Protect • Comply • Thrive

Cyber Security and IT Governance Critical Issues

Top 11 challenges to address in 2014

www.itgovernance.co.uk

FOREWORD

At IT Governance we have a mission to meet the evolving cyber security and IT governance needs of today's organisations, directors, managers and practitioners.

In the fast paced world of technology and information overload, managing security and optimising IT resources for maximum business value are only few of the key challenges businesses face.

We have looked at past and current developments in order to identify the top trends for which businesses must prepare.

In 2014, more than ever before, organisations globally will be put to the test by a whole new spectrum of issues arising from emerging technologies, changes of user behaviour, new standards, laws and regulations as well as increasing security risks. Addressing these will only be made possible through a fully integrated approach which encompasses people, process and technology.

Those who succeed in tackling these challenges holistically will thrive. Those who don't may experience a much harder time fulfilling their business potential.

1. THE SPLIT IN MANAGEMENT SYSTEMS WILL INCREASE

The public and private sectors will be encouraged to pursue divergent cyber security standards, fracturing the skill and competence ecosystem and creating gaps in security for attackers to exploit.

Will businesses be forced to make a decision about the standard or framework in which to invest based on the costs of these investments?

- The UK government has recently released the **BIS Ten Steps to Cyber Security** and will also launch a 'kitemark' standard for cyber security in 2014.
- The US has released a **voluntary cyber security framework** for national infrastructure.
- ENISA, the EU's Agency for Network and Information Security, will be developing **European cyber security standards** separate from international standards.
- **PAS 555** was published in 2013 as a specification for cyber security risk management.
- **ISO 27001**, the international information security management standard, already accounts for more than 20,000 certifications.
- Businesses that want to work with the UK government may have to meet the new **kitemark standard**, in addition to meeting the requirement of existing standards such as ISO 27001 and other international standards and frameworks.

2. BYOD WILL CREATE EVER-EXPANDING SECURITY RISKS

The productivity and financial benefits of 'Bring-Your-Own-Device' (BYOD) will so evidently outweigh the traditional corporate-centred model that many organisations will embrace it, without first putting in place an adequate security infrastructure. This, combined with increasing mobile and home working, will open many new opportunities for attackers.

- **66%** of BYOD users are concerned about the risk of data interception.
- BUT **64%** of BYOD users will connect to any free wi-fi available.[1]
- Moving from a basic BYOD implementation to a comprehensive BYOD implementation can realise **gains of up to $1300 per user**.
- There were 198 million BYOD devices in 2013 and their number is expected to double to **405 million by 2016**. [2]
- According to Gartner Research, globally, **88%** of executives report employees use their personal computing technologies for business purposes today. [3]

Sources:

[1] GFI Survey 2013 - http://www.gfi.com/documents/GFI_Wireless_Survey_US.pdf)
[2] Cisco IBSG Report - http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf
[3] Help Net Security - http://www.net-security.org/secworld.php?id=16169

Protect • Comply • Thrive

www.itgovernance.co.uk

3. CYBER CRIMINALS WILL BECOME MORE PROFESSIONAL

There will be a growing interaction between state-sponsored cyber warriors and those deployed by serious organised crime. This will lead to an increase in the range, breadth and sophistication of attacks (involving DDoS, network infiltration, APTs) – combined with a proliferation of lower-level attacks against smaller, less secure organisations which, while individually netting say £10k per attack, will increasingly be carried out on an industrial scale.

- Stuxnet, Duqu and Flame, all appear to be related, and targeted against state holdings. Their latest iterations are now hitting private organisations. [1]
- Russia has executed a cyber attack on Estonia. [2]
- Operation Aurora was targeted at major US organisations, including Google, Northrop Grumman and Dow Chemical. [3]
- **71% of all cyber attacks** in the 2nd quarter of 2013 originated from China and Indonesia. [4]
- **63% of organisations** think it is only a matter of time until they are targeted by an APT. [5]

Sources:

[1] CrySyS - http://www.crysys.hu/skywiper/skywiper.pdf
[2] The Guardian - http://www.theguardian.com/world/2007/may/17/topstories3.russia
[3] The Washington Post - http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html
[4] Akamai report - http://www.akamai.com/dl/documents/akamai_soti_q213.pdf?WT.mc_id=soti_Q213
[5] ISACA - http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf

4. THE INTERNET OF THINGS WILL BECOME TARGET TO CRIMINALS

While the Internet of Things will initially be an area of cyber experimentation, cloud services (particularly high value targets like payment gateways and any service that processes personal data) will be increasingly targeted. There will be major breaches.

- **8 billion** connected objects in 2012
- **10 billion** by the end of 2013
- **50 billion** by 2020 [1]

"As more devices become connected, they will provide an increasing set of features (like integration with Facebook, social media accounts, and apps), creating a larger and increasingly vulnerable attack surface for hackers to exploit."

Harvard Business Review [2]

Sources:

[1] Cisco news feature - http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342
[2] Harvard Business Review - http://blogs.hbr.org/2013/06/rethinking-security-for-the-in/

Protect • Comply • Thrive

www.itgovernance.co.uk

5. ‘CYBER RESILIENT’ WILL REPLACE ‘CYBER SECURE’

Migration to the Internet and increasing software sophistication will, between them, introduce increasing software vulnerabilities which will be exploited by savvy cyber attackers. While less savvy organisations will respond by trying to restrict staff mobility, social engineering and Internet access, as security incidents proliferate and the reality of living permanently with irreducible levels of cyber threat finally sinks in more savvy organisations will gradually replace ‘cyber secure’ with ‘cyber resilient’ as the target organisational status.

In 2012,

- **79% of the victims** of data breaches were targets of opportunity
- **96% of data breaches** were not difficult.
- **97% of data breaches** could have been avoided with simple or intermediate controls.
- **85% of data breaches** took weeks to discover. [1]

“Many organisations will be shocked out of complacency by discovering that, rather than never having had an attack, their defences were actually breached months ago.”

Alan Calder, Founder and Executive Chairman of IT Governance

Sources:

[1] Verizon Report 2012 - http://issuu.com/steelhenge/docs/rp_data-breach-investigations-report-2012_en_xg

Protect • Comply • Thrive

www.itgovernance.co.uk

6. THERE WILL BE A SHORTAGE OF CYBER SECURITY PROFESSIONALS

The world shortage of cyber security professionals who are able to combine technical security expertise with process (management system) competence, regulatory compliance awareness and an understanding of business requirements will become much more severe for some years before the situation starts to improve.

- **43%** of cyber security professionals rate their position as the most difficult one in the organisation. [1]
- **56%** of information security professionals believe there is a shortage of information security personnel in their organisation. [2]

"It could take up to 20 years to address the skills gap [in cyber security] at all levels of education."

National Audit Office [3]

Sources:

[1] SecureWorld Insight - http://www.net-security.org/secworld.php?id=16113
[2] (ISC)2 - https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf
[3] National Audit Office - http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

Protect • Comply • Thrive

www.itgovernance.co.uk

7. SOCIAL MEDIA SERVICES WILL RAISE THE CYBER RISKS

The proliferation of social media services will drive more and more people to be increasingly indiscreet about personal data, opening up myriad of new identify theft, phishing, pharming, waterhole and other attack opportunities. Staff will even more obviously become the 'weakest link' with social engineering and blended attacks much more common.

- **47** social networks with >1 million users in 2008 compared to **87** social networks with >1 million users in 2013. [1]
- **556** social media 'crimes' in the UK in 2008 compared to **4098** social media 'crimes' in the UK in 2013. [2]
- Nearly **50% growth**[4] in the time spent on social media from 2011-2012. [3]
- **43%** of information security professionals consider social media a significant security concern. [4]

Sources:

[1] Wikipedia - http://en.wikipedia.org/wiki/List_of_social_networking_website
[3] BBC - http://www.bbc.co.uk/news/uk-20851797
[3] Nielsen report - http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf
[4] (ISC)2 - https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

8. A SMALL DIGITAL ELITE WILL SHUN MOST FORMS OF 'OPEN' DIGITAL MEDIA

Conversely, a small digital elite will shun most forms of 'open' digital media as they become more savvy about protecting their communications and data. This digital elite will increasingly deploy personal email and mobile device encryption, two-factor authentication and single password tools.

Microsoft is supporting this trend through improving the accessibility of privacy tools, while comparing the actions of some governments to APTs.

"Indeed, government snooping potentially now constitutes an "advanced persistent threat," alongside sophisticated malware and cyber attacks."

Microsoft blog [1]

Sources:

[1] Microsoft blog - http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx

Protect • Comply • Thrive

www.itgovernance.co.uk

9. THE INTERSECTION B/W REGULATION AND CYBER SECURITY WILL BECOME MORE OVERT

New data protection and privacy regulations in Europe, South Africa, Australia and elsewhere, combined with upgrades to the PCI DSS standard, will drive digital security efforts in organisations that will simultaneously have respond to competing government requirements around digital security. CISOs will have to broaden the skills and tools available in their teams in order to respond to this range of challenges.

Data protection laws are being updated and expanded globally.

- The **Payment Card Industry Data Security Standard** (PCI DSS) v3.0 has come into force on 1 January 2014.
- The adoption of the **General Data Protection Regulation** (GDPR) within the European Union (EU) is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years.
- The Chinese **Telecommunications and Internet Personal User Data Protection Regulations** took effect on 1 September 2013.
- The South African **Protection of Personal Information Bill** became law on 26 November 2013.
- **The Australian Privacy Act** comes into effect on 12 March 2014 including the introduction of the Australian Privacy Principles (APPs) and a new credit reporting regime governing credit-related personal information.

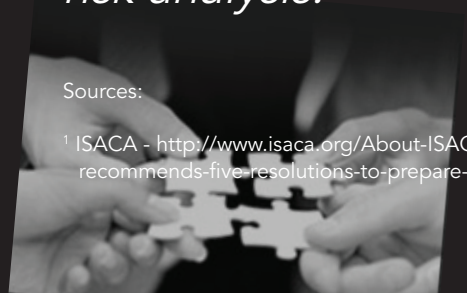
Protect • Comply • Thrive

www.itgovernance.co.uk

10. IT SERVICE MANAGEMENT AND CYBER SECURITY WILL NEED TO MERGE

The worlds of IT Service Management (primarily organisations embracing ITIL® and ISO/IEC 20000) and cyber security will have to hybridize to deliver secure services that enable their organisations. In larger organisations, frameworks like COBIT® will increasingly bring cross-organisational control processes which will need to integrate IT service management and cyber security silos.

"With some elements of IT security operational responsibility (including malware detection, event analysis and control operation) increasingly being outsourced to cloud providers, smart leaders are enabling their internal security experts to become hunters instead of just defenders. This allows them to proactively seek out the most hard-to-detect threats, build internal intelligence capabilities (e.g., "threat intelligence"), construct better metrics and invest in operational risk analysis." [1]



Sources:

[1] ISACA - http://www.isaca.org/About-ISACA/Press-room/News-Releases/2013/Pages/ISACA-recommends-five-resolutions-to-prepare-IT-professionals-for-2014-trends.aspx

11. THE PRESSURE TO COMPLY WILL GROW

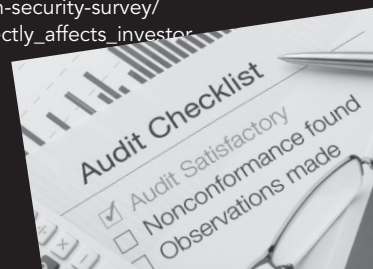
Auditors, investors, non-executive directors and regulators will apply growing pressure to organisations in public, private and voluntary sectors across the world to put in place appropriate cyber security and IT governance frameworks.

- Security incidents are up **25%** with average cost of these incidents is up **18%** in 2013. [1]
- **70%+** investors want to review an organisation's cyber security practices before investing.
- Nearly **80%** would not consider investing in a company with a history of cyber attacks. [2]

"Put simply, few organizations have kept pace with today's escalating risks - and fewer still are prepared to manage future threats."

PWC

Sources:
[1] PWC - http://www.pwc.com/gx/en/consulting-services/information-security-survey/
[2] HBGary survey - http://www.hbgary.com/article/cybersecurity_directly_affects_investor_attitudes_new_hbgary_survey_finds_survey_reveals



Protect • Comply • Thrive

We can help you address the challenges in 2014 by drawing on our 10+ years of experience and leadership in the IT governance, risk management and compliance (IT-GRC) arena.

Our business-led approach is focused on cost-effectiveness and practicality and is supported by our comprehensive offering of professional resources including books, tools, training courses and consultancy.

www.itgovernance.co.uk

CONTACT US

w: www.itgovernance.co.uk

t: + 44 (0) 845 070 1750

e: servicecentre@itgovernance.co.uk

@ITGovernance

/it-governance

/ITGovernanceLtd


Books


Toolkits


Training


E-learning


Software


Consultancy