IBM Security
Intelligence. Integration. Expertise.

IBM

So You Think You May Have Been Compromised?

What you should do next…

Martin Overton
ERS Team Lead, Security Consultant, Ethical Hacker, Malware Specialist, Forensics, etc.
IBM ERS, CSAR

Video – You Don’t Want This to be YOU….

Organizations face four major challenges in operations around incident management

Assumption #1:	Assumption #2:	Assumption #3:
I am under attack right now.	**Attackers are already in.**	**No endpoint device is secure.**

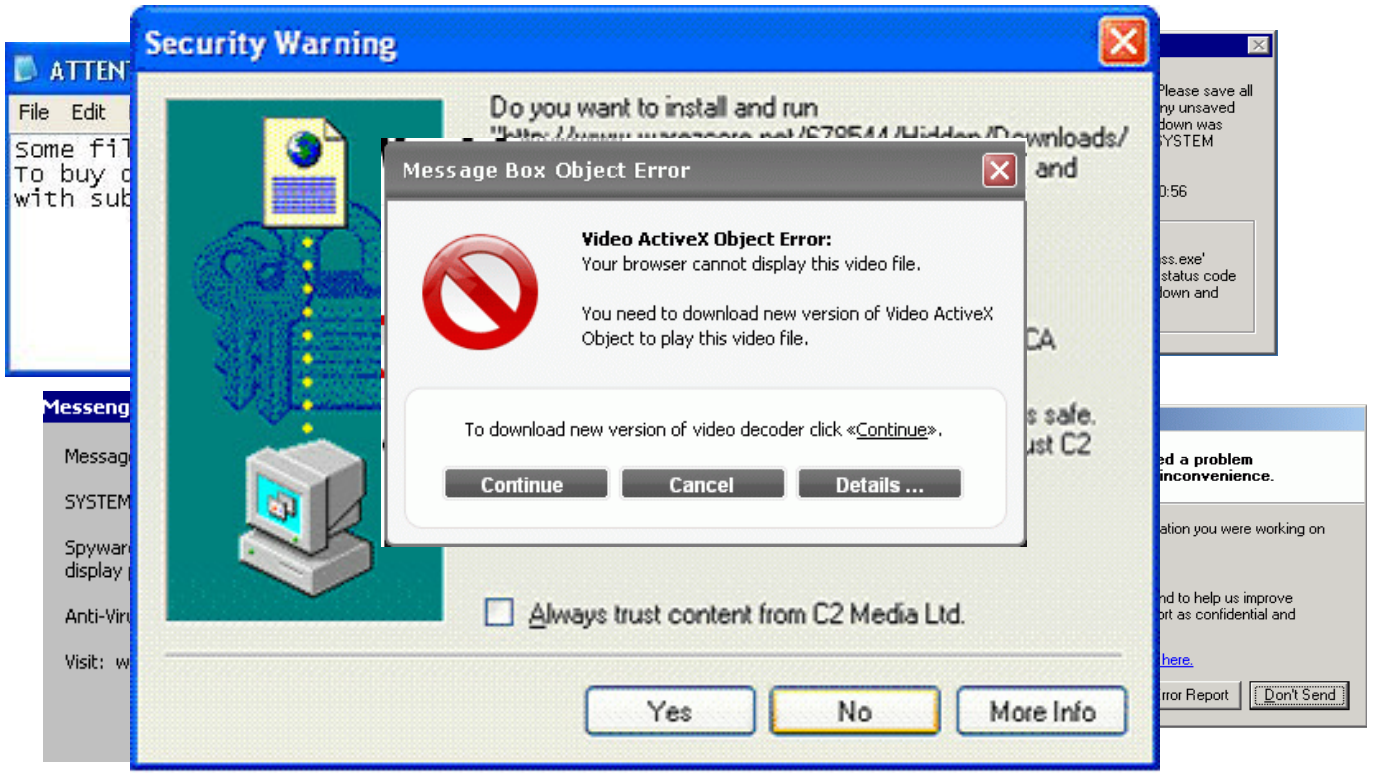
Organizations typically lack:

- ***Unified, cross-company policy and process for incident response***
- ***Actionable insight and information upon which to act***
- ***Incident management and forensic analysis tooling for remote system capture and analysis***
- ***Resources or skills to actively respond to and investigate security incidents***

"Information is the new worldwide currency. Every piece of data is valuable to someone, somewhere, somehow"

(IDC, Worldwide and U.S. Security Services Threat Intelligence 2011-2014 Forecast)

Error Messages Are Your Friends



Forensics

- Initial triage with system owner, and other interested parties.

- Full audit trail (log) of everything you have done, run, etc., including full time/date stamps.

- Follow order of volatility; memory, network, disk…
  - So you want to ideally dump the memory of the suspect system and analyse the dump using tools like Volatility*, HB Gary Responder, etc.
  - Then do a live disk image, and accept that some data will be lost or incomplete.
  - Now do a cold disk image, using dd, FTK Imager, or your preferred solution (just ensure it is a forensically sound image)

***Link to some nice Volatility malware analysis and tutorial videos**:
http://www.youtube.com/watch?v=zhQP07YKLL0
http://www.youtube.com/watch?fv=aGZ_GT-0l0U

What To Look For?

- ✓ New accounts created that you didn't authorise
- ✓ Existing accounts being used during non-business hours, non-working hours for that user's id, or from IPs/locations that are not expected
- ✓ Locked out accounts that you can't explain
- ✓ Access to protected/encrypted material or applications that the user has no right accessing, or attempting to access
- ✓ Data spikes (especially outbound) from systems:
  - ✓ Those that have sensitive or other valuable data
  - ✓ Those that do not normally make outbound connections
- ✓ Connections to/from IP addresses in countries that you do not do business with
- ✓ Connections to/from known botnet command and control systems or known bad (non-business related) domains or IPs

Wireshark - Win32/Sality.nar - DNS

No.	Time	Source	Destination	Protocol	Info
70	234.159163	192.168.11.11	80.77.240.31	DNS	Standard query A www.kjwre9fqwieluoi.info
71	234.564516	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
72	234.820249	192.168.11.11	80.77.240.31	DNS	Standard query A kukutrustnet777.info
73	235.182315	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
74	235.187219	192.168.11.11	80.77.240.31	DNS	Standard query A kjwre77638dfqwieuoi.info
75	235.228857	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
81	257.030097	192.168.11.11	80.77.240.31	DNS	Standard query A pzrk.ru
82	257.206096	80.77.240.31	192.168.11.11	DNS	Standard query response A 78.110.50.107
137	261.038559	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.bl.spamcop.net
138	261.065218	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
139	261.067704	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.bl.spamcop.net
140	261.302014	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
141	261.304526	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.cbl.abuseat.org
142	262.121206	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
143	262.125486	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.cbl.abuseat.org
145	262.161344	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
146	262.163908	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.list.dsbl.org
154	262.215000	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
156	262.222187	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.list.dsbl.org
157	262.234219	192.168.11.11	80.77.240.31	DNS	Standard query A egydom.com
158	262.253901	192.168.11.11	80.77.240.31	DNS	Standard query A www.yahoo.com
160	262.428410	80.77.240.31	192.168.11.11	DNS	Standard query response CNAME www.yahoo-ht3.akadns.net A 87.248.113.14
162	262.735509	80.77.240.31	192.168.11.11	DNS	Standard query response A 38.113.185.98
168	263.150719	192.168.11.11	80.77.240.31	DNS	Standard query A sosite_averi_sositeee.haha
169	263.218706	192.168.11.11	80.77.240.37	DNS	Standard query A 95.243.77.80.list.dsbl.org
171	263.554778	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name
172	263.557364	192.168.11.11	80.77.240.37	DNS	Standard query A 2.0.0.127.sbl-xbl.spamhaus.org
173	263.759509	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
175	263.964374	80.77.240.37	192.168.11.11	DNS	Standard query response A 127.0.0.2 A 127.0.0.4
176	263.966885	192.168.11.11	80.77.240.37	DNS	Standard query A 95.243.77.80.sbl-xbl.spamhaus.org
177	264.140534	192.168.11.11	80.77.240.37	DNS	Standard query A sosite_averi_sositeee.haha
179	264.142547	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name
181	264.145182	192.168.11.11	80.77.240.37	DNS	Standard query A 2.0.0.127.zen.spamhaus.org
182	264.164623	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name

What To Look For?

- ✓ Unusual amounts of malware detections, login failures, and IPS/IDS alerts for any system
- ✓ Unusual outbound connections on ports that you do not allow through your firewall
- ✓ Changes to your website/database content or links that you can't explain
- ✓ Files that have appear corrupted, especially office documents, spreadsheets, presentations, databases, graphics files and PDFs
- ✓ File size changes (unexpected), including system files, new software installs (unapproved), hacking tools, keygens, cracks, encryption tools, ftp or irc server or remote access tools (including commercial ones) not approved for company use.
- ✓ Attempts to delete or modify logs files, audit trails or hide files (applications or data), such as via Alternate Data Streams or marking them as hidden

Wireshark - Win32/Sality.nar - SMTP

No.	Time	Source	Destination	Protocol	Info
437	266.729739	192.168.11.11	72.232.11.26	TCP	cognex-insight > http [ACK] Seq=1 Ack=1 Win=65250 Len=0
439	266.934442	72.232.11.26	192.168.11.11	TCP	http > cognex-insight [ACK] Seq=1 Ack=133 Win=6432 Len=0
441	266.934881	72.232.11.26	192.168.11.11	TCP	http > cognex-insight [FIN, ACK] Seq=205 Ack=133 Win=6432 Len=0
442	266.935093	192.168.11.11	72.232.11.26	TCP	cognex-insight > http [ACK] Seq=133 Ack=206 Win=65046 Len=0
443	266.935393	192.168.11.11	72.232.11.26	TCP	cognex-insight > http [FIN, ACK] Seq=133 Ack=206 Win=65046 Len=0
444	267.138925	72.232.11.26	192.168.11.11	TCP	http > cognex-insight [ACK] Seq=206 Ack=134 Win=6432 Len=0
460	281.710469	192.168.11.11	216.39.53.3	TCP	gmrupdateserv > smtp [SYN] Seq=0 Win=64240 Len=0 MSS=1460
461	281.884354	216.39.53.3	192.168.11.11	TCP	smtp > gmrupdateserv [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1450
462	281.884703	192.168.11.11	216.39.53.3	TCP	gmrupdateserv > smtp [ACK] Seq=1 Ack=1 Win=65250 Len=0
463	281.886115	192.168.11.11	216.39.53.3	TCP	gmrupdateserv > smtp [FIN, ACK] Seq=1 Ack=1 Win=65250 Len=0
464	281.888062	192.168.11.11	195.24.77.223	TCP	bsquare-voip > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
465	281.934936	195.24.77.223	192.168.11.11	TCP	http > bsquare-voip [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1450
466	281.935147	192.168.11.11	195.24.77.223	TCP	bsquare-voip > http [ACK] Seq=1 Ack=1 Win=65250 Len=0
468	281.981802	195.24.77.223	192.168.11.11	TCP	http > bsquare-voip [ACK] Seq=1 Ack=176 Win=6432 Len=0
469	282.012776	216.39.53.3	192.168.11.11	TCP	smtp > gmrupdateserv [ACK] Seq=1 Ack=2 Win=65535 Len=0
471	282.025110	216.39.53.3	192.168.11.11	TCP	smtp > gmrupdateserv [FIN, ACK] Seq=137 Ack=2 Win=65535 Len=0
472	282.025214	192.168.11.11	216.39.53.3	TCP	gmrupdateserv > smtp [RST, ACK] Seq=2 Ack=137 Win=0 Len=0
473	282.026569	192.168.11.11	216.39.53.3	TCP	gmrupdateserv > smtp [RST] Seq=2 Win=0 Len=0
475	287.209554	195.24.77.223	192.168.11.11	TCP	http > bsquare-voip [FIN, ACK] Seq=191 Ack=176 Win=6432 Len=0
476	287.209774	192.168.11.11	195.24.77.223	TCP	bsquare-voip > http [ACK] Seq=176 Ack=192 Win=65060 Len=0
477	287.210184	192.168.11.11	195.24.77.223	TCP	bsquare-voip > http [FIN, ACK] Seq=176 Ack=192 Win=65060 Len=0
478	287.255717	195.24.77.223	192.168.11.11	TCP	http > bsquare-voip [ACK] Seq=192 Ack=177 Win=6432 Len=0

What Can You Do?

- ✓ Capture network traffic to help understand what is actually happening
- ✓ Investigate account creation, lockout and misuse
- ✓ Investigate all systems connecting to “bad” domains and IP addresses
- ✓ Investigate any corrupted files (check last modified and creation date, as that may be important)
- ✓ Make forensics copies of systems that you suspect are compromised; both memory and the whole physical disk (not just partitions), also capture the network connections active via Netstat –ano (or similar if not a Windows OS)
- ✓ Disconnect infected or possibly compromised systems from your network (either physically or by disabling the switch port); that includes disabling WiFi!
- ✓ Quarantine all suspect systems and removeable media that has been used in them
- ✓ Boot from a RescueCD (assuming you don’t have whole disk encryption) and run tools to check for known malware, rootkits, bootkits, and other security risks from read-only media (CD/DVD or USB thumbdrive that has a write-protect switch enabled).

Wireshark - Win32/Sality.nar - HTTP

No.	Time	Source	Destination	Protocol	Info
86	257.408508	192.168.11.11	78.110.50.107	HTTP	GET /img/logoh.gif?32ae9c=23250500 HTTP/1.1
96	257.596138	78.110.50.107	192.168.11.11	HTTP	HTTP/1.0 200 OK
103	259.787076	192.168.11.11	78.110.50.107	HTTP	GET /img/logos.gif?32b90b=16620855 HTTP/1.1
113	259.972191	78.110.50.107	192.168.11.11	HTTP	HTTP/1.0 200 OK
120	260.758789	192.168.11.11	195.24.77.223	HTTP	GET /utest/manna.txt?32baf0 HTTP/1.1
122	260.806410	195.24.77.223	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/plain)
130	260.858603	192.168.11.11	195.24.77.223	HTTP	GET /utest/ip.php HTTP/1.1
132	260.907392	195.24.77.223	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/html)
149	262.168587	192.168.11.11	89.149.227.194	HTTP	GET /tratata5/?32c281=29939337 HTTP/1.1
151	262.214015	89.149.227.194	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/html)
166	262.941670	192.168.11.11	38.113.185.98	HTTP	GET /logod.gif?32c2df=29940183 HTTP/1.1
167	263.145463	38.113.185.98	192.168.11.11	HTTP	HTTP/1.1 404 Not Found (text/html)
202	265.461658	192.168.11.11	87.248.113.14	HTTP	GET /?3326640 HTTP/1.1
214	265.588940	87.248.113.14	192.168.11.11	HTTP	HTTP/1.1 302 Found (text/html)
223	265.694747	192.168.11.11	217.146.186.51	HTTP	GET /?p=us HTTP/1.1
309	265.969402	217.146.186.51	192.168.11.11	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
311	265.972357	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
313	265.974811	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
315	265.976901	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
317	265.979722	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
319	265.981334	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic

Key Incident Response Steps

- The following is a guide for customers, but it is useful to understand the basic steps involved.

- Preparation:
  - Gather and learn the necessary tools, become familiar with the environment.
- Identification:
  - Detect the incident, determine its scope, and involve the appropriate parties.
- Containment:
  - Contain the incident to minimize its effect on neighboring IT resources.
- Eradication:
  - Eliminate compromise artifacts, if necessary, on the path to recovery.
- Recovery:
  - Restore the system to normal operations, possibly via reinstall or backup.
- Wrap-up:
  - Document the incident's details, retail collected data, and discuss lessons learned.

First Thoughts…

- During an incident, especially a critical one, is not the time to decide who should be involved and what role they should play. Responsibilities need to be clearly defined, written and rehearsed. Only then can you hope for an efficient and effective handling of an incident…It is also not an excuse for a witch hunt or the blame game.

- **This is not news to a security professional, but it may serve as an excellent example to management as to why drills should be run that include Human Resources, Information Technology, Legal, Management and Security Team personnel?**

What Do You Need Help With?

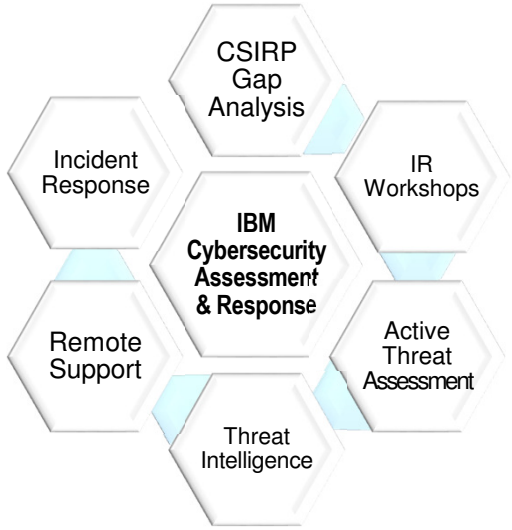
- Unless you have in-house forensics skills:
  - Get advice from an expert in this area
  - Do not try and fix it yourself as you will damage, modify or erase valuable evidence
- Have an initial Triage call with them:
  - Explain what you have seen and what if anything you have captured/secured
  - Explain what actions you have taken
  - Explain what your concerns are
  - Explain what your goals and deliverables are
  - Listen to the advice given and act on it
  - Decide based on the advice given, what the next steps should be and whether you want full assistance going forward to fully understand, recover and put in place solutions that will improve your security posture
  - If a criminal act has been committed you may need to inform any suitable regulatory bodies and/or local law enforcement

How Can You Detect?

- Use a multi-layered or defence in depth approach to security monitoring:
  - Multiple anti-malware defences (with multiple detection engines at the perimeter; email, ftp, web and scan SSL traffic!)
  - IDS/IPS systems properly tuned to match your infrastructure and minimise false positives
  - Regular reviews of logs; event logs, syslog, firewall, proxy, anti-malware, etc. Or even better use a SIEM to aggregate and analyse the logs as this may identify attackers/bad traffic patterns that you may otherwise miss
  - End-point security, deploy suitable levels dependant on the users access rights to your “crown jewels” or other key systems, processes or data. This is not just deploying anti-malware, it could include white-listing, IPS, behavioural analysis, change detection, anti-fraud tools, etc.
  - Do not just rely on tools, you need skilled staff to manage, acknowledge alerts and take relevant action. There is no silver-bullet!

Best Practices: Ensure you have access to the resources and tools needed to respond quickly to the inevitable incident

- Clients should consider retaining expert security consultants prior to an incident. This ensures guaranteed access to **resources**, **knowledge** of your environment, and **predictable response** times.
- As an example, IBM's Emergency Response Service Subscription includes:
  - •Initial one-day workshop for **incident planning**
  - •**120 staff hours** per year, which can be utilized remotely or on site at the client's discretion for emergency response services or preventative services
    We can perform these preemptive incident preparation services at the beginning or any given time during the subscription:
    - **Active threat assessment**
    - **Cyber Security Incident Response Program gap assessment**
    - **Incident response training and simulated exercise**
  - •**Unlimited** emergency declarations
  - •**Two seats** on the X-Force Threat Analysis Service
  - •**Quarterly** check point, remote support, and update on threat landscape



ERS Hotline

Have an emergency? Call IBM ERS 24x7x365

(US) 1-888-241-9812

(WW) 1-312-212-8034

Emergency response services – Subscription delivery model

IBM

Emergency Response Service (ERS)

Subscription ONLY benefits (1,2,3 & 5)

Ad-hoc only gets benefit 4 at a higher cost than subscription customers

1

Kick-off workshop:

Conduct a one-day initial planning workshop to gather information, review current incident response plan and process for making a declaration, discuss mock scenario of responding to an incident and exchanging incident data.

2

Preemptive and readiness activities:

Utilizing part of the subscription hours, provide gap assessment or development of a CSIRP. Perform tabletop / simulated incident response scenario walkthrough and conduct active threat assessment to uncover existing hidden threats.

3

Ongoing checkpoint and incident assistance:

Ongoing checkpoints and threat review will be conducted throughout the subscription on a monthly basis. An assigned incident case manager / lead analyst will be available for incident related advice and assistance.

4

Emergency incident support:

IBM ERS stands by 24x7x365 to provide immediate response to an emergency declaration. The emergency incident is report via contacting the ERS hotline or the assigned case manager, who will provide the initial triage.

5

Predictive and actionable threat intelligence:

Access to IBM X-Force Threat Analysis Service (XFTAS) that evaluates global online threat conditions and provides analysis for proactive security management.

IBM Cybersecurity Incident Response Planning Service

Avoid Common CSIRP[1] mistakes to build a plan that works

At least 50 percent of the CSIRPs evaluated by IBM security consultants show no evidence of a formal document lifecycle or a history of continual revisions.

Having an incident response plan in place saved U.S. organizations on average USD1.2 million per data breach in 2013.

- **An incident response plan is the foundation** on which all incident response and recovery activities are based:
  - ✓ It provides a **framework** for effectively responding to any number of potential incidents
  - ✓ It specifically defines the organization, **roles and responsibilities** of the computer security incident response ream (CSIRT)
  - ✓ It should have criteria to assist an organization determine **types and priorities** of each security incident
  - ✓ It defines **escalation and communication procedures** to management, executive, legal, law enforcement, and media depending on incident conditions and severity
  - ✓ It must be **regularly updated and fully tested** via dry runs

CSIRP Review and Gap Assessment

CSIRP Development

Incident Mock Tests and Table Top Exercise

IBM Active Threat Assessment (ATA)

IBM Cybersecurity Assessment and Response
IBM Active Threat Assessment (ATA)

Coordinated Attack Simulation
Targeted penetration testing helps identify vulnerable systems and applications from an attacker's perspective, conducted with broad coverage or using a customized and simulated events. An on-site coordinator assists with validating that detection mechanisms are successfully detecting malicious activity.

Tool based APT Forensic Scanning
Checks for the presence of behavioral Indicators of Compromise (IOCs) frequently seen with intrusions indicating a currently active but previously unknown compromise.

Memory (RAM) Analysis
For systems identified with suspicious activity, a remote memory (RAM, volatile data) analysis may be done looking for common malware traits.

System Log Analysis
Logs from firewalls, IDS/IPS devices, Network AV servers, DNS and other systems can help reveal IOCs of an intruder or the presence of malware.

Critical Controls Review
Assessment of the level of implementation of SANS Top 20 Critical Security Controls helps to develop an overall security strategy.

Think of the ERS subscription service as being like an insurance policy….

Peace of mind knowing that you are covered…When things go wrong, IBM are there to help…

•The IBM ERS Service

Ad-Hoc

Call one number and help will be offered:

- 24/7 365 even <u>without</u> an existing contract
- Initial Triage call with ERS specialists within an hour
- Understand the attack/incident and suggest first steps (to do and not to do)
- Remote and/or on-site assistance
- 0 hours of consultant time included
- Skilled and experienced ERS specialists when and where you need them…

40 Hours Subscription

- Call one number and help will be offered: 24/7 365
- Initial Triage call with ERS specialists within an hour
- Understand the attack/incident and suggest first steps (to do and not to do)
- Remote and/or on-site assistance
- 40 hours of consultant time included
- On-site or remote kick-off meeting with the customer to understand what they really need. *Crown-Jewels, Previous Incidents and Pain Points*
- Two XFTAS seats (up to the minute threat data and advisories) tailored to the customers needs.
- Unused hours by the 4th Quarter can be used for other services, such as CSIRP, Malware Defence Reviews, GAP analysis and mock scenarios, etc.
- Skilled and experienced ERS specialists when and where you need them…

120 Hours Subscription

- Call one number and help will be offered: 24/7 365
- Initial Triage call with ERS specialists within an hour
- Understand the attack/incident and suggest first steps (to do and not to do)
- Remote and/or on-site assistance
- 120 hours of consultant time included
- On-site or remote kick-off meeting with the customer to understand what they really need. *Crown-Jewels, Previous Incidents and Pain Points*
- Two XFTAS seats (up to the minute threat data and advisories) tailored to the customers needs.
- Unused hours by the 4th Quarter can be used for other services, such as CSIRP, Malware Defence Reviews, GAP analysis and mock scenarios, etc.
- Skilled and experienced ERS specialists when and where you need them…

No matter if you've been hacked, DDoSed, infected, or suffered some other security breach, or even <u>think</u> you might have!

Summary - What NOT to do?

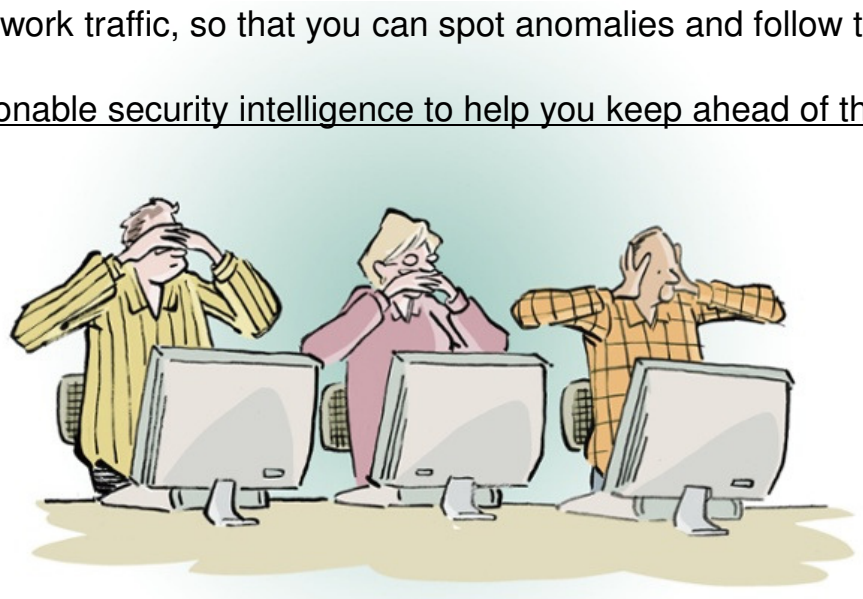
- You DON'T have to make the same mistakes. It is not compulsory ;-)
- It isn't IF you get compromised, it is when, as it will happen!
- Have an Incident Response Plan and test it (regularly), otherwise it will be headless chicken mode.
- If you haven't got incident response and forensics skills in-house, buy in the skills (from us!) ;-)
- You shouldn't try to fix the problems themselves as they may damage valuable evidence or at least make it harder for the forensics team to identify it.
- Forensics isn't easy, it takes time, be patient.

Source: http://finextra.com/video/video.aspx?videoid=662&topic=retail

Summary - What to do?

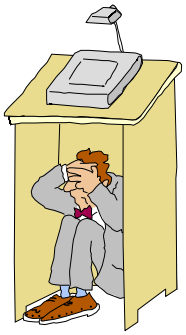
- Carry out regular penetration tests, or at least vulnerability scans (they are NOT the same thing!) Test web sites that are Internet facing (including beyond authentication).
- Follow industry best practice, patch as quickly as you can (or use some form of virtual patching or mitigation technology)
- Make sure that passwords are changed regularly (and that they are complex). Don't forget to revoke access for leavers (even more important when shared account credentials are used; which is NOT good!)
- Ensure that staff are adequately trained and that simple security policies and procedures are in place.
- Encrypt data wherever possible to help minimise the risk if it does get stolen.
- Analyse your logs (firewall, proxy, endpoint, etc.), act on alerts, use SIEM and/or use dedicated staff to do the analysis
- Baseline your "normal" network traffic, so that you can spot anomalies and follow them up

- Be risk aware and get actionable security intelligence to help you keep ahead of the threat!



Video – Be One of These….

Questions?



?

Contact Details:

Martin Overton

Phone: +44 (0)2392 563442

Email: overtonm@uk.ibm.com

Twitter: @martin_sec

also on LinkedIn, FaceBook, Xing

Lots of conference papers here: http://momusings.com/papers

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM

IBM **Security**

Intelligence. Integration. Expertise.