THE DEVIL IS IN THE CONTRACTUAL DETAILS

Dr Andrea C Simmons
i3GRC Limited
DISAPPOINTING HEADLINES
How does this help?

NHS Digital to ignore IT security recommendations despite WannaCry

£1bn estimated cost not considered worth it, despite ongoing attacks targeting NHS data

NHS Digital is set to ignore the IT security recommendations of its own chief information officer, Will Smart, citing the estimated cost of between £800 million and £1 billion. It claims that the investment would not be "value for money".

The recommendations were the result of a review, published in February, that was commissioned by government in response to the WannaCry ransomware attack, which affected one-fifth of all NHS trusts in the UK. The NHS was especially hard hit, not least due to a lack of up-to-date patching on Windows 7 workstations across the monolithic organisation, one of the biggest employers in the world.

The recommendations in Smart's review had been endorsed by the National Cyber Security Centre (NCSC). However, documents acquired under Freedom of Information by the Health Service Journal (HSJ), indicate that NHS Digital has opposed adoption of the recommendations on the grounds that they would not "be value for money".
Are we becoming inured?

Source: http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
UNREASONABLE EXPECTATIONS
Multi Disciplined

Source: Corporate Defense Umbrella, Source: Lyons, 2016
Wide scope expected of “us”

<table>
<thead>
<tr>
<th><strong>Strategic security</strong></th>
<th><strong>Technical security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security framework</td>
<td>Hardware hardening</td>
</tr>
<tr>
<td>Policy development</td>
<td>Incident response</td>
</tr>
<tr>
<td>Awareness campaigns (ISTAP)</td>
<td>Firewalls</td>
</tr>
<tr>
<td>Security procedures</td>
<td>Anti-virus software</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>Intrusion detection and prevention</td>
</tr>
<tr>
<td>IS management systems</td>
<td>Vulnerability scans</td>
</tr>
<tr>
<td>Risk analysis</td>
<td>Penetration testing</td>
</tr>
<tr>
<td>Best practices</td>
<td>Data-loss prevention tools</td>
</tr>
<tr>
<td>Data privacy (GDPR)</td>
<td>Access control</td>
</tr>
<tr>
<td>Crisis management</td>
<td>System security</td>
</tr>
<tr>
<td>Organisational view</td>
<td>Network security</td>
</tr>
<tr>
<td>Security regardless of technology</td>
<td>System monitoring</td>
</tr>
<tr>
<td>Government models (Cyber Essentials)</td>
<td>IT disaster recovery</td>
</tr>
</tbody>
</table>
IISP Skills Framework

Section A
Information Security Governance and Management

Section B
Threat Assessment and Information Risk Management

Section C
Implementing Secure Systems

Section D
Assurance: Audit, Compliance and Testing

Section E
Operational Security Management

Section F
Incident Management, Investigation and Digital Forensics

Section G
Security Discipline is not used.

Section H
Business Resilience

Section I
Information Security Research

Section J
Management, Leadership, Business and Communications

Section K
Contributions to the Information Security Profession and Professional Development
Security concerns of the modern day CISO

Source: https://www.optiv.com/ciso-periodic-table
<table>
<thead>
<tr>
<th>ISACA</th>
<th>CISA</th>
<th>CISM</th>
<th>CRISC</th>
<th>CGEIT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Career Path</strong></td>
<td>Lead IT Auditor</td>
<td>Chief (Information) Security Officer (CSO / CISO)</td>
<td>Chief Risk Officer (CRO)</td>
<td>Chief Information Officer (CIO)</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>IT Audit</td>
<td>Information Security</td>
<td>Risk Management</td>
<td>IT Governance</td>
</tr>
<tr>
<td><strong>Work Performed</strong></td>
<td>Provide assurance by conducting audits and assessments of information systems</td>
<td>Oversee, direct and manage information security activities</td>
<td>Identify, evaluate and manage risk through the development, implementation and maintenance of information systems controls</td>
<td>Define, establish, maintain and manage a framework of IT governance</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>Submit verified evidence of a minimum of 5 years of verifiable IS audit, control or security experience (substitutions available)</td>
<td>Submit verified evidence of a minimum of 5 years of information security management work experience (covering 3 of the 4 job practice domains)</td>
<td>Submit verified evidence of a minimum of 3 years of risk and information systems controls experience (covering 3 of the 5 job practice domains)</td>
<td>Submit verified evidence of the 5 years experience requirements as defined by the CGEIT Job Practice</td>
</tr>
<tr>
<td><strong>Additional requirements</strong></td>
<td>Adhere to the ISACA Code of Professional Ethics</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2015 iProarness. All rights reserved.
No (explicit) mention of Contract Management here...

Source: https://www.ncsc.gov.uk/blog-post/cybok-release-first-knowledge-areas
Source: https://www.cybok.org/
THE CONTRACT IS KING
Given this…

Finally...!

Privacy program governance:
- Policies and standards
- People and organizational management
- Environmental inputs
- Expectation management and complaints

Privacy risk management:
- Risk appetite
- Risk identification
- Risk profiling
- Risk assessment
- Issue management

Privacy process, risk and control framework:

Focus areas:

Governance:
- Accountability and compliance
- Privacy and security by design
- Privacy data assessment (appropriate collection & use)
- Incident and breach management

Use of data:
- Consent and privacy notification
- Data protection
- Data rights management
- Records management

Validation:
- Contract management
- Third-party risk management
- Internal and external assurance
- Continuous monitoring and improvement

Compliance, technology enablement, monitoring and reporting:

Privacy culture:

Philosophically speaking

• If these are the manifold expectations of “us”...:
  • Subject-matter experts in the technical aspects of ever-changing threats, vulnerabilities, exploits and information technologies in the specific operational context of their own organization; and
  • Trusted advisers to the people who are responsible for making the business decisions about security-related risks, with the business acumen needed to bridge the gap between technical detail and organizational impact.

• ... why can we not expect the same of our colleagues in other disciplines – Legal, Procurement, IT, HR etc?

• Why are we expected to be the ones responding to security and/or data protection/privacy questionnaires in the BID process? Why does the business team not “get” this stuff yet?
Commercial Law vs Data Law

• Be under no illusions...
• This is not being adequately addressed
• Spend time with your Procurement colleagues
• But put them in the same room as the Lawyers
• The DPO role is an advisory one – the others need to thrash this out!
Normalizing the deviance

Legal grounds and lawful bases

Processing is lawful if one of these bases exists

Consent
The consent of a data subject to the processing of his/her personal data

Legitimate interests
There is a weighed & balanced legitimate interest where processing is needed and the interest is not overridden by others

Public interest
Public authorities and organizations in the scope of public duties and interest

Lawfulness of processing

Contractual necessity
Processing is needed in order to enter into or perform a contract

Legal obligations
The controller is obliged to process personal data for a legal obligation

Vital interests
It is vital that specific data are processed for matters of life and death

Source: https://www.i-scoop.eu/gdpr/legal-grounds-lawful-processing-personal-data/
All done yet?

Steps to work with your 3rd party providers

1. Make a list of solution providers that touch your data
2. Map out the path your data takes during the lifecycle and determine criticality
3. Review TOMs
4. Assess the level of risks
5. Review all contracts and introduce new clauses to ensure data privacy measures
6a. Make your suppliers sign the new BCR contracts / clauses and are able to provide proof they are GDPR compliant
6b. Switch to 3rd party providers that are GDPR compliant

This process needs to be repeated on a regular basis.

Source: https://www.mailjet.com/gdpr/mailjet-gdpr-compliance/
FUTURE IMPERFECT?
8 events to make or break a CISO

1. Change of management
2. Breach
3. Audit / New Findings
4. Mergers & Acquisitions
5. Maturity Shift
6. Large Scale project(s)
7. Tech Replacement
8. Management briefing

Speak the language of business
1. Risk
2. Revenue
3. Employee efficiency
4. Strategic value
5. Cost
6. Customer satisfaction

Source: https://www.cybereason.com/thank-you/8-moments-that-can-make-or-break-a-ciso
Source: http://cybr.ly/2lWA64t
There’s nothing new under the sun

The CISO 2016-2020... The 2018 CISO Evolution

- Plan path away from operations
- Refine risk management processes to business language
- Widen vision to privacy, data management and compliance
- Build support network
- Create focus and attention of business leaders

Source: https://www.slideshare.net/cisoplatform7/super-ciso-2020-how-to-keep-your-job
CONCLUSIONS
Read this!

The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win

Gene Kim, Kevin Behr, and George Spafford
Listen to this!

A conversation with Sam Curry - https://www.cybereason.com/thank-you/8-moments-that-can-make-or-break-a-ciso?

Source: https://trustedadvisor.com/why-trust-matters/understanding-trust/understanding-the-trust-equation
OVER TO YOU...
Thank you!

Dr 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 352941
Web: www.i3grc.co.uk
i3GRC/SPS – Who are we?

• 20 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.
RESOURCES
Resources

A. https://www.linkedin.com/pulse/i-ciso-gary-hayslip-cissp-
C. https://www.infosecskills.com/content/cybercareers
I. Listen to this: First 90 days: https://www.linkedin.com/pulse/new-ciso-get-your-first-90-days-action-items-here-samuel-liles/
Speaker Profile

Andrea Simmons  FBCS CITP CISM CISSP MA M.Inst.ISP
- Andrea brings more than 20 years direct information security, assurance and governance experience, helping clients establish appropriate controls and achieving and maintaining security certifications. Andrea’s was previously Chief Information Security Officer for HP Enterprise Services, a role 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 returned to independent consultancy to take forward a framework developed through doctoral research - i3GRC™.

Contributions
- Fellow of the BCS, Chartered Institute for IT - http://www.bcs.org/blogs/security
- Senior Member of the ISSA, http://www.issa.org/
- ISACA member, http://www.isaca.org/
- Previously:
  - 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/
  - Member of the BCS Security Community of Expertise
  - Volunteer delivering Safe and Secure Online programs to UK schools for ISC2, https://www.isc2.org/
i3GRC™

Source: www.i3grc.co.uk