Cyber threats: hiding in plain sight

Andrea Simmons, *FBCS CITP, CISM, CISSP, MA, M.Inst.ISP, Senior Member ISSA*

Managing Consultant, www.i3grc.co.uk

PhD Candidate in Information Assurance, thesis complete

Director, Institute of Information Security Professionals (IISP)

Member, BCS Security Community of Expertise

What are we talking about?

cy•ber•threat
/ˈsībərˌTHret/

noun

1. the possibility of a malicious attempt to damage or disrupt a computer network or system (source: Oxford Dictionaries)

2. any type of malicious activity or actor that leverages computers and networks to adversely impact other computers and networks, to include everything from well-known forms of malware (e.g., viruses, worms, and Trojans) to malicious insiders and targeted attacks (source: CyberEdge Group)

Organisation sponsors:

So just threats then....

- Disruption, death from disruption anticipated by 2017
- **Connectivity**
- **Crime**
- Tech rejectionists create **chaos**
- **Complexity** (conceals fragility)
- Dangerous infrastructure dependence
- Weaponized vulnerabilities (already seen this)
- Legacy technology crumbles (95% of ATMs in the US run Windows XP.....)
- **Complacency** (includes international border threats – and ongoing impact from data breaches
- **Consolidation** endangers competition

Source: http://www.cio.com/article/2898037/security0/9-biggest-information-security-threats-for-the-next-two-years.html#slide13

Organisation sponsors:

We are not entirely blind...

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

Donald Rumsfeld

Read more at http://www.brainyquote.com/quotes/quotes/d/donaldrums148142.html#XqXsJRRh364iCpHK.99

Organisation sponsors:

Cyber Trust and Crime Prevention

The Foresight project on Cyber Trust & Crime Prevention launched its findings on 10th **June 2004**. http://www.bis.gov.uk/foresight/our-work/projects/published-projects/cyber-trust

Organisation sponsors:

ESR DUBLIN 2015

Top 20 Controls

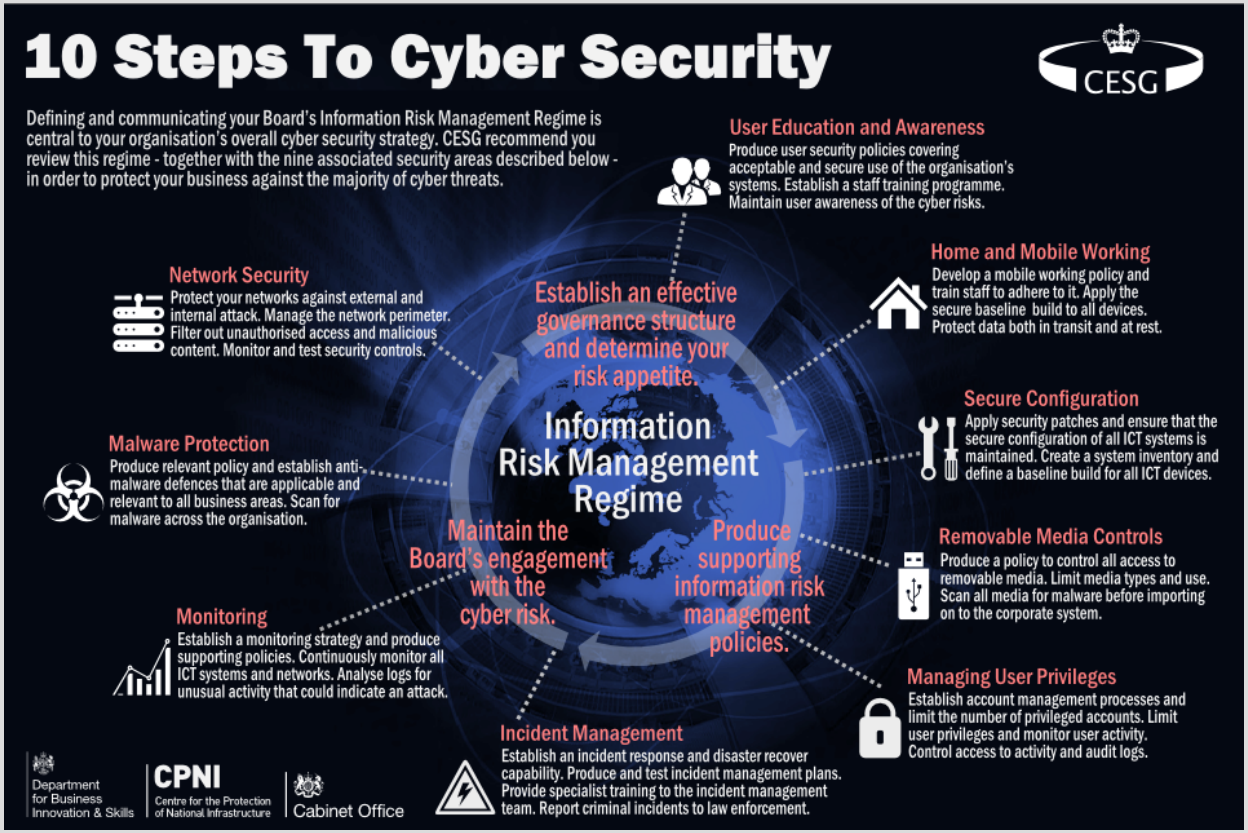
They were the Critical Controls before they were "for Effective Cyber Defense".... It's all in the marketing

http://www.cpni.gov.uk/advice/cyber

Organisation sponsors:

NSAI · saadian YOUR INFORMATION - OUR INNOVATION · FutureAnalytics Planning + Research + Economics · UNINOVA · TFC · q-validus · NEN

Then came...



CYBER ESSENTIALS PLUS

Source: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

Organisation sponsors:

NSAI saadian FutureAnalytics Planning + Research + Economics UNINOVA TFC q-validus NEN

Current security posture

- ☑ 70% of respondents are spending greater than 5% of their IT budgets on security.
- ☑ 71% were affected by a successful cyberattack in 2014, but only 52% expect to fall victim again in 2015.
- ☑ For the second consecutive year, mobile devices (smartphones and tablets) are perceived as IT security's weakest link, closely followed by social media applications.
- ☑ Security analytics is the top-ranked network security technology planned for acquisition in 2015, followed by threat intelligence and next-generation firewalls.
- ☑ Nearly a third lack tools to inspect SSL-encrypted traffic for cyberthreats.
- ☑ Containerization/micro-virtualization technology is the top-ranked endpoint security and second-ranked mobile security technology planned for acquisition in 2015.
- ☑ Only 23% of respondents are confident their organizations have made adequate investments to monitor the activities of privileged users.

Source: 2015 CyberThreat Defense Report, North America & Europe, Cyber Edge Group research

Organisation sponsors:

Perceptions and concerns

- ☑ Phishing, malware, and zero-days give IT security the most headaches.
- ☑ 59% of respondents experienced an increase in mobile threats over the past year.
- ☑ Inadvertent exposure of confidential data is the top concern with SaaS-based file sharing applications.
- ☑ Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by lack of security budget.
- ☑ Nearly two-thirds of security professionals view SDN as having a positive impact on their ability to defend against cyberthreats.

Source: 2015 CyberThreat Defense Report, North America & Europe, Cyber Edge Group research

Organisation sponsors:

Attack surface reduction

- ☑ Network access control (NAC) remains the top technology for reducing a network's attack surface.
- ☑ Less than 40% of organizations conduct full-network active vulnerability scans more than once per quarter.
- ☑ Only 20% of IT security professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks.

Source: 2015 CyberThreat Defense Report, North America & Europe, Cyber Edge Group research

Organisation sponsors:

Black swan – how rare, really?

Our response should be simple…"we are not afraid", as we have the practices and technology necessary to blunt these types of attacks

Organisation sponsors:

Cyber in the news…

- The car industry is already impacted by issues with the safety of the driverless systems (Chrysler)– and then there's the "deceipt devices" (VW and…..)
- Clinton email server – 8 Oct 2015
  http://www.foxnews.com/politics/2015/10/08/clinton-email-server-reportedly-target-cyberattacks-from-china-south-korea/
- US OPM government data breach impacted 22.1 million
  http://edition.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/
- Ashley Madison breach proves hackers can and *will* take away your CEO's job – 38 million individual records impacted
  http://recode.net/2015/08/30/ashley-madison-breach-proves-hackers-can-and-will-take-away-your-ceos-job/
- Sony attack – "unparalleled and well planned crime" – Head of Entertainment, Amy Pascal lost her job, blamed on North Korea
  http://uk.businessinsider.com/hacking-experts-call-sony-cyber-attack-unparalleled-and-well-planned-crime-2014-12?r=US&IR=T
- South Korean banks and broadcasters
  - http://www.telegraph.co.uk/technology/internet-security/9943388/Cyber-warfare-more-must-be-done.html
  - http://www.slideshare.net/moriyachi/cyber-attack-on-south-korean-2013323-02
- North Korea – hacking warriors being trained
  - http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors-trained-teams_n_2943907.html
- China IP address link to South Korea attack
  - http://www.bbc.co.uk/news/world-asia-21873017

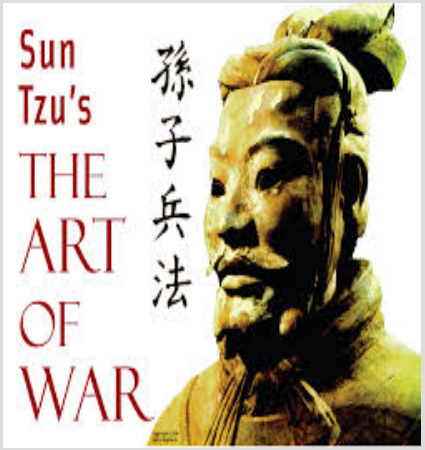
Organisation sponsors:

And now we have....

Organisation sponsors:

Cyber is NOT new

1. Physical Security
2. Communications Security (COMSEC) [40s]
3. Operational Security (OPSEC) [50s]
4. Automated Data Processing Security [60s]
5. Computer Security (COMPUSEC) [90s]
6. IT Security (ITSEC) [90s]
7. Information Systems Security (INFOSEC) [90s]
   - Merged COMSEC and COMPUSEC following rapid change in technology
   - Combined in a new paradigm to become INFOSEC, internationally recognised in Common Criteria
8. Information Assurance [00s]
9. Cyber – in the media..... [10s]



3000 BC

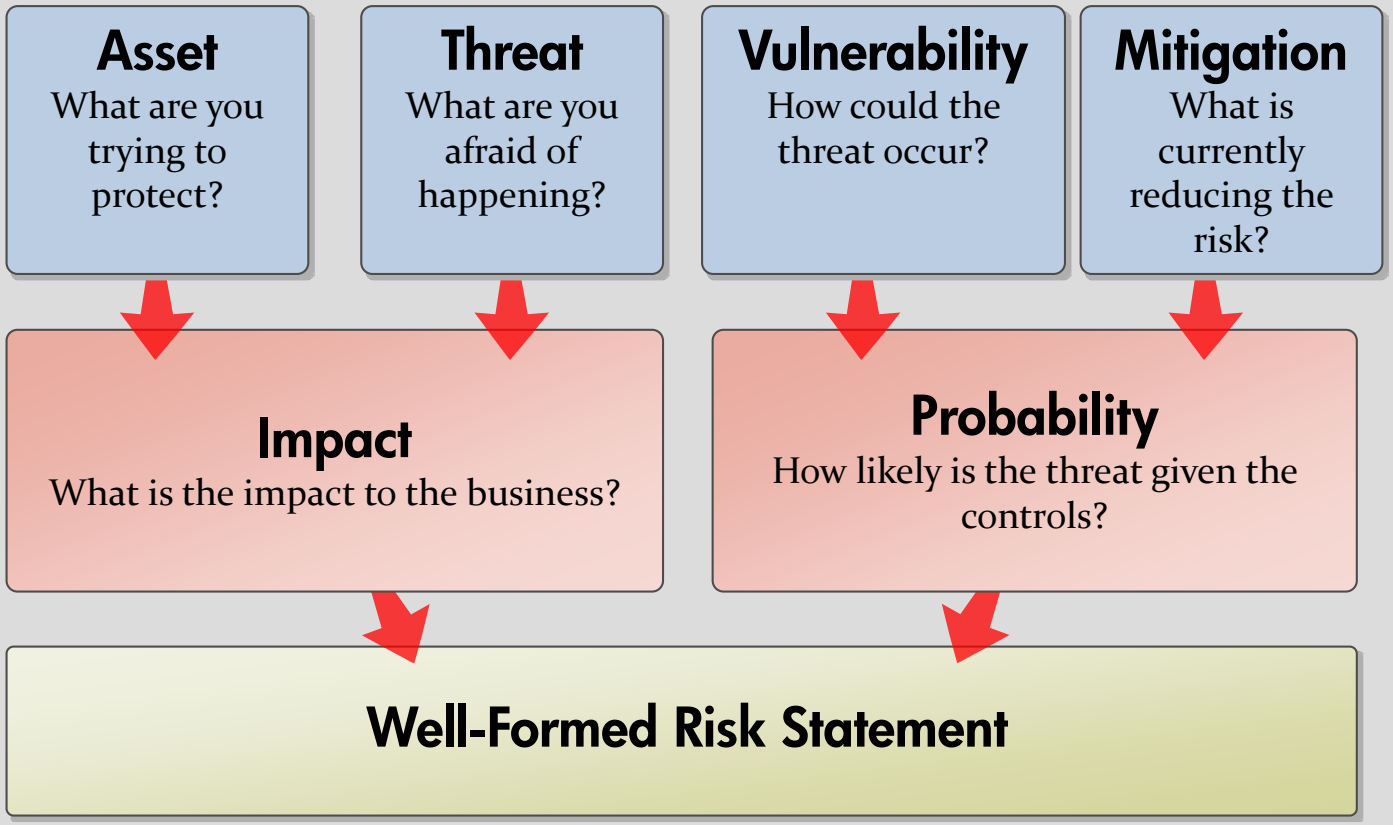
Organisation sponsors:

The Library of Babel

- Enshrines all information
- Yet no knowledge can be discovered there precisely because all knowledge *is* there
- Shelved side by side with all falsehood

Jorge Luis Borges, 1941

Cyber is only *one* element of a *bigger* picture



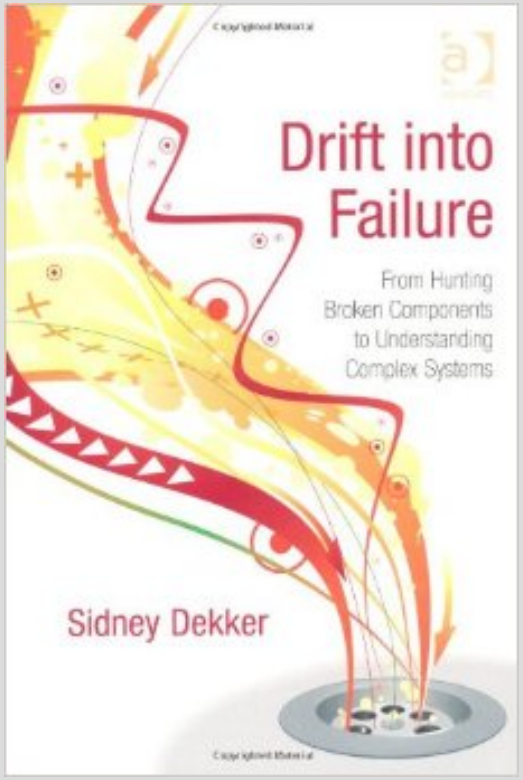
Organisation sponsors:

Still not designing in security

- **Design and build**. Consider compliance and privacy requirements; design security features; develop use cases and abuse cases; complete attack surface analysis; conduct threat modelling; follow secure coding standards; use secure libraries and use the security features of application frameworks and languages.
- **Test**. Use dynamic analysis (DAST), static analysis (SAST), interactive application security testing (IAST), fuzzing, code reviews, pen testing, bug bounty programs and secure component life-cycle management.
- **Fix**. Conduct vulnerability remediation, root cause analysis, web application firewalls (WAF) and virtual patching and runtime application self-protection (RASP).
- **Govern**. Insist on oversight and risk management; secure SDLC practices, metrics and reporting; vulnerability management; secure coding training; and managing third-party software risk.

Source: 2015 State of Application Security: Closing the Gap

Normalizing the deviance



Organisation sponsors:

Turn the problem…

- Cyber Security
- Skills crisis
- Volumes of data
- Lack of security intelligence
- Inattentional blindness – when we focus on one thing, we miss another

Source: **Pink Bat Thinking** http://play.simpletruths.com/movie/pink-bat/?cm_mmc=CheetahMail-_MO-_-10.10.11-_-TPODmovie&utm_source=CheetahMail&utm_campaign=TPODmovie

Organisation sponsors:

…into a solution

- Frameworks are available – they need to be properly utilised
- Actionable Intelligence – the next "big" thing – need to "mine" your log data to work out what's going on
- Unseen solutions – being created with ease

Source: **Pink Bat Thinking** http://play.simpletruths.com/movie/pink-bat/?cm_mmc=CheetahMail-_MO-_-10.10.11-_-TPODmovie&utm_source=CheetahMail&utm_campaign=TPODmovie

Organisation sponsors:

Cyber Hygiene

- Unpatched and out of date machines put us all at risk
- Hygiene as a meme (memetics) - an idea, behavior or style that spreads from person to person within a culture
- Semiotics - the study of signs and sign processes (semiosis), likeness, analogy, metaphor, symbolism, signification, and communication.
- Me centric vs us centric / Free riding vs common good
- Check out: http://www.zdnet.com/10-security-best-practice-guidelines-for-consumers-7000012171/
- Getsafeonline, Cyber Awareness Month (Oct) and yet 123456 was the top password for thousands of Ashley Madison site members.....
- Maybe CSI:Cyber will be the tipping point in public awareness?

Organisation sponsors:

Collective self deception

To die for an idea; it is unquestionably noble.

But how much nobler it would be if men died for ideas that were true!

H.L. Mencken

The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge.

Prof Stephen Hawking

Organisation sponsors:

Organisation sponsors:

Thank you

- Andrea C. Simmons, CISSP, CISM, FBCS CITP, M.Inst.ISP, MA

- *Email*: andrea.simmons@bcs.org
- *LinkedIn:* *www.linkedin.com/in/andreasimmons*
- *Mobile*: +44 7961 508775
- *Land*: +44 1905 356268

Organisation sponsors:

Speaker profile

- **Andrea Simmons** **FBCS CITP CISM CISSP MA M.Inst.ISP**

  Andrea brings more than 17 years direct information security, assurance and governance experience, helping clients establish appropriate controls and achieving and maintaining security certifications. Andrea's most recent role as ***Chief Information Security Officer*** for ***HP Enterprise Security*** was one of worldwide influence addressing Security Policy and Risk Governance seeking to support and evidence the delivery of organisational assurance across a wide portfolio of clients and services. Her work has included development of a patentable enterprise governance, risk & compliance (eGRC) approach to addressing business information governance needs. Andrea has returned to independent consultancy to take forward i3GRC™.

- **Achievements**

  Author of ***Achieving Best Practice in Public Sector Information Security***, Ark Group Publishing, ISBN 978-1-906355-39-5, published December 2008

  Author of ***Once more unto the Breach – Managing Information Security in an Uncertain World***, ISBN: 9781849283885, first published Spring 2012, updated and revised December 2014 http://www.itgovernance.co.uk/products/3901

  Fellow of the BCS, Chartered Institute for IT - http://www.bcs.org/blogs/security and member of the *Security Community of Expertise*

  Management Committee Member of the Information Assurance Advisory Council, http://www.iaac.org.uk/

  Director of the Institute of Information Security Professionals, https://www.iisp.org/imis15/

  Senior Member of the ISSA, http://www.issa.org/

  ISACA member, http://www.isaca.org/

  Volunteer delivering Safe and Secure Online programs to UK schools for ISC2, https://www.isc2.org/

Organisation sponsors:

Backup

Organisation sponsors:

NSAI saadian FutureAnalytics Planning + Research + Economics UNINOVA T F C q-validus NEN

The premise (1)

- There is less of a "cyber skills crisis" and more of an "understanding crisis".
- We need less of the cyber-waffle and bring us back to the basics in a strongly impassioned plea.
- "cyber" requires a full and detailed understanding of the basics; basics that still hold true as first principles and *must* be learned in the same way as learning that Tuesday follows Monday, or "30 days hath September, April, June and November".....

The premise (2)

- Worshipping at the foot of all things "cyber" (it was "cloud“ before then…and we’ve got “big data”) is proving to be a distraction that is taking us off course from succeeding at our necessary information protection endeavours
- Building security in across both the software design landscape and the infrastructure architecture, to ensuring board level understanding – is what we should be focusing on – Actually… it’s what we’ve been focusing on for **15 years so far** ….. So where are we going wrong?

People, Process, Technology

The dynamics are changing….

"Security is 10% product and 90% process" – Bruce Schneier

- Security needs physical, technical and administrative controls to be in place
- Security is about embedding a framework approach incorporating people, process and technology
- Security is about protecting your data from harm from natural disasters, from man-made attacks, and from technical problems.

Controls defined

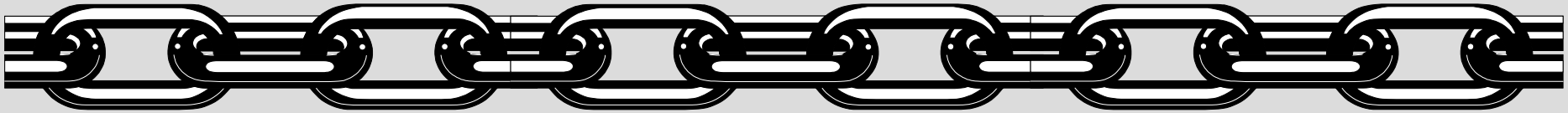
- Preventive controls ("before the fact") – The most important control type since, if 100% effective (which it never is), none of the others would be necessary – physical barriers, passwords, etc.
- Detective controls ("after the fact") - If a preventive mechanism fails, this is the first type of control necessary to identify the facts prior to correction – audit trails, monitoring, etc.
- Corrective controls ("before or after the fact") - designed to correct a problem once identified – change control, overrides, etc.
- Compliance controls ("enforcing the fact") - designed to keep you inside the law and your Chief Executive Officer out of jail – observing data protection laws, avoiding libel, etc.
- Deterrent controls ("instead of the fact") - designed to advise against certain forms of action - security policy, logon warning, etc.

(Palmer, 2011)

Information Security Programs

Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

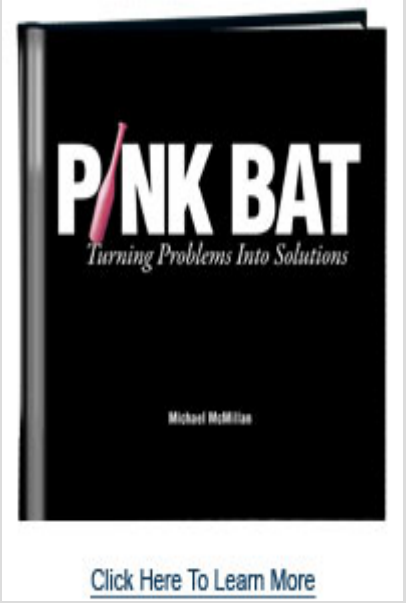


Adversaries attack the weakest link…where is yours?

Organisation sponsors:

Pink Bat Thinking

- Pink bat thinking required
- Turn the problem into the solution.....
- http://play.simpletruths.com/movie/pink-bat/?cm_mmc=CheetahMail-_MO-_-10.10.11-_-TPODmovie&utm_source=CheetahMail&utm_campaign=TPODmovie



Organisation sponsors: