can have many controls in one platform
• You can have these services with UK Sovereignty across the PSN
• You can have a flexible contract
• You can do it all on a limited budget
Cryptography
From Black Art
to
Popular Science

Fred Piper
Aims of Lecture

- To enjoy ourselves
- To look at some implementation issues for cryptographic systems
- To see how cryptography has changed in the last 40 years
Industry’s Problems with Implementing Cryptography

- No real problems with algorithms – it’s the wraparounds
- Serious concerns about some recent events – DigiNotar, RSA, Wikileaks, Snowden revelations
- Not sure how they should be regarding possibility of quantum computers
- Cryptography needs standards (change slowly), but Industry needs flexibility
- Need for early warning about necessary changes (e.g. key lengths)
- Concerns about timeliness of hardware (cryptographers recommend changes faster than hardware can be replaced)
A Little History

• Pre-1975: Hush hush!
  – Practised mainly by Governments and military
• Early 1980s: Courses start
  – Customers start to know what they require
• Early 1990s: Qualifications start
  – The role of security manager is no longer a punishment
• Early 2000s: Popular science
  – Everyone knows about it
• Today: Fundamental to e-commerce, e-Government etc
Royal Holloway: Our Most Famous Ex-Student?
Why is the Profile of Cryptography Growing?

• Increase in volume of communications over insecure channels
• Increased requirement for remote access to information
• Regulatory requirements for ‘adequate’ protection of data
• Need for electronic ‘equivalent’ to handwritten signatures and other forms of identification
• It can be fun!
Bletchley Park
Some Important Changes since 1945

- Advent of software
- Advent of fast computers
- Advent of new communications media
- Advent of binary codes
- Increase in general awareness
- Many applications other than provision of confidentiality
- Public key cryptography
- Seen as part of a wider discipline: Information Security
What is Information Security?

Information Security includes the following three aspects:

• **Confidentiality**
  – Protecting information from *unauthorised* disclosure, perhaps to a competitor or to the press

• **Integrity**
  – Protecting information from *unauthorised* modification, and ensuring that information, such as a customer list, can be relied upon and is accurate and complete

• **Availability**
  – Ensuring information is available when *you* need it

**NOTE:** Impersonating an authorised user is often a more effective form of attack than ‘breaking’ the technology
Authentication

- It is important to authenticate people and devices
- Man-in-the-Middle Attacks
- How to beat a Grand Master at chess
Early Definition of a Cipher System

Message $m$ is encrypted using the Encryption Algorithm with a Key to produce the Cryptogram $c$. The Ciphergram is then intercepted and decrypted using the Decryption Algorithm with the same Key to produce the original Message $m$. The Key establishment channel is (secure).
Confidentiality

How do you keep a secret?

• Don’t let anyone have access to the information
• Disguise it so that ‘unauthorised’ people cannot understand it
  – Shared secrets rely on trust
  – Trust in people, processes, technology
• If you use cryptography to protect your information then there will be a key to which you must deny access
Warnings

- If that key is lost and the algorithm is strong then your data is lost ‘forever’
- If someone else gains access to that key then they almost certainly have access to your information
Disclaimer: Cryptography ≠ Security

- Crypto is only a tiny piece of the security puzzle
  - but an important one
- Most systems break elsewhere
  - incorrect requirements or specifications
  - implementation errors
  - application level
  - social engineering
Attacking Cryptographic Systems

- There are many attacks including:
  - Break the algorithms
  - Attack associated protocols
  - Attack key management
  - Attack the hardware
  - Impersonate genuine users
  - Bribe genuine users
  - Espionage
Kerchoff’s Principle

- The security of a cryptographic system should not depend on keeping the encryption algorithm secret

**It does not say**
- The encryption algorithm should be made public

**However**
- Anyone assessing the security of a cryptographic system needs to have confidence that the algorithm is strong

**So:**
- Financial institutions should use public algorithms where appropriate
A Fact of Life!

- In theory there is no difference between theory and practice. In practice there is.
It is NOT just about Algorithms

Early 1980s:
• Thorn EMI conference
  “Security is People”

Early 1990s:
• Ross Anderson’s paper
  “Why crypto systems fail”

Early 2010s:
• See Kenny Paterson’s homepage
Cryptographic Systems

- The use of strong algorithms prevents attackers from calculating or guessing keys
- Keys need to be stored and/or distributed throughout the system
- Keys need protection
Protecting Keys (Storage or Distribution)

- Physical security
  - Tamper Resistant Security Module (TRSM)
  - Tokens (Smart Cards)
- Components
  - Secret Sharing Scheme
- Key hierarchies
  - Keys encrypted using other keys
  - Lower level keys derived from higher level ones
Side Channel Attacks (1)

To find a cryptographic key

- **Exhaustive key search attacks** try to find the secret key by random trial and error
- **Side channel attacks** try to use additional information drawn from the physical implementation of the cryptographic algorithm at hand so as to be **substantially better than trial and error**
Some Recent ‘Changes’

• More attacks concentrate on the implementation of the algorithm and the accompanying protocols
• Some exploit error messages
• Academic research is becoming less ‘blue skies’ and focussing on real systems/problems
• Theory and practice are getting closer to each other
Error Messages

ATM transaction

• Incorrect PIN
• Insufficient funds in account
• Exceeded daily limit
Some Things Never Change

• The widespread use of encryption for confidentiality has always been a cause of concern for Governments
• Simplified version of Government’s position
  – They are happy to support the use of strong encryption for ‘good’ purposes
  – Unhappy about the use of strong encryption for ‘bad’ purposes
Saints or Sinners?

Who are the ‘good’ guys?
Law Enforcement’s Dilemmas

- Do not want to intrude into people’s private lives
- Do not want to hinder e-commerce
- Want to have their own secure communications
- Occasionally use interception to obtain information
- Occasionally need to read confiscated, encrypted information
• After 35 years, I have finished a comprehensive study of European comparative law

• In Germany, under the law, everything is prohibited, except that which is permitted

• In France, under the law, everything is permitted, except that which is prohibited

• In the Soviet Union, under the law, everything is prohibited, including that which is permitted

• And in Italy, under the law, everything is permitted, especially that which is prohibited
Problem

- Who, or what, can we trust?
Any Questions?

• You can contact me at
  fred.piper@codesandciphers.net