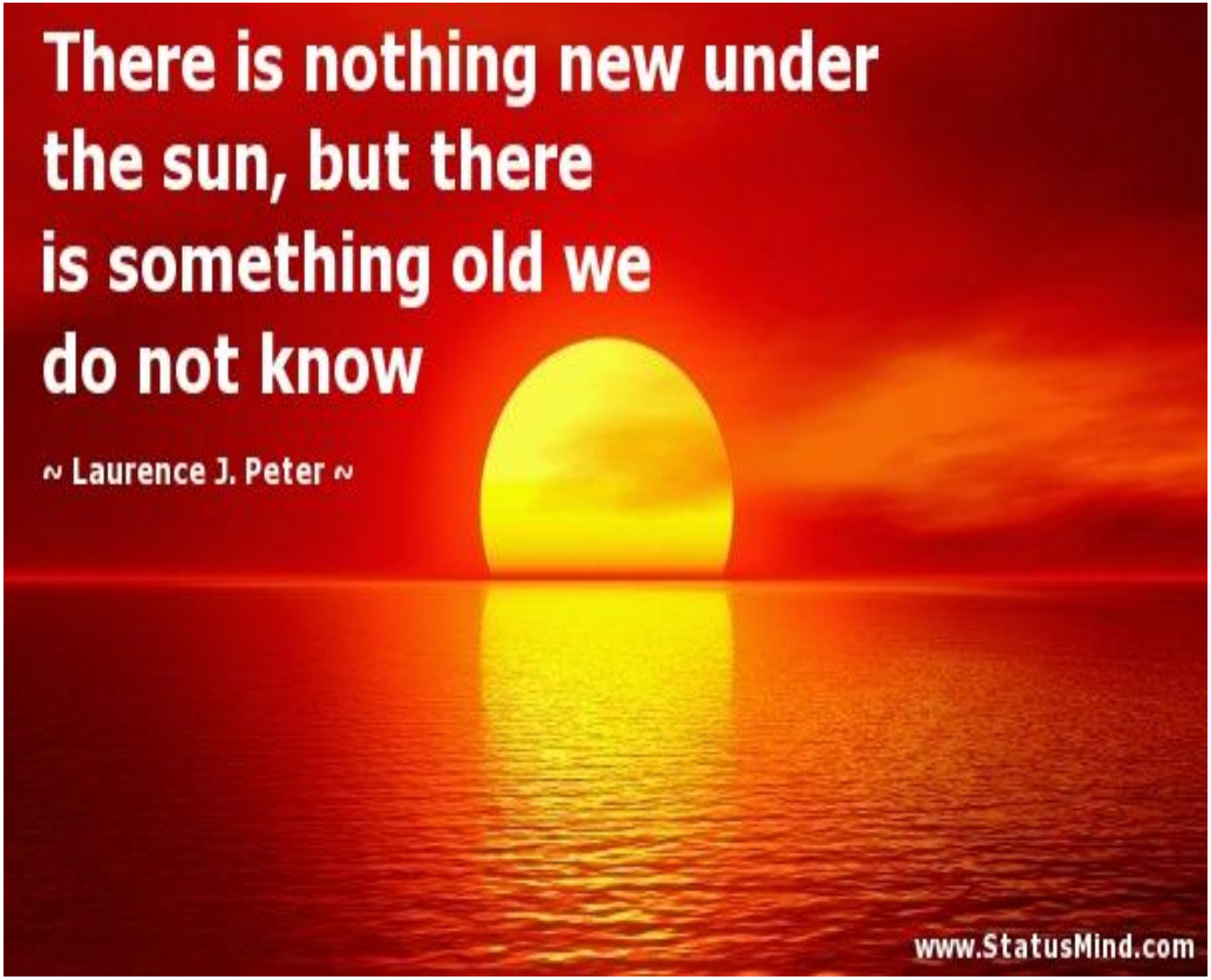
There is nothing new under the sun

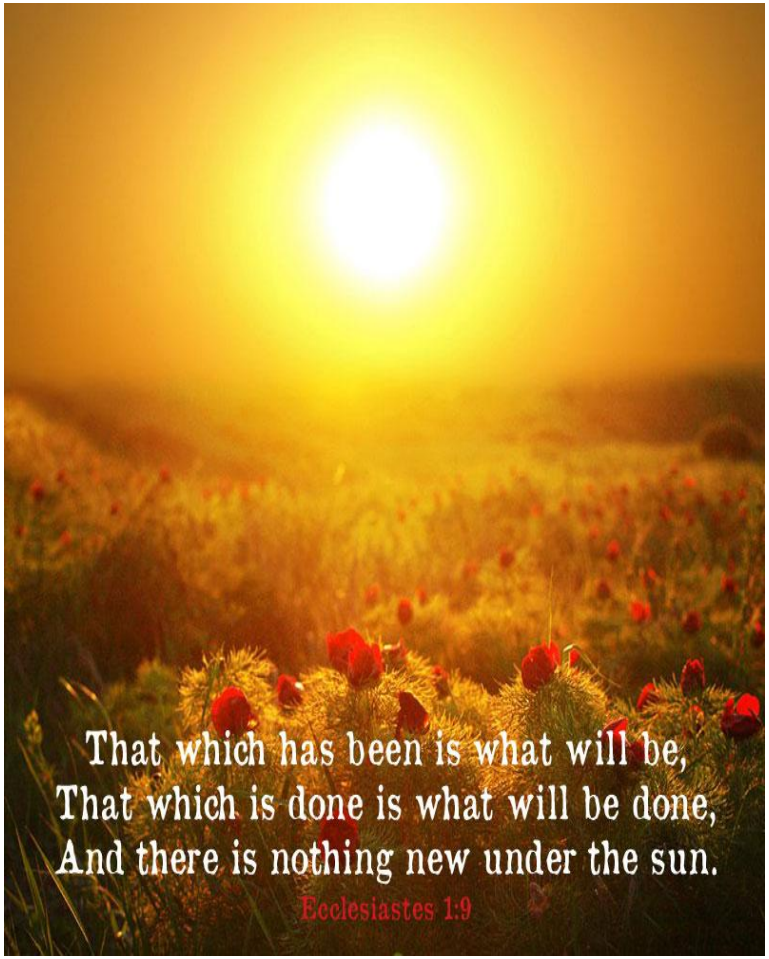
Avoid the panic: we can plan for new regulation and cyber-attacks

Presented on: 23rd March 2016

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



nihil sub sole novum



Read: http://www.tripwire.com/state-of-security/security-awareness/there-is-nothing-new-under-the-sun/

Small Business Reputation & The Cyber Risk

KEY POINTS

Cyber security was cited as one of their top concerns by less than a quarter of small businesses

23%

yet it is fast becoming the only way to do business:

83%

of consumers surveyed are concerned about which businesses have access to their data and

58%

said that a breach would discourage them from using a business in the future.

Recently published KPMG Supply Chain research supports this;[2]

94%

of procurement managers say that cyber security standards are important when awarding a project to an SME supplier and

86%

would consider removing a supplier from their roster due to a breach.

UK small businesses value their reputation as one of their key assets. Yet they are hugely underestimating the likelihood of a cyber breach happening to them and its long term impact:

60%

of small businesses surveyed have experienced a cyber breach, but only

29%

of those who haven't experienced a breach cited potential reputational damage as an 'important' consideration.

The impact of a cyber breach can be huge and long lasting.

89%

of the small businesses surveyed who have experienced a breach said it impacted on their reputation. Those who experienced a breach said the attack led to:

31% Brand damage

30% Loss of clients

29% Ability to win new business

Quality of service is also a risk. Those surveyed who experienced a cyber breach found it caused customer delays

26%

and impacted the business' ability to operate

93%

Source: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

History matters

Cyber is not *new* …

Sources: http://blog.oxforddictionaries.com/2015/03/cyborgs-cyberspace-csi-cyber/ and http://www.itgovernance.co.uk/blog/weekly-podcast-why-you-cant-ignore-information-security-in-2016/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2016-01-19&kmi=andreasimmons%40tiscali.co.uk

- Late **1940s** – **cybernetics** - concerned with the study of communication and control systems in living beings and machines
- **1960s** onwards – cyber temporary or nonce words – **cyborg** being the most memorable
- **1966** – **cybermen**, Dr Who
- **1972** - **Cyborg**, novel by Martin Caidin – which inspired ***The Six Million Dollar Man*** and ***The Bionic Woman***
- **1982** – **cyberspace** appeared – coined by William Gibson in his science fiction novella Burning Chrome (guess what that must have spurred?!). Cyberspace is defined as the "notional environment within which electronic communication (esp. via the internet) occurs." [OED]
- **1990s** – peak of popularity of *cyberspace* to refer broadly to the world of electronic communications (including the Internet)
- **1990s-2000s** – saw the rise of e- everything, supplanting previous *cyber* formations – i.e. e-commerce, not cyber-commerce. During this time, cyber took on the more negative formations- *cyberwar, cyber attack, cybercrime, cyberterrorism and cyberbullying*
- **2010** – ***Cyberwar***, Richard Clarke
- And from then on the data breaches have escalated in scale, audacity and impact…but we're becoming inured ☹
- **2015** - **487,731,758** leaked records, including infamously Ashley Madison and TalkTalk! 80% of companies had a security incident in 2015 [Source: www.infosecurity-magazine.com/news/80-companies-had-a-security/]

Did you see it?!

Frameworks / Timelines / Semantics

Earlier

- Physical Security
- Communications Security (COMSEC) [40s]
- Operational Security (OPSEC) [50s]
- Automated Data Processing Security [60s]
- Cyber men [60s]

1990….

- Computer Security (COMPUSEC)
- IT Security (ITSEC)
- Information Systems Security (INFOSEC)
  - Merged COMSEC and COMPUSEC following rapid change in technology
  - Combined in a new paradigm to become **INFOSEC**, internationally recognised in Common Criteria

2000…

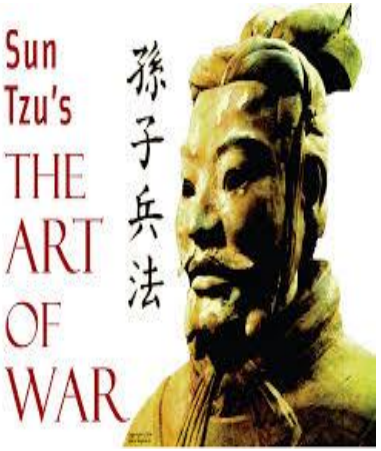
- 2002 UK NHS IG Toolkit
- UK IA Strategy
- 1st UK Cyber Security Strategy

2010…

- Cyber Security in the media
- Information Protection
- **i3GRC™**

Future…

- **INFOSEC - Information Security**
- **IA - Information Assurance**
- **IG - Information Governance**



3000 BC

It’s a journey, not a destination...wider context

- 2001 – **Convention on Cybercrime** – signed by the Council of Europe, more countries than the EU – including Canada, Japan, the United States, and South Africa on 23 November 2001, in Budapest. As of July 2015, the non–Council of Europe states that have ratified the treaty are Australia, Canada, Dominican Republic, Japan, Mauritius, Panama, Sri Lanka, and the United States.
- 2002 – January – Bill Gates sent an infamous email establishing the Trustworthy Computing (TwC) initiative [TCI]
- 2007/8 - Serial breaches of information / data security; multiple government reports providing advice and guidance [ACS Published book 1 on Public Sector InfoSec]
- 2009 - Publication of National **Cyber Security** Strategy
- 2009 - Publication of **Digital Britain** [ACS wrote a Chapter in a book on Resilience]
- 2009 - BYOD
- 2010 – Raw data now….
- 2011 – the rise of the **Cloud**
- 2012 – **Wikileaks** and **3D printing** [ACS Published book 2 on Managing Security]
- 2013 – **Big Data** and **Snowden**
- 2013 – Network Information Security (NIS) Directive initially proposed
- 2014 – TCI closed and staff redistributed ☹
- 2014 – **Hybrid** Cloud and **Smart** machines [ACS Edited book 2 for reprint in 2015]
- March 2015 – creation of **i3GRC™**
- 2015 – **WYOD**
- October 2015 – Schrems sues Facebook; Safe Harbor thrown out
- December 2015 – National Information Security (**NIS**) Directive; Global Data Protection Regulation (**GDPR**)

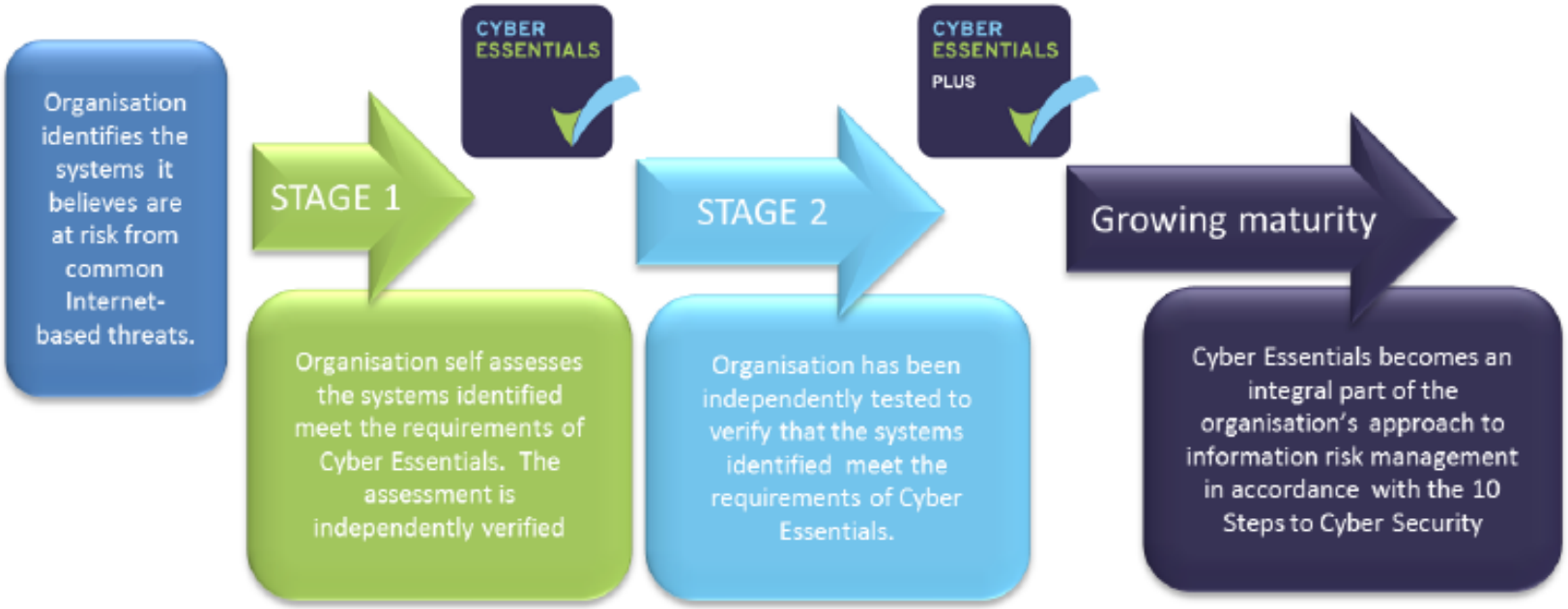
Cyber Trust and Crime Prevention

Wheel built

The Foresight project, carried out in 2003, 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

Cyber Essentials – and existing basics

Cyber Essentials - Scheme Overview

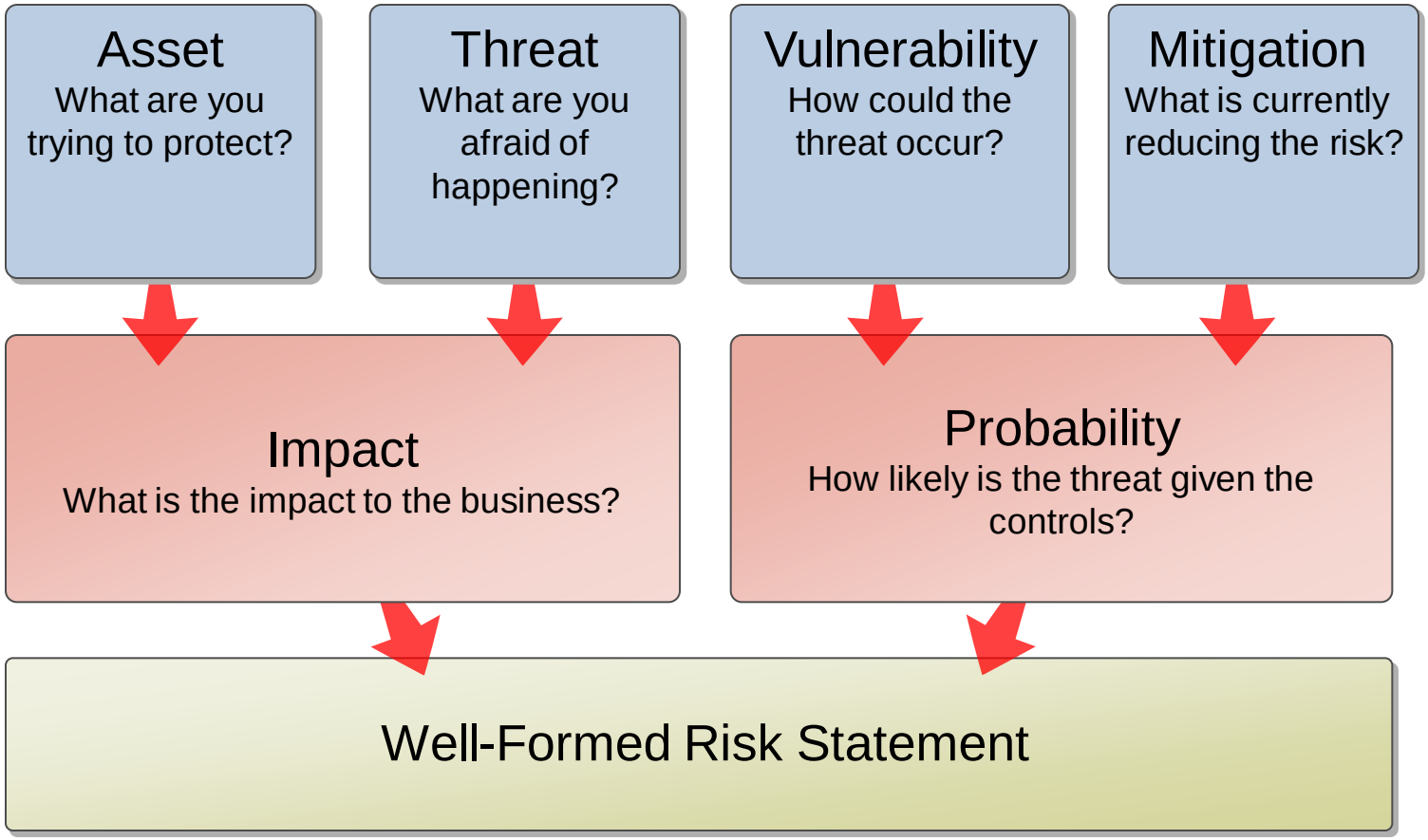


Source: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

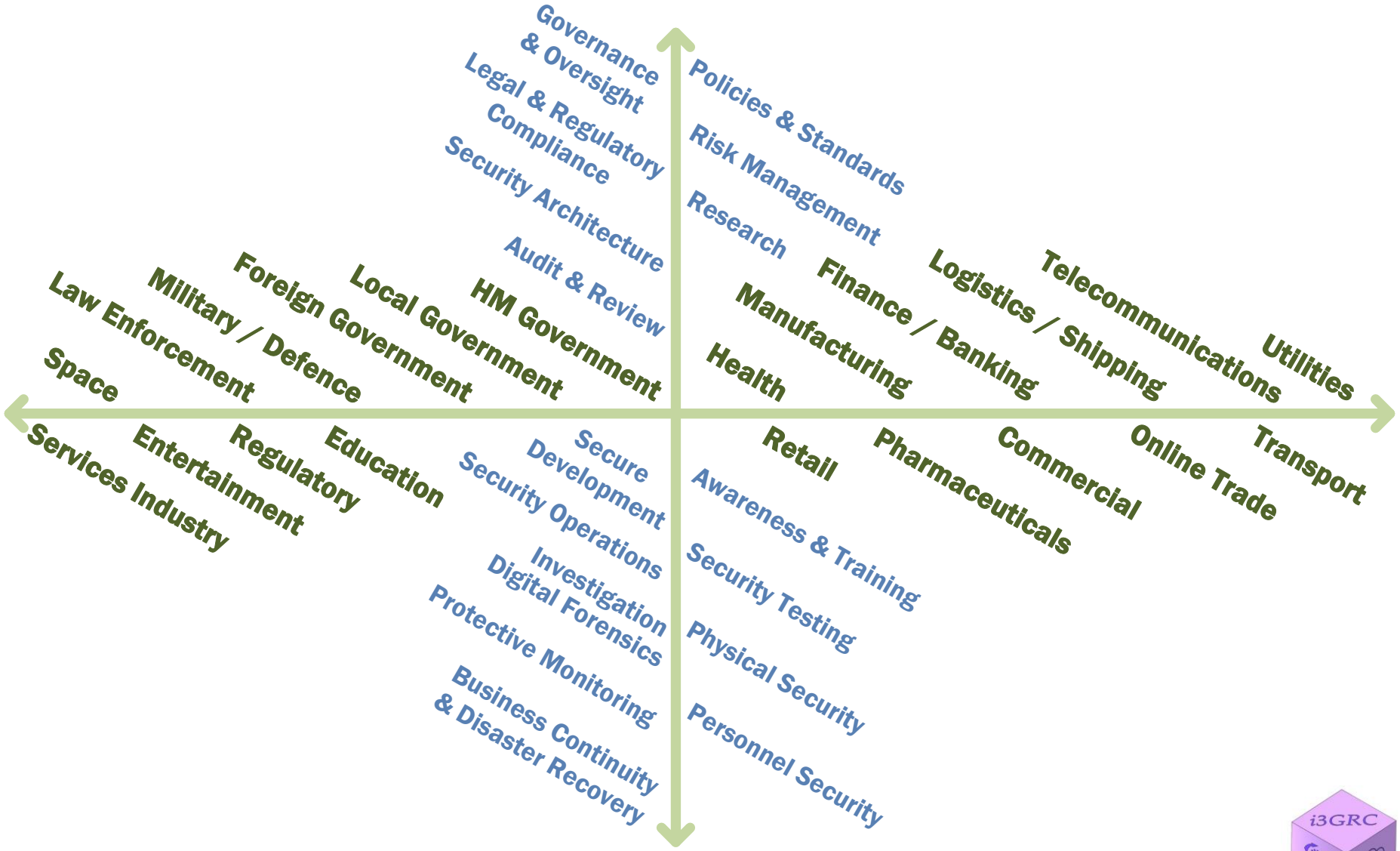
Cyber Essentials – 5 key areas

1. **Boundary firewalls and internet gateways** - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
2. **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organisation.
3. **Access control** – Ensuring only those who should have access to systems to have access and at the appropriate level.
4. **Malware protection** – ensuring that virus and malware protection is installed and is it up to date.
5. **Patch management** – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.

Cyber Security is only ONE element of a BIG picture

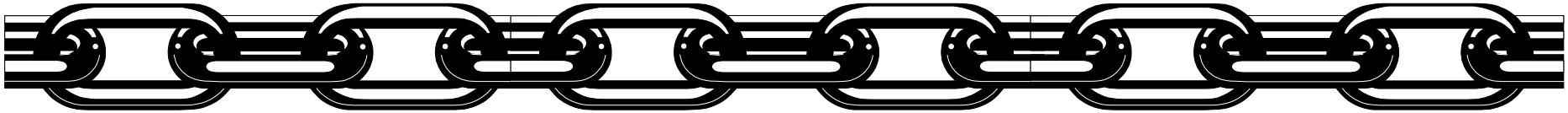


Just *part* of a bigger picture



Information Security Programs

Wheel built



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?

20 Critical Security Controls

for Effective Cyber Defense

The 20 Critical Controls enable cost-effective computer and network defense, making the process measurable, scalable, and reliable throughout the U.S. government, in the defense industrial base, and in other organizations that have important information and systems to protect. It is based on actual threats. The controls were selected by a consensus of the major U.S. government organizations that defend against cyber attacks as the controls that are most critical for stopping known attacks. Only one other security framework is based on threat – The Strategies to Mitigate Targeted Cyber Intrusions published by the Australian Defence Signals Directorate – which are also presented here.

The 20 Critical Controls prioritize the less threat-related catalog of guidelines published by the U.S. National Institutes of Standards and Technology (NIST) in Special Publication 800-53.

This poster offers a snapshot of the purpose and main features of each of the 20 Critical Controls, shows the NSA ratings of each control based on how well it accomplishes attack mitigation, where it fits in the overall hierarchy of required controls, and the level of technical maturity that has been reach in implementing the control. The poster also maps the 20 Critical Controls to the Australian Defence Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions and the NIST Special Publication 800-53, Revision 3, Priority 1 Controls.

You'll find the up-to-date 20 Critical Controls, Version 3 document posted at: www.sans.org/critical-security-controls

And the Strategies to Mitigate Targeted Cyber Intrusions posted at: www.dsd.gov.au/infosec/top35mitigationstrategies.htm

UK Centre for the Protection of National Infrastructure (CPNI) is developing advice to support the 20 Critical Controls: www.cpni.gov.uk/advice/infosec

NSA's Attack Mitigation View Of The 20 Critical Controls

The National Security Agency categorized the 20 Critical Controls both by their attack mitigation impact and by their importance.

Categories of Attack Mitigation

ADVERSARY ACTIONS TO ATTACK A NETWORK

Reconnaissance	Get In	Stay In	Exploit
Hardware Inventory (CAG 1)	Secure Configuration (CAG 1)	Audit Monitoring (CAG 14)	Security Skills & Training (CAG 9)
Software Inventory (CAG 2)	Secure Configuration (CAG 10)	Boundary Defense (CAG 13)	Data Recovery (CAG 8)
Continuous Vuln Access (CAG 4)	Application SW Security (CAG 6)	Admin Privileges (CAG 12)	Data Loss Prevention (CAG 17)
Networking Engineering (CAG 19)	Wireless (CAG 7)	Controlled Access (CAG 15)	Incident Response (CAG 18)
Penetration Testing (CAG 20)	Malware Defense (CAG 5)	Penetration Testing (CAG 20)	
	Limit Ports/PS (CAG 11)		

STOP ATTACKS EARLY — STOP MANY ATTACKS — MITIGATE IMPACT OF ATTACKS

Ranking in Importance: In order for a critical control to be a priority, it must provide a direct defense against attacks. Controls that mitigate: known attacks; a wide variety of attacks; attacks early in the compromise cycle; and the impact of a successful attack will have priority over other controls. Special consideration will be given to controls that help mitigate attacks that we haven't discovered yet.

- **VERY HIGH** – These controls address operational conditions that are actively targeted and exploited by all threats.
- **HIGH** – These controls address known initial entry points for targeted attacks.
- **MEDIUM** – These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.
- **LOW** – These controls are about optimizing, validating, and/or effectively managing controls.

Proof Of Value In Automating The 20 Critical Controls

Automating the critical controls provides daily, authoritative data on the readiness of computers to withstand attack as well as prioritized action lists for system administrators to maintain high levels of security. At the same time, it eliminates the massive financial waste associated with thick audit reports that are out-of-date long before they are published.

But such claims need proof.

At the US State Department, we see the first agency-wide implementation of automated security monitoring with unitary scoring giving system administrators unequivocal information on the most important security actions that need to be implemented every day. And the results are in:

In the first year the risk score for hundreds of thousands of computers across the State Department dropped by nearly 90% while those of other federal agencies hardly changed at all. (Chart 1) And the risk reduction continues to today. As importantly, when a major new threat arose, the State Department was able to get 90% of it systems patched in 10 days (Chart 2) while other agencies, without automation and scoring and sysadmin prioritization, got between 20% and 65% of their systems patched in several months.

Chart 1: 90% Risk Reduction In Less Than A Year

Chart 2: Threat-based mitigation: Giving the high priority fix a 40 point risk score gained rapid remediation to 80%; increasing it to 320 points pushed compliance to 90%.

	20 Critical Security Controls: Critical Security Control	Critical Security Control Description	National Security Agency Assessment of the 20 Critical Controls: Tier	Attack Mitigation	Dependencies	Technical Maturity	The Australian Government's Strategies to Mitigate Targeted Cyber Intrusions: Ranking	Description	Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls
							1 2 3 4	*Once organizations have implemented the top four mitigation strategies, firstly on computers used by employees most likely to be targeted by intrusions and then for all users, additional mitigation strategies can then be selected to address system security gaps to reach an acceptable level of residual risk*	
1	**Inventory of Authorized and Unauthorized Devices**	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.	1	Very High	Foundational	High			CM-8 (a, c, d, 2, 3, 4) PM-5 PM-6
2	**Inventory of Authorized and Unauthorized Software**	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.	1	Very High	Foundational	High	4.	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker.	CM-1 • CM-2 (2, 4, 5) • CM-3 CM-5 (2, 7) • CM-7 (1, 2) CM-8 (1, 2, 3, 4, 6) • CM-9 PM-6 • SA-6 • SA-7
3	**Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers**	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.	1a	Very High	Capability	High	1. 2. 3. 15. 16. 20. 21.	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version. Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker. Network-based Intrusion Detection/Prevention System to identify anomalous behavior such as process injection, keystroke logging, driver loading and call hooking. Application-based firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. Anti-virus software with up-to-date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop anti-virus software from different vendors.	CM-1 • CM-2 (1, 2) CM-3 (b, c, d, e, 2, 3) CM-5 (2) • CM-6 (1, 2, 4) CM-7 (1) • SA-1 (a) SA-4 (5) • SI-7 (3) PM-6
4	**Continuous Vulnerability Assessment and Remediation**	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.	1a	Very High	Capability	High	1. 2.	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.	RA-3 (a, b, c, d) RA-5 (a, b, 1, 2, 5, 6)
5	**Malware Defenses**	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.	1a	High/ Medium	Capability	High/ Medium	4. 5. 12. 14. 21.	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker. Host-based Intrusion Detection/Prevention System to identify anomalous behavior such as process injection, keystroke logging, driver loading and call hooking. Application-based firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. Anti-virus software with up-to-date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop anti-virus software from different vendors.	SC-18 SC-26 SI-3 (a, b, 1, 2, 5, 6)
6	**Application Software Security**	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).	2	High	Capability	Medium	20.	Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems.	CM-7 • RA-5 (a, 1) SA-3 • SA-4 (3) • SA-8 SI-3 • SI-10
7	**Wireless Device Control**	**Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if it matches an authorized configuration and security profile and has a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.	2	High	Capability	Medium			AC-17 AC-18 (1, 2, 3, 4) SC-9 (1) • SC-24 SI-4 (14, 15)
8	**Data Recovery Capability**	**Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.	2	Medium	Capability	Medium			CP-9 (a, b, d, 1, 3) CP-10 (6)
9	**Security Skills Assessment and Appropriate Training to Fill Gaps**	**Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.	2	Medium	Capability	Medium	6.	User education e.g. Internet threats and spear phishing, socially engineered e-mails. Avoid: weak passphrases, passphrase reuse, exposing e-mail addresses, unapproved USB devices.	AT-1 • AT-2 (1) AT-3 (1)
10	**Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**	**Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments:** Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.	3	High/ Medium	Capability/ Dependent	Medium/ Low	15. 19.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	AC-4 (7, 10, 11, 16) • CM-1 CM-2 (1) CM-3 (2) • CM-5 (1, 2, 5) CM-6 (4) • CM-7 (1, 3) • IA-5 IA-2 (1, 6) • IA-5 • IA-8 • SC-9 SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18)
11	**Limitation and Control of Network Ports, Protocols, and Services**	**Allow remote access only to legitimate users and services:** Apply host-based firewalls and port filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.	3	High/ Medium	Capability/ Dependent	Medium/ Low	13. 19.	Application-based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming network traffic. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	CM-6 (a, b, d, 2, 3) CM-7 (1) SC-7 (4, 5, 11, 12)
12	**Controlled Use of Administrative Privileges**	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.	4	High/ Medium	Dependent	Medium	3. 16. 17. 18. 21.	Minimize the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for e-mail and web browsing. Multi-factor authentication especially implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository. Randomized local administrator passphrases that are unique and complex for all computers. Use domain group privileges instead of local administrator accounts. Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words. Disable LanMan password support and cached credentials on workstations and servers to make it harder for adversaries to crack password hashes.	AC-6 (2, 5) AC-17 (3) AC-19 AU-2 (4)
13	**Boundary Defense**	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").	4	High/ Medium	Dependent	Medium/ Low	6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 19. 20. 21. 22. 23. 24.	Whitelisted e-mail content filtering allowing only attachment types required for business functionality. Preferably convert Word, PDF and Microsoft Office attachments. Block spoofed e-mails using Sender Policy Framework checking of incoming e-mails, and a "hard fail" SPF record to help prevent spoofing of your organization's domain. Web content filtering of incoming and outgoing traffic, using signature, reputation ratings and other heuristics, and whitelisting allowed types of web content. Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. Web domain whitelisting for all TPS SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy. Anti-virus software with up-to-date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop anti-virus software from different vendors. Block attempts to access web sites by their IP address instead of by their domain name. Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries. Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	AC-17 (1) • AC-19 • AU-2 (4) AU-3 (1,2) • AU-4 • AU-5 AU-6 (a, 1, 5) • AU-8 AU-9 (1, 2) • AU-12 (2) • SI-4 (8)
14	**Maintenance, Monitoring, and Analysis of Security Audit Logs**	**Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:** Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.	4	Medium	Dependent	Medium	23. 24. 25.	Centralized and time-synchronized logging of allowed and blocked network activity, with regular log analysis, storing logs for at least 18 months. Centralized and time-synchronized logging of successful and failed computer events, with regular log analysis, storing logs for at least 18 months. Full network traffic capture to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.	AC-17 (1) • AC-19 • AU-2 (4) AU-3 (1,2) • AU-4 • AU-5 AU-6 (a, 1, 5) • AU-8 AU-9 (1, 2) • AU-12 (2) • SI-4 (8)
15	**Controlled Access Based on the Need to Know**	Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.	4	Medium	Dependent	Medium/ Low	15. 30.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. TLS encryption between e-mail servers to help prevent legitimate e-mails being intercepted and used for social engineering. Perform content scanning after e-mail traffic is decrypted.	AC-1 • AC-2 (b, c) AC-3 (4) AC-4 • AC-6 MP-3 • RA-2 (a)
16	**Account Monitoring and Control**	**Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.	4	Medium	Dependent	Medium/ Low	18.	Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.	AC-2 (e, f, g, h, j, 2, 3, 4, 5) AC-3
17	**Data Loss Prevention**	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.	5	Medium/ Low	Dependent	Low	29.	Removable and portable media control as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	AC-4 • MP-2 (2) • MP-4 (1) SC-7 (6, 10) • SC-9 • SC-13 SC-28 (1) • SI-4 (4, 11) • PM-7
18	**Incident Response Capability**	**Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	5	Medium	Dependent	Low			IR-1 • IR-2 (1) IR-4 • IR-5 IR-6 (a) • IR-8
19	**Secure Network Engineering**	**Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.	6	Low	Indirect	Low	15. 19.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	IR-4 (2) • SA-8 SC-7 (1, 13) • SC-20 • SC-21 SC-32 • PM-7
20	**Penetration Tests and Red Team Exercises**	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems—to test existing defenses and response capabilities.	6	Low	Indirect	Medium/ Low			CA-2 (1, 2) • CA-7 (1, 2) RA-3 • RA-5 (4, 9) SA-12 (7)

NSA identifies these 3 controls as having special value for immediate implementation in organizations that have not yet implemented more complete defenses.

AUSTRALIA: Australian Government Department of Defence — UNITED KINGDOM: CPNI Centre for the Protection of National Infrastructure — UNITED STATES: Homeland Security — SANS Institute, Winter 2012

Wheel built

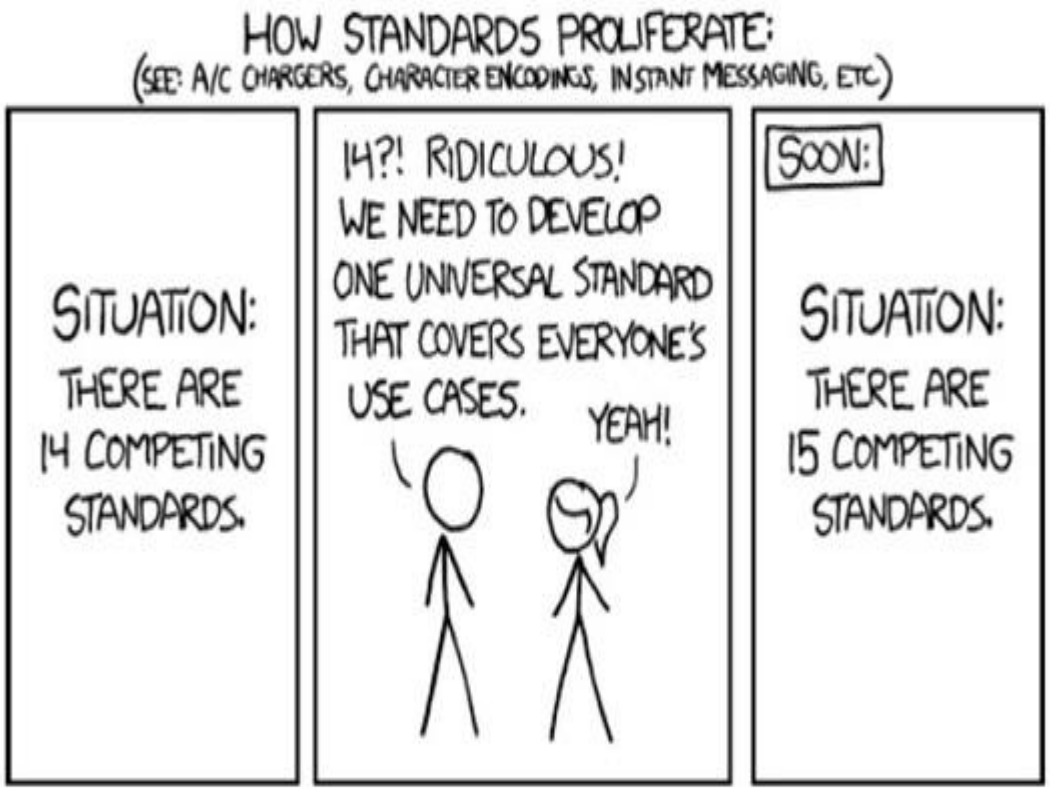
Top 20 Controls
They were the Critical Controls before they were "for Effective Cyber Defense"…. Includes a Privacy Impact Assessment template

http://www.cpni.gov.uk/advice/cyber
OR
https://www.cisecurity.org/critical-controls/

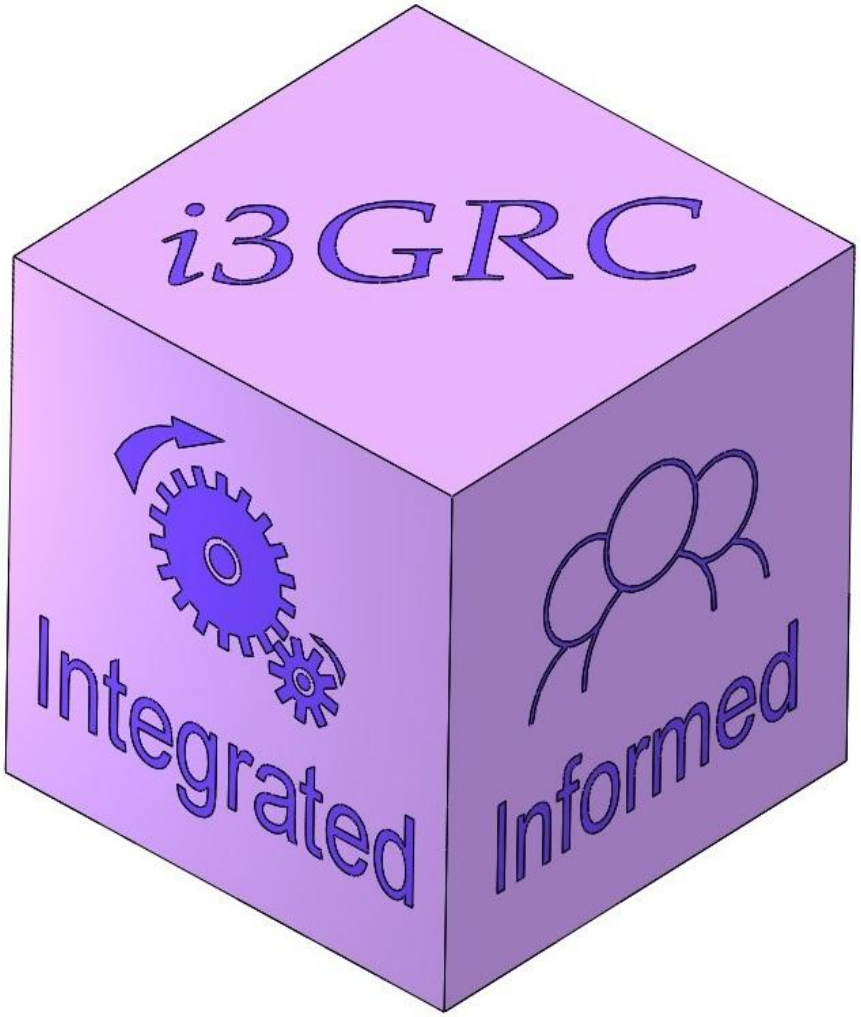
i3GRC Integrated Informed

Our reality ☹

Multiple Wheels built



i3GRC™



Changing Landscape

HOW MANY TIMES A DAY ARE YOU HANDING OVER YOUR INFORMATION?

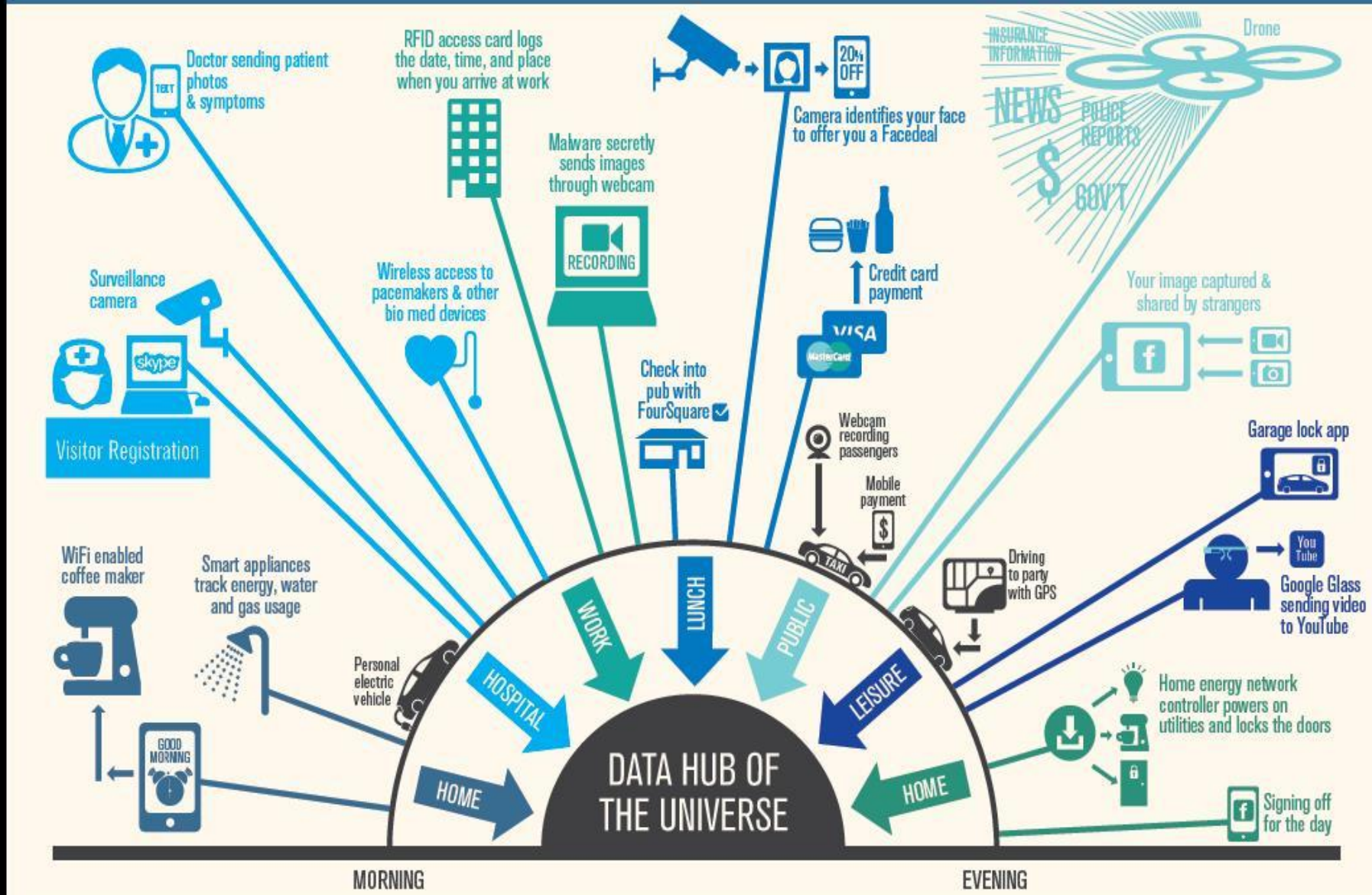
PRIVACY PROFESSOR
www.privacyguidance.com

From the moment we wake – and turn on that WiFi-enabled "smart" coffeemaker– to the time we make our final Facebook sign off for a long, restful sleep, we are leaving a digital trail. Most of us have no idea how the data about our daily habits, our purchases – even our routes to work – is being collected or how it's being shared.

The infographic below outlines just a few of the hundreds of ways we voluntarily open our everyday lives to intelligence-gathering marketers, companies, government agencies, data bureaus and unknown others, simply by using our vast and growing array of technologies.

THE TAKE-AWAY?

Understand how much data you are sharing simply through every day use of gadgets and apps. Be aware of how that data may be revealing some pretty intimate details about you. If taken out of context, it may result in damaging assumptions. What can you do to lessen the data trail you leave behind every day?



The landscape

- Privacy – DP, data residency, data sovereignty, Safe Harbor, GDPR, PII handling, PCI
- Data Retention – different requirements globally
- Legislation and Regulations - sector specific – HIPAA, PCI, ITAR (home paternity test and fitness tracker data not included under HIPAA yet)
- 3rd party requirements – different (often competing, sometimes conflicting) contractual obligations may apply
- Network Information Security (NIS) directive
- EU-USA Transatlantic Trade and Investment Partnership (TTIP) – due for ratification 2018, the same time that GDPR will become law

And yet…

- Shadow IT.... We lack data governance, we lack line of sight of our data ☹
- Deceit devices
- The double Irish – pioneered by Apple Inc in the 1980s [Source: https://en.wikipedia.org/wiki/Double_Irish_arrangement]
- The most recent financial crash was ultimately born of greed and a palpable lack of ethics – see The Big Short! [Source: http://www.imdb.com/title/tt1596363/]
- Be clear there's a thread of unethical behaviour running through business – much of which is *not* illegal

GPDR – initial thoughts

- Data protection “by design and by default”
- Data Controllers must take a positive approach to information security – so? Why does Principle 7 not already mean that?
- Citizens at the heart of DP with the “right to know” (an extension of P5) and the “right to be forgotten” (an extension of P6) – neither of these are **new** rights
- Organizations under scrutiny for their data collection (an extension of P1,2) and processing activities (an extension of P3,4)
- Fines to be levied for data breaches to amount to 2% of a company’s annual worldwide turnover
- Organisations should already know and understand how they process and handle data
- 93% of breaches can be attributed to mistakes made by end-users.

Safe Harbor broken and yet...

Wheel built

Generally Accepted Privacy Principles (GAPP)

- Principle 1: Management
- Principle 2: Notice
- Principle 3: Choice and Consent
- Principle 4: Collection
- Principle 5: Use, Retention and Disposal
- Principle 6 and 7: Access and Disclosure to Third Parties
- Principle 8: Security for Privacy
- Principle 9: Quality
- Principle 10: Monitoring and Enforcement

Source: American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) GAPP, August 2009

Encryption expectations

Regulation	Region	Breach Notification	Safe Harbor Exemptions	Recommendations on Encryption
PCI DSS		✓	✓	Encryption a "critical component"
GLBA		✓	✓	Safe harbor "if encryption has been applied adequately"
HIPAA, HITECH		✓	✓	Safe harbor "if encryption has been applied adequately"
EU Directives		Proposed	Proposed	Encryption likely to be recommended
ICO Privacy Amendment		✓	✓	Notification not required if there are "measures in place which render the data unintelligible."
Privacy Amendment		✓	Not specified	Not specified but you should to "take adequate measures to prevent the unlawful disclosure"
US State Privacy Laws		✓	Generally Yes	Typical breach definitions: - Personal Information: "data that is not encrypted" - Breach: "access to unencrypted data"

Follow the money

- Google moved from Ireland to Germany – where DP law is tighter – in order to be protected from the US government requesting access to the data – this *sounds* good but....
- Think global - **All your stuff is readable by Uncle Sam. Worldwide** - Microsoft has sued the US government, challenging its right to access European data in its Dublin data centre. The US government can do so because ***it recognises no territorial limits to US power in its laws: everywhere in the world is the United States***.
- Ownership of plcs, data location, data sovereignty
- What % of global companies is % of EU companies?
- How many SMEs are reliant on global companies?
  - Microsoft (Windows, Office 360 etc)
  - Google (gmail, maps, calendar etc)
  - Amazon (cloud services) - new entrant
  - Salesforce (CRM etc)

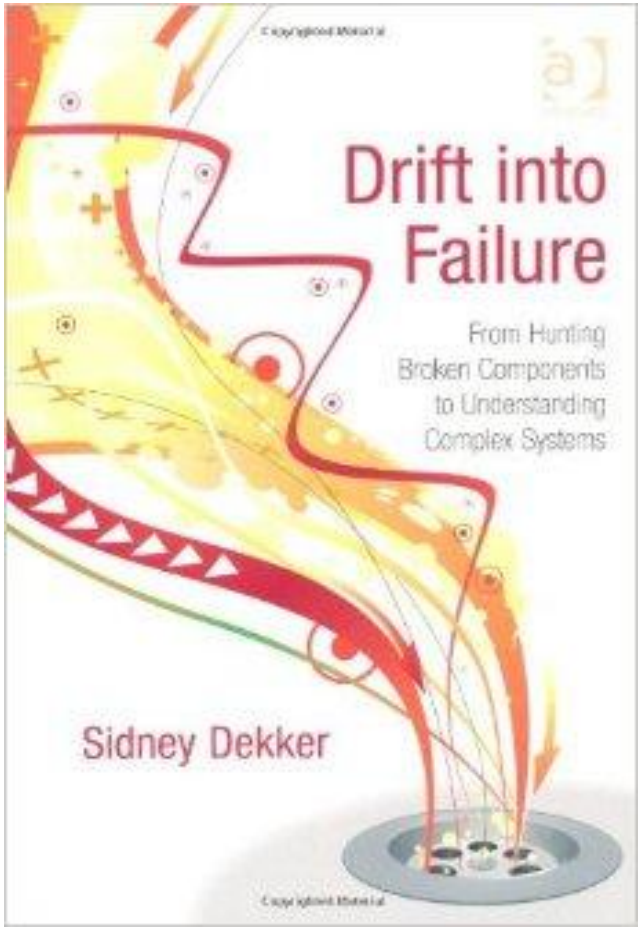
2015 HfS Global IT Services Top 10

Rank 2014	Service Provider	Est IT Services Revenue 2014 ($Bn)	Market Share (%)
1	IBM	52.5	8.1%
2	HP	27.6	4.3%
3	Accenture	26.6	4.1%
4	Fujitsu	25.4	3.9%
5	SAP	16.4	2.5%
6	Oracle	13.8	2.1%
7	CapGemini	13.4	2.1%
8	TCS	12.2	1.9%
9	NTT Data	12.0	1.9%
10	CSC	11.8	1.8%
	Top 10	211.8	32.8%
14	Cognizant	8.9	1.4%
16	Infosys	7.3	1.1%
20	Wipro	5.3	0.8%
22	Amazon Web Services	4.6	0.7%
24	HCL	4.4	0.7%
	Total Market	644.8	100.0%

Source: HfS Research 2015. *Estimated from services provider financials. Revenues fitted to nearest calendar year (2014). Since the last time we published a top 10 list for IT services, we made some adjustments to criteria for revenue inclusion, classifying some IT service revenue as business services. This mainly impacted NTT Data and Fujitsu.*

Conclusions

Normalizing the deviance



Turn the problem…

- Cyber Security
- Skills crisis
- Volumes of data
- Lack of security intelligence
- Right to be forgotten (RTBF)
- Data sovereignty
- GDPR understanding
- 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

...into a solution

- Frameworks are available – they need to be properly utilised
- Actionable Intelligence – need to “mine” your log data to work out what’s going on
- Technology is not always the solution! (It’s usually the problem!)
- Unseen solutions – can be created with ease

Wherever security is perceived to be the enemy of productivity, an organization will be at risk of a data breach.

[Source: Tony Pepper, CEO, Egress Software Technologies – Awareness of GDPR is not Enough – Action is Needed, p.22, infosecurity, Q4 2015, Volume 12, Issue 4]

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

Over to you!

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
***Web*:** www.i3grc.co.uk

i3GRC™/ SPS - Who are we?

- **17** years experience in compliance, audit, security risk management, security lifecycle management, information assurance, information governance, data protection and freedom of information
- Training customers and Consulting customers
- **Accreditations and memberships** of various bodies including ISC2, ISSA, ISACA, BCS, IISP, IRMS, BCI
- **Trademarked framework *i3GRC*** ™(integrated and informed information governance risk and compliance)
- **Process and Compliance Capability** – ISO27001, PCI, GRC, DPA, SAS 70, HIPAA, ISAE 3402
- **Industry coverage** – public and private sector – industry and technology agnostic! Everyone has *some* information that needs protection.

ISO/IEC 27001:2013

DATA PROTECTION ACT 1998

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™.
- **Contributions**
  - **Chapter** in Trim, P.R.J. and Caravelli, J. (2009) ***Strategizing Resilience and Reducing Vulnerability***, New York: Nova Science Publishers, Inc. ISBN 13: 978-1-60741-693-7
  - **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/