Professor John Walker FBCS CISM CRISC ITPC CITP

Threat Update - 2013

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Who AM I

Interim CISO – EU/USA Based Global Financial Organisation
Director of Cyber Research (Ascot Barclay Group)
Member ENISA CEI Listed Experts - http://www.enisa.europa.eu/
Registered International Expert Witness
Chair - ISACA Security Advisory Group (London)
Editorial Board – Cyber Security Research Institute (CRSI)
Microsoft Partner
Freelance Writer
Visiting Professor School of Science and Technology NTU
Visiting Professor/Lecturer – University of Slovenia

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

SITREP – 11/02/13

Criminals are Winning – and the Rewards are HIGH
http://www.bankinfosecurity.co.uk/blogs/new-fraud-scheme-launched-via-chat-p-1403

Hacktivists are, well Active (*NOT forgetting Cyber Radicals*)

PCI-DSS has been found to be FLAWED

The Standard of '*Overcompensation*'

Skills Low – *they need to be honed*

International Threats Ignored

Too many Reports – NOT enough Action

Lack of Reporting

Lack of Public Security Awareness

"Lack of robust access controls is a risk we see," he says. "Processors aren't diligent enough about monitoring access to certain systems."

Sloppy Security

Visa's alert about cash-out schemes warned card issuers to be on the lookout for suspicious activity linked to debit accounts. Although Perez would not discuss any additional details related to the alert, he says the real problem is sloppy network security and gaps in **Payment Card Industry Data Security Standard** compliance. These bad habits can enable hackers to access card data that's used in the cash-out schemes.

ISACA
London Chapter

Yesterdays Threat

a) Malware – Once considered by Government Agencies to be a passing nuisance is now a significant threat!

b) SPAM – Thought to only be a communication which had to be managed. Now it is a major conduit for Malware, and other adverse infiltrations!

c) Cyber Intelligence Gathering is a reality and not a myth (consider the Cuckoos Egg)!

d) Cyber Attacks have taken place against the UK, US, and Germany to name but a few!

e) Root Servers are regular targets!

f) IP is everywhere, and so the threats are commensurate and rising!

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Some ~~Good~~ Bad Examples

1. *DNS*
2. *Exposures & Vulnerabilities*
3. *Users – Education & Awareness (Not me Gov)*
4. *Patch & Fix (or NOT)*
5. *Bleeding Edge Technologies*
6. *Virtualisation & Cloud (and its **not** new)*
7. *Lack of Standards*
8. *New Age Malware (Smart Cell Phone)*

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Real-Time, Real-World

LONDON, Jan/07: The Director General of MI5 warned British companies of possible cyber-attacks originating from China.

The Prime Minister's office accused China of engaging in state-sponsored espionage targeting integral parts of Britain's economy, using the computer infrastructure of Banks and financial services.

*April 2010 the **Cabinet Office assessed the threat from Electronic Attack from Russia, and China was rated SEVERE**. Better late than never:*

China blamed for cyber-terrorism

by Robert Blincoe

28 Jul 2008

Be the first to comment

Professor John Walker has accused the Chinese government of being behind the 'Titan Rain' attacks

China has been accused of sponsoring cyber-terrorism at a conference organised by the UK Home Office.

Professor John Walker, managing director of forensics consultancy Secure-Bastion, said at the International Crime Science Conference in London last week that the Chinese government was behind the 'Titan Rain' attacks on the US and the UK.

NOTTINGHAM TRENT UNIVERSITY

ISACA Trust in, and value from, information systems London Chapter

Public Exposures

Hotels & Public Access Points can present very insecure & hostile environments which can & *do* exposure their users!

Example of a deployed Access Point at a well know London Hotel which is *compromised* & possibly being exploited today!

MAC Address: 02:C0:DE:XX:XX:XX
State: Node is Up
First Seen: 23 November 2012 05:30:17

Active services: 2
443/https Secure World Wide Web HTTP (SSL)
8080/http-proxy Common HTTP proxy/second web server port

Where am I? > Home > Opinion > Security > Security Technology

Incidents in hotels sow reservations abo

24 Sep 2009

Comments: 2

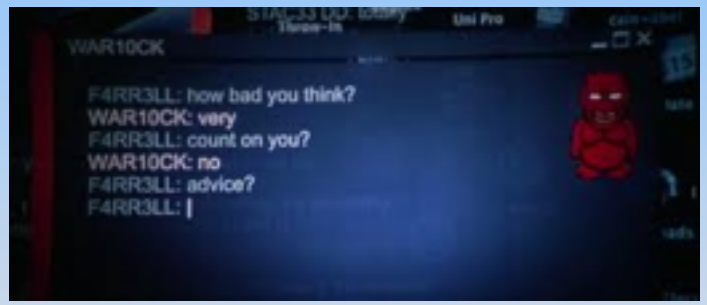
The Radisson Hotel chain recently joined the ranks of companies owning up to significant breaches of computer systems, compromising credit and debit card data.
Like many professionals, I have travelled extensively. Being a security expert, along the way I have made a number of observations, which highlight how often security has not been a high priority.

Some time ago at a hotel in Cyprus, I was directed to place my bags in an unlocked baggage room. I noticed the flashing lights of a computer in a cupboard. Opening the door, I was looking at and had access to the hotel's IT systems, including the primary server, complete with keyboard and monitor. It was completely insecure, and allowing interaction with the system.

http://www.computing.co.uk/ctg/opinion/1844378/incidents-hotels-sow-reservations-security

ISACA
Trust in, and value from, information systems
London Chapter

Die Hard – 4 – With Nails



Fiction-or-Fact!

ISACA
London Chapter

Exposures & Children

> A much needed service – *very important to be backed* – and this work *must* continue – but:

> I am not interested in the reporting of Abuse, but more concerned with Action to protect.

> I would like to see more direction given to parents as to the Risk of the Internet – this is sadly, still the missing element – *e.g. Webcams*

E.g. Windows 8 applications for easy *Remote Control* & *Access*.

> I would wish to see CEOP get more press, and coverage *before* the event in *Proactive* mode, and not post, in the *Reactive* mode as a conduit for the reporting of successful abuse

> Needs wider *Public Awareness* and partnerships

ISACA
Trust in, and value from, information systems
London Chapter

Critical Infrastructures Exposed

By the very nature of what the Power Industry supply, and support - they are a **Target**! – ***But they don't seem to know it!***

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

911 ?

Security Lessons Learned from California Power Outage

John Walker | GUEST OPINIONS | 14 SEP, 2011

Share

The 9th of September 2011 saw **a power outage** in the U.S. affecting 5 million people in the area of Southern California - the root cause analysis of which is said to have been one single employee switching out a piece of problematic equipment. The upshot of this single act is nevertheless extremely worrying, as it manifested in traffic chaos, cancelation of flights, the shutting down of two nuclear reactors, a widespread impact on business, and on the residents.

This event does, however, raise a number of questions and points back to the long debate about the security of **Supervisory Control and Data Acquisition (SCADA) systems** which are considered, in some cases, to host a soft underbelly for cyber attacks. There is

http://www.bankinfosecurity.co.uk/blogs/ddos-its-about-internet-insecurity-p-1408

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Smart Phones and BYOD

The advent of the Smart Cell Pones – (Hand Held Micro Computers) host a vast range of features, and are no longer simple devices which *just* make Telephone Calls.

They are installed with high capacity storage capabilities well in excess of their early Big Brothers and Sisters based on 8086 Chips.

They are hosting Bluetooth, WiFi (802.11 . ..), and Web Access – they talk to the Internet, and communicate into Clouds.

They are also enjoying the interest of Malware Writers, and currently there are approximately 300 such applications in circulation.

The AV Companies are responding with early solutions . . . . *but*

They are the next new target . . . . . Watch them rise in 2013 . . .

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Potential Exposure (Proven)

- *FOCA*
- *Metadata*
- *PDA's*
- *Mobile Phones*
- *Smart Printers (MFD's)*
- *I/O Devices*
- *Firewall Aware Malware*
- *Internet, Sharing, SharePoint, Dynamic URL*
- *FireSheep (New Nov 2011)*

To name but a few of the potentials to host insecurity

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Advanced Threats

Cyber attacks of *eCrime/eFraud are*, ***Phishing***, ***Cyber-Extortion***, ***RockPhish*** and ***FastFlux***, ***Scams*** *(419)*, ***Spear Phishing***, ***Malware***, ***Botnets***, ***Rootkits***, *and* ***DoS/DDoS*** are some examples of the methods of choice of *Criminals*, *Organised Crime*, and *Hacktivist* to attack business, systems, and the end-user community alike.

These acts are ***remote*** from the enterprise perimeter, so ***physical*** assess may prove to be impossible as the related ***artifacts will be dynamic***.

To accommodate a level of **CSIRT First Responder Digital Forensics**, and Investigative Response, the methodology to be employed is referred to as:

Distance Based Digital Forensics

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Groups & Rationale

5/11/12

NOTTINGHAM TRENT UNIVERSITY

ISACA
Trust in, and value from, information systems
London Chapter

Physical Threats

- *Times are Changing – Consider!*

- *East Midlands Airport*
- *Stephen Timm's*
- *Chicago*
- *Mumbai (x2)*

May we conclude that, if the prospect of 'Radicalisation' is interwoven in our Society, should we expect to see more use of Cyber Tools in 2013! – Low Cost Munitions, with High Impact Potentials!

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Global Cyber Threats

http://www.counterterrorbusiness.com/

ISACA
London Chapter

Unrestricted Warfare

Unrestricted Warfare is a book on military strategy written in 1999 by two colonels in the People's Liberation Army, Qiao Liang and Wang Xiangsui.

ISACA
London Chapter

Islamic Jihad

Global Islamic Media Front's (GIMF)

ISACA
Trust in, and value from, information systems
London Chapter

DDoS

Are Banks Winning the DDoS Battle?

Traffic Monitoring Shows Decline in Online Outages

By Tracy Kitten, January 18, 2013. Follow Tracy @FraudBlogger

Credit Eligible Email Tweet Like Share


John Walker

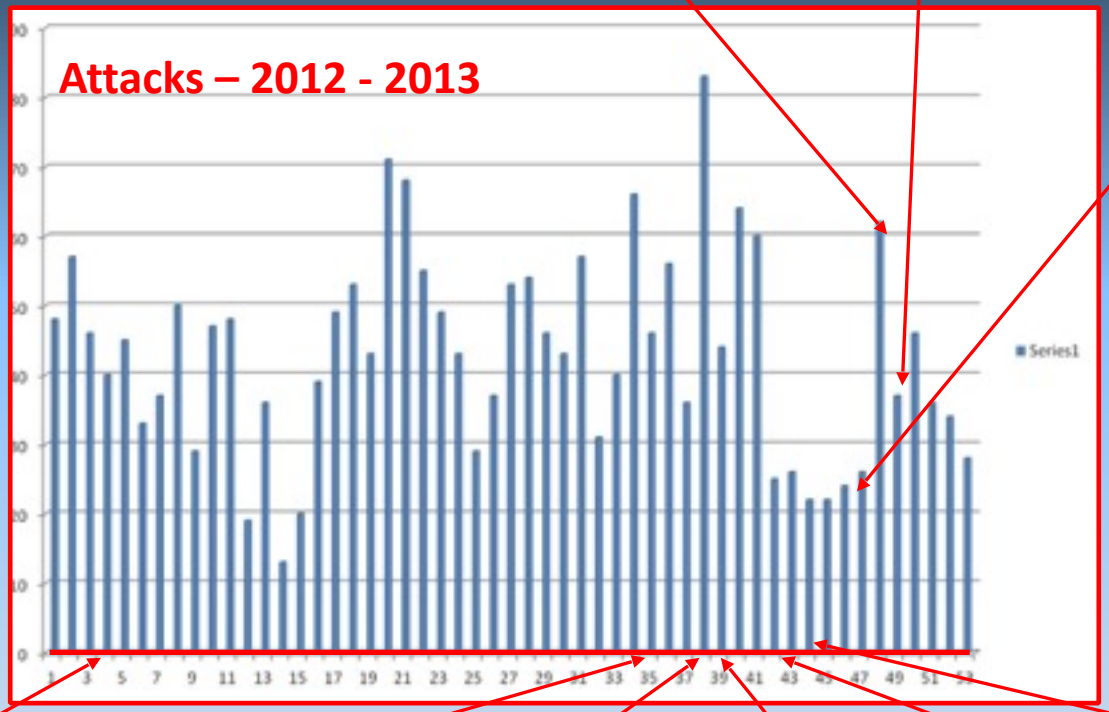
Despite the claims of hacktivists, U.S. banking institutions say their websites now suffer fewer and less severe outages linked to traffic surges tied to **distributed-denial-of-service attacks**. And online traffic patterns tracked by one third-party monitoring service appear to support the banks' contention.

Keynote Systems Inc., an Internet and mobile cloud testing and monitoring firm that tracks online traffic, reports that outages affecting U.S. banking websites have declined in recent weeks, during phase 2 of the hacktivists' DDoS campaign. Keynote tracks site availability statistics for all leading U.S. financial institutions and other companies across numerous industries.

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Global Attacks



California = 38
Honk Kong = 50

Italy = 20
China = 428

California = 33

California = 31

Hong Kong = 66
Turkey = 52
Poland = 10
Brazil = 19
California = 20

Turkey = 161
California = 22

South Korea = 24
Japan = 36
Venezuela = 15
Brazil = 34
California = 24
Indiana = 25
Australia = 4

Italy = 24
California = 30
Brazil = 53

Venezuela = 11

ISACA
London Chapter

From Russia with Love - CaaS

Offering	Price
Cheap email spamming service	US$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US$50–500 per 50,000–1,000,000 emails
SMS spamming service	US$3–150 per 100–10,000 text messages
ICQ spamming service	US$3–20 per 50,000–1,000,000 messages
1-hour ICQ flooding service	US$2
24-hour ICQ flooding service	US$30
Email flooding service	US$3 for 1,000 emails
1-hour call flooding service (i.e., typically takes call center services down)	US$2–5
1-day call flooding service	US$20–50
1-week call flooding service	US$100
SMS flooding service	US$15 for 1,000 text messages
Vkontar da	
Mail.ru ad	
Yandex.ru a	
Skype SMS	
Email spamr	

Offering	Price
Linux rootkit that replaces ls, find, grep, and other commands	US$500
Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers	US$292

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

Offering	Price
1-day DDoS service	US$30–70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Source = Trend Micro

ISACA
Trust in, and value from, information systems
London Chapter

CyberWar - CyberConflict

Cyber War is now considered to be a reality, and represents an Aggressive capability which hostile nations may utilise against a target.

Cyber War capabilities exist in Nations where their internal technology Capabilities are extremely low, but they do have high capabilities to attack outside their logical boarders.

It is anticipated that Cyber War will be an activity which would be a joined force alongside Kinetic Warfare.

In certain conditions, Cyber War holds the potential to escalate into Kinetic engagements.

Early singes have been seen of Hostile Government Capabilities.

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Advanced Threats

Called **A**dvanced **T**hreats, **A**dvanced **P**ersistent **T**hreats (**APT**), **A**dvanced **E**vasion **T**echniques (**AET**) – they are all New *Age Cyber Threats that carry Payload.*

And it is highly likely they are responsible for many of the well Publicised security breaches, and the state of ***Assumed Compromise****.*

OSI-Layers	Sample Protocols	Sample Evasions
7. Application	SMB	Filename obfuscations
6. Presentation		
5. Session	NetBIOS	Inject chaff-traffic
4. Transport	TCP	Time-wait decoy
3. Network	IPv4	Send duplicate fragments
2. Link		
1. Physical		

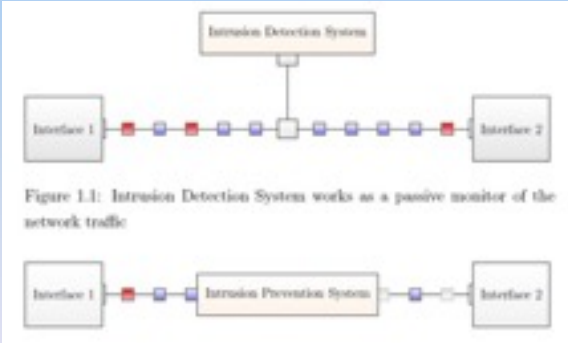
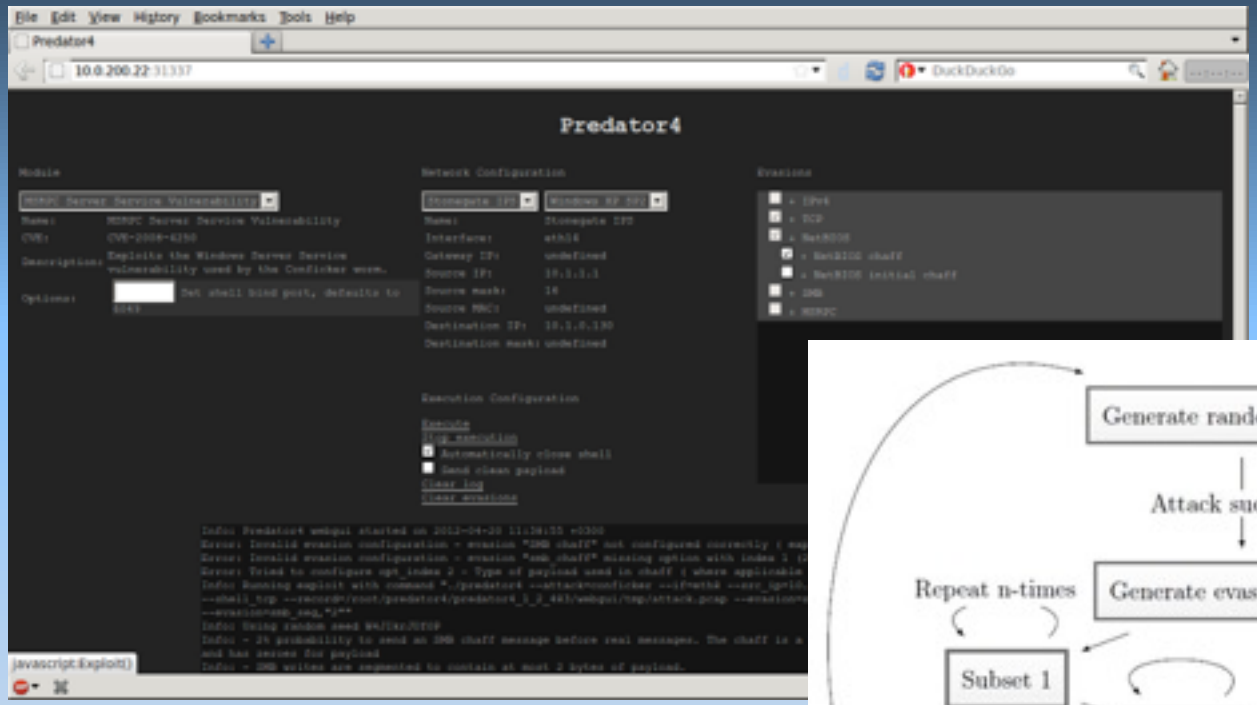


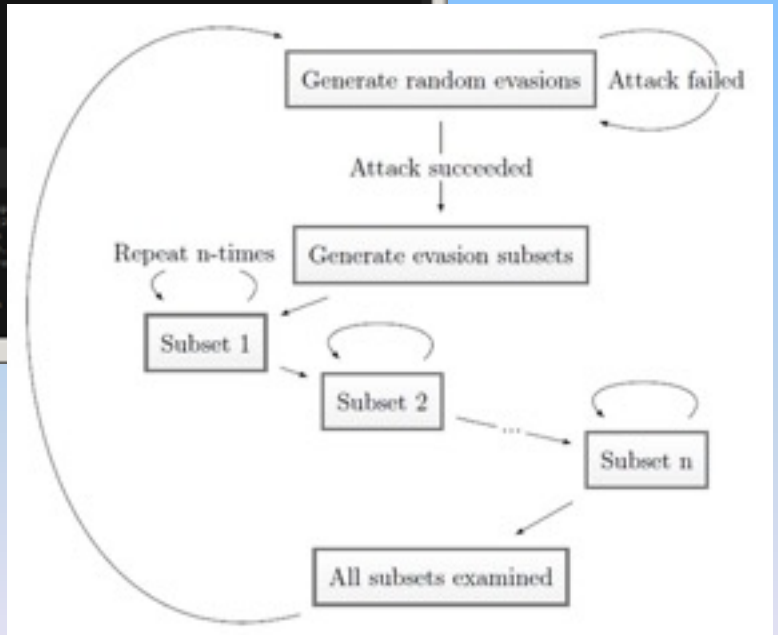
Figure 1.1: Intrusion Detection System works as a passive monitor of the network traffic

NOTTINGHAM TRENT UNIVERSITY

ISACA Trust in, and value from, information systems London Chapter

Firewall Evasion





Evader at work

STONESOFT

ISACA
Trust in, and value from, information systems
London Chapter

Socio-Economic Implications

One overall Society Wide implication is, by Socio-Economic Implication we (the Global Village) have embedded the environment of Internet dependencies into the very fabric of our lives – and Cloud *will* expand these dependencies.

Social, Business, Government, all of which are now entwined into the interconnected environment, the *Genie is Out*, and may not be placed back in the bottle.

Business Operations are highly dependent - Governments are highly reliant on Internet Operability. Socially be it from IP TV, VoIP, or even Home working, again dependency is high . . . . Making it, and us an ideal surface of Attack.

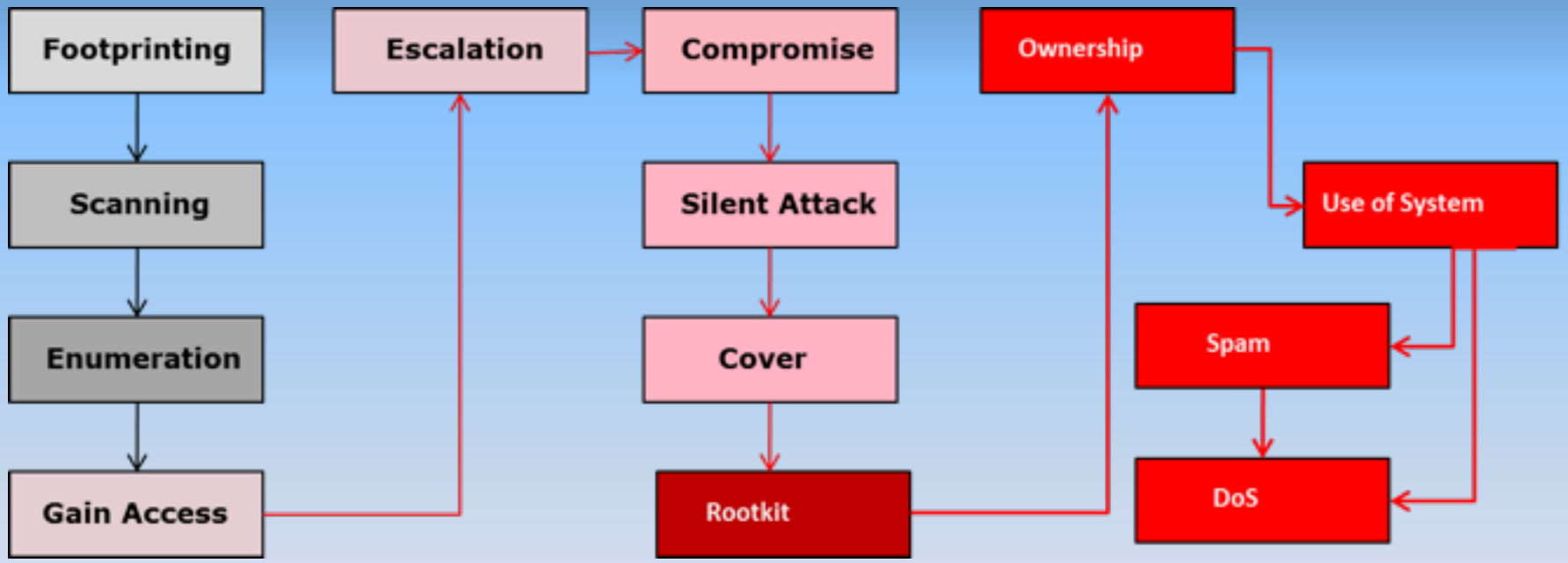
This dependency on an environment with no real Governance, Cross Boarder Control, or for that SLA, makes us significantly vulnerable, in the *Medium* to *Long Term* . . . and it WILL have consequences!

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Cyber Extortion – Anatomy of Attack

Distance Based Digital Forensics will be triggered by the manifestation of impact from *any one* of *many* variations of attack conditions – and Footprinting can also include eMail based Social Engineering.



Logs, Alerts, and Notifications should notify adverse conditions.

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Response - *DOING*

Upon engaging with an event classified as Distance Forensics (the Unknown) **DO**:

a) Triage the event - *trace*
b) Contain all Dynamic Artifacts (Logs, traces, events, eMail (including headers)
c) Conduct Intelligence Gathers from *known* facts, to reveal the *unknown* circumstance,
d) Taxonomy of the attack type (***e.g. below, Utube Page containing Malware***)
e) Investigate Logs/Service Desk Reports, and any other form of possible information
f) Confirm with other CSIRT Members their status – communicate the event for purpose of Situational Awareness

g) Document
h) Real-Time Threats Assessment
i) Monitor
j) Preserve Artifacts & Evidence
k) Assess need for Third Party Reporting – Law Enforcement Vice (CMA), DPA68, PCI-DSS, ISP etc
l) Consider Corporate Communications Position
m) Consider taking down impacted systems/or reducing their operability - Assess any Sprawl Conditions

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Response – *Do Not's*

Upon engaging with an event classified as Distance Forensics (the Unknown) **DO NOT**:

a) Engage with any adversarial actors
b) Disclose any Internal Information or Names/Numbers
c) Attempt any active logical connections – back to the attacker – it may provoke
d) Send any form of communications
e) Acknowledge any emails

Remembering:

a) Any contact provides an opportunity
b) Capitulation could result in further extortion or attempts to compromise
c) Compensations may attract adverse interest (ML, Press, other Hackers, or Hacktivist Group
d) interest to a Soft, willing Target
e) Exemplification on the Internet by Hacktivist of any communications etc

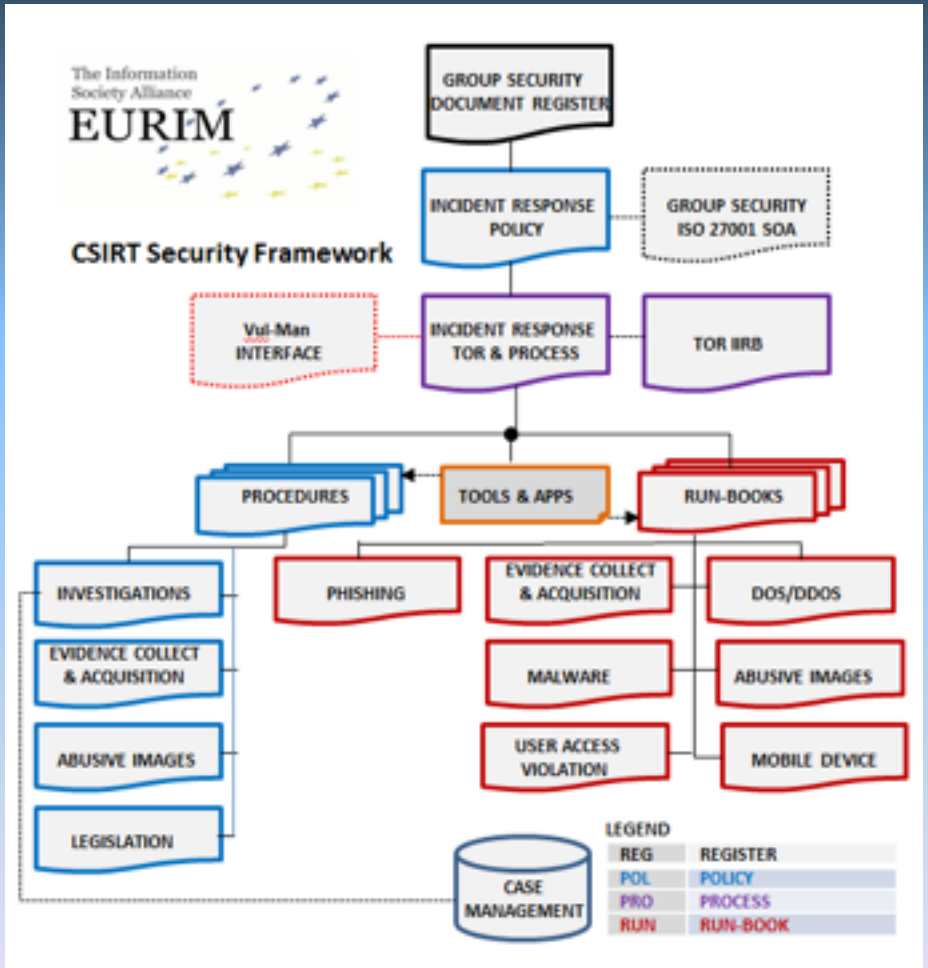
ISACA
Trust in, and value from, information systems
London Chapter

First Responders & CSIRT

There is a very real need to deploy a CSIRT, including:

a) **First Responder**
b) **GRC**
c) **Forensics**

It can be done a very low cost, and still Provision high end Operational capabilities



Based on:

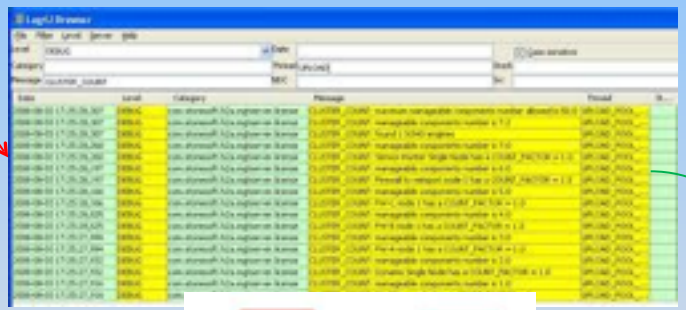
ISO 27001
ISO 27001
CoBIT 5.0

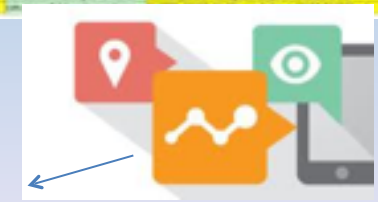
NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

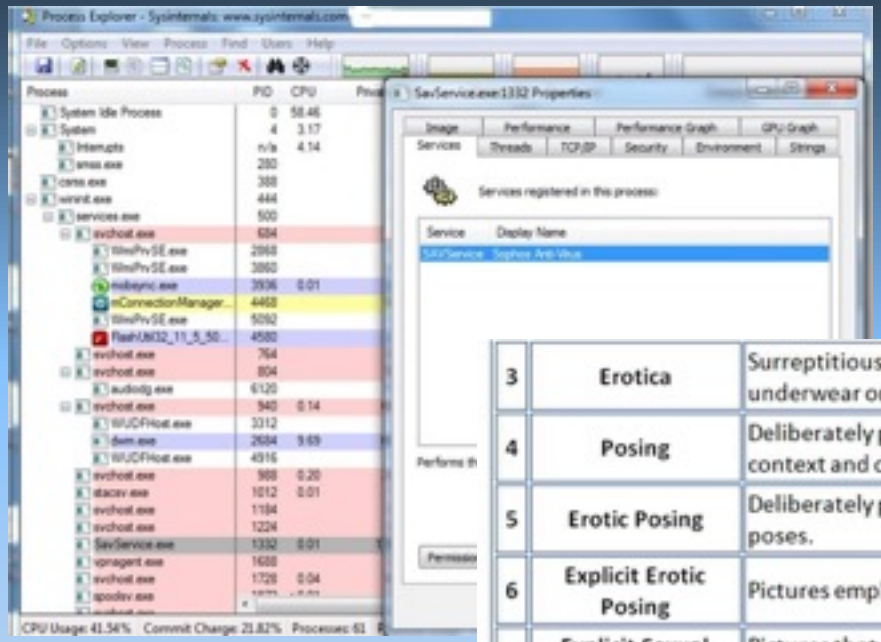
Global CSIRT Capabilities

A concept that could be a reality with the right level of interest.





Forensic Readiness - 1



GROUP SECURITY EVIDENCE COLLECTION & ACQUISITION POLICY

Client Group Security

09th January 2012

Version 0.1

3	Erotica	Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.
4	Posing	Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organisation suggests sexual interest).
5	Erotic Posing	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses.
6	Explicit Erotic Posing	Pictures emphasising genital areas, where the child is either naked, partially clothed or fully clothed.
7	Explicit Sexual Activity	Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.

nhtcu

Good Practice Guide for Computer based Electronic Evidence

Association of Chief Police Officers

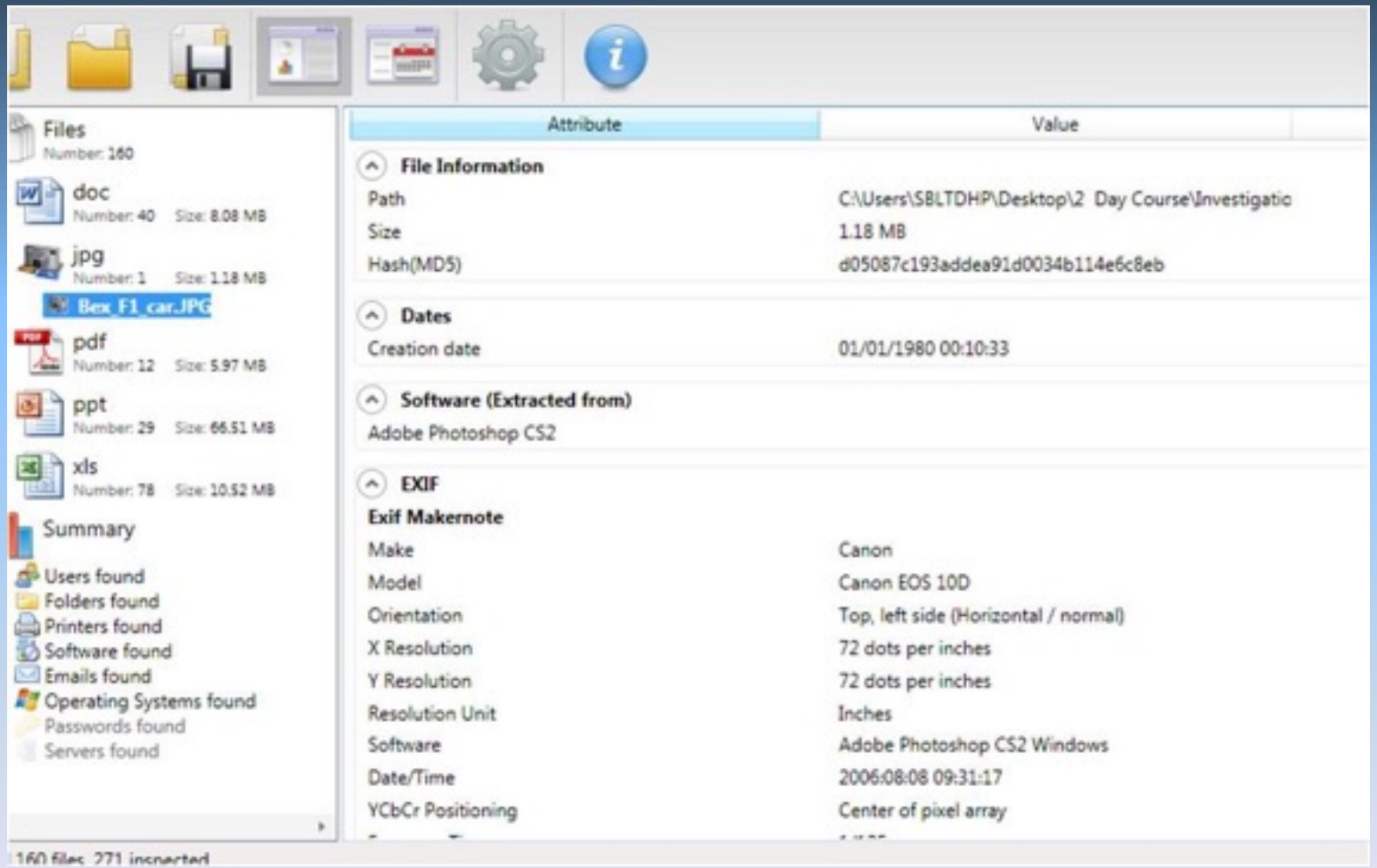
A.13.2.3	Collection of evidence	*Control* Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

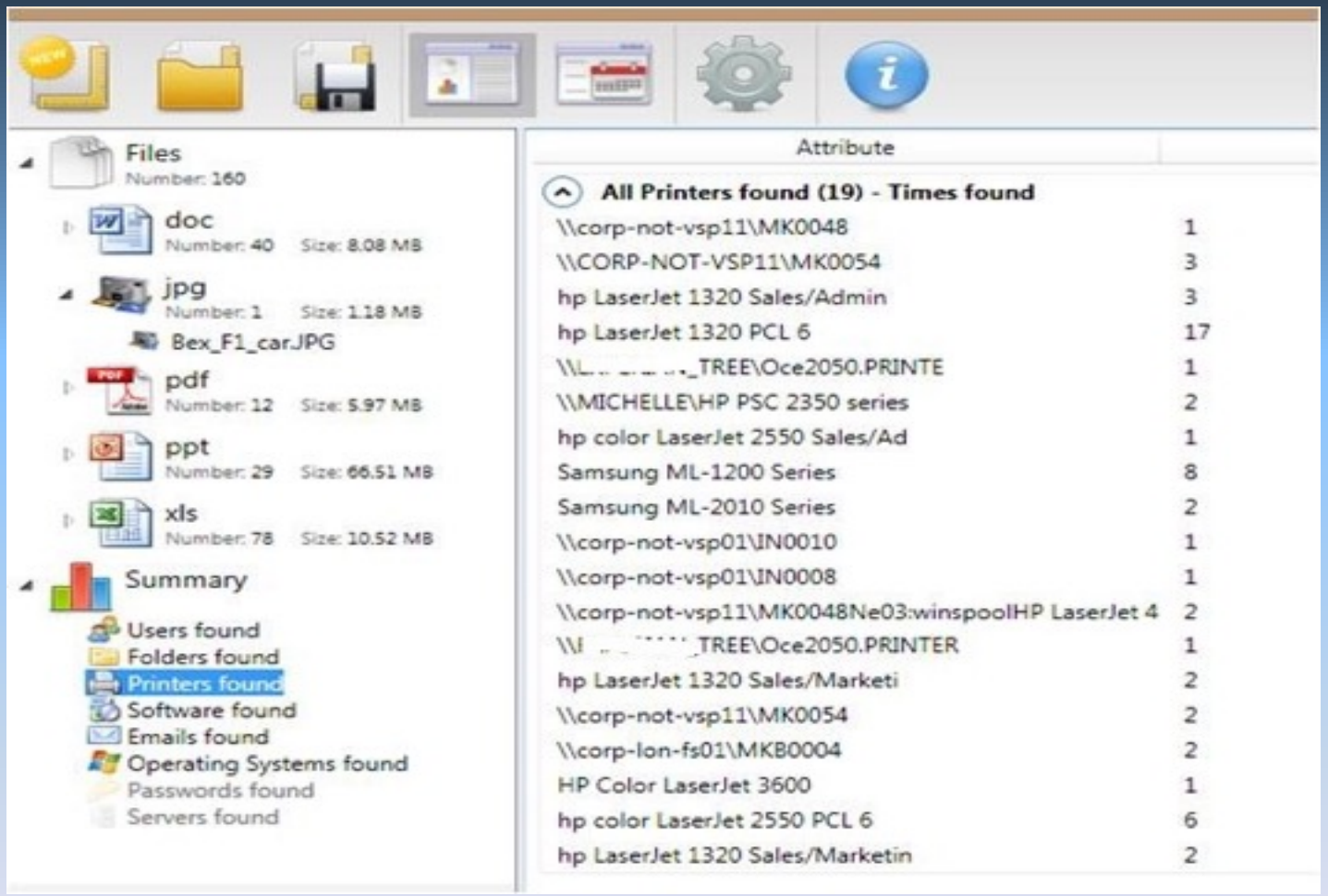
Forensic Readiness - 2



NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

Forensic Readiness - 4



NOTTINGHAM TRENT UNIVERSITY

ISACA London Chapter

AET Bibliography

[1] Stonesoft antievasion website:
http://aet.stonesoft.com/
[2] Department of defense standard internet protocol. RFC 760, January 1980: **http://tools.ietf.org/html/rfc760**
[3] DARPA internet program protocol specication. RFC 793, September 1981: **http://tools.ietf.org/html/rfc793**
[4] Architectural principles of the internet. RFC 1958, June 1996:
http://tools.ietf.org/html/rfc1958
[5] Sploit, a mutant exploit generator, 2006:
http://www.cs.ucsb.edu/~seclab/projects/sploit/
[6] Damballa discovers advanced evasion techniques being used by six crimeware families to carry out global cyber attacks, February 2012:
http://www.damballa.com/press/2012_02_28PR.php
[7] Stonesoft evader, July 2012:
http://evader.stonesoft.com/
[8] Allman, E. The robustness principle reconsidered. Queue 9, 6 (June 2011), 40:40{40:47.
[9] Balzarotti, D. Testing Network Intrusion Detection Systems. PhD thesis, Politecnico di Milano, 2006.
[10] Bidou, R. IPS shortcomings. In Black Hat US Proceedings (2006).

ISACA
Trust in, and value from, information systems
London Chapter

Thank you

Remember - There are Professionals and Organisations willing to help Combat the Threat – the problem is, *there is no take up of the extended hand!* But:

WE MUST ACT NOW

NOTTINGHAM TRENT UNIVERSITY

ISACA
Trust in, and value from, information systems
London Chapter