Protect ○ Comply ○ Thrive

IT Governance Blog

About Us

Visit our Webshop

Blog Home Business Continuity Cyber Security Data Protection

IT Best Practice IT Governance PCI DSS Other Blogs

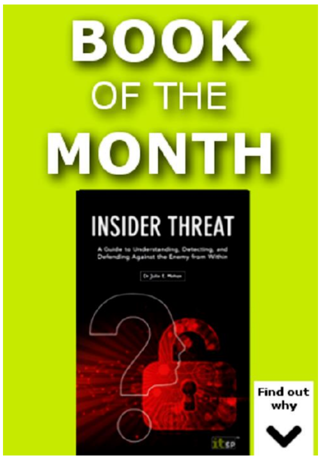
Humans in cyber security – the weakest link

Andrew Wright 13th April 2016

This is a guest article written by Andrew Wright. The author’s views are entirely his own and may not reflect the views of IT Governance.

The cyber security of any organisation can only ever be as strong as its weakest link. The biggest vulnerabilities of a system are not necessarily found within hardware or software, but rather with the people who use it.

IBM’s 2015 Cyber Security Intelligence Index reports that 95% of cyber security breaches are due to human error. To complicate matters, more than half of all security attacks are caused by individuals who had insider access to organisations’ IT systems. Organisations can be responsible for hundreds or thousands of employees, each with their own unique set of behaviours, motives and working practices. Detection technology and security packages, no matter how sophisticated, will always be limited



SOCIAL MEDIA

WRITE FOR US

IT Governance is looking to publish relevant, well-written, informative and original articles. If you have an article that meets these by this human factor.

The disguised threat

Symantec's 2015 Security Threat Report states that 73 spear phishing emails are detected by Symantec every day, and the number of spear phishing campaigns are increasing. Spear phishing campaigns target individuals and organisations to acquire information by masquerading as a legitimate entity. The technique is part of a wider concept known as social engineering, in which humans are psychologically manipulated by exploiting cognitive biases and schema in order to steal information.

Research is often performed on individuals prior to contacting them, usually through social media and company websites, in order to skim valuable information that can provide credibility to an email, or even a phone call. Spear phishing can encourage willing users to unknowingly install malware on their computer or give away personal information and passwords.

The personal touch

If a file or script can be uploaded direct to a computer inside the organisation, then it can effectively bypass all of the existing protection software without detection.

Sometimes this 'personal touch' can manifest itself in the form of baiting. A creatively named USB drive (e.g. 'Upper Management Bonus Scheme 2016') or CD that is left in the coffee room can exploit human curiosity, and provides a simple and effective means of introducing malware to a target computer or system. To complicate matters, IBM's 2015 Cyber Security Intelligence Index reported that 31.5% of all

criteria, then please send it in.

Search the site

Search

CATEGORIES

- Business Continuity
- Cyber Resilience

attacks recorded in 2014 were performed by malicious insiders.

Thinking about the human factor

Human factors is the study of the interactions between humans and their environment in order to improve the capabilities of the human and reduce human error. As cyber crime is quickly becoming a multifaceted, dynamic and constantly evolving threat to security, organisations need to begin spending more time and resources on their employees, and not just their firewalls.

Although human weaknesses are varied between organisations, there are running themes across all reported incidents of cyber crime. Businesses that arrange organisational awareness campaigns, training on best security practices, and building up a questioning and safe working culture can ensure that their employees do not become the next victim of social engineering. The organisation that rewards caution and a questioning attitude will almost certainly save more money and time than the one that is unwilling to put the effort and resources into building up an intelligent workforce within an intelligent working system.

Share now…

Related Posts

ICO issues £180k fines,

Assess the risks of cloud

Trustwave Security

- Cyber Security
  - Cyber Essentials
  - ISO 27001
  - Risk Management
- Data Protection
  - EU GDPR
- IT Best Practice
  - ITIL/ITSM/ISO 20000
  - Project Management
- IT Governance
  - COBIT
  - IG Toolkit
  - ISO 9001
- Other Blogs
  - Book Reviews
  - Breaches and Hacks
  - Fighting cyber crime
  - Guest Posts
  - Law Firms
  - Podcast
  - Product Blog
  - Technical Experts
  - Toolkits
- PCI DSS
- Training
- Uncategorised
- Uncategorized

[illegible] all [illegible] secure professionals have “false sense of security”

About The Author

Andrew Wright

Andrew Wright (MSc) is a consultant with Corporate Risk Associates Ltd and a specialist in Nuclear Physics, Human Reliability Assessment, Human Factors, and Probabilistic Risk Assessment. He has managed and led several projects for EDF Energy including safety critical systems and key operator actions. Andrew is the Secretary for the Human Reliability Assessment Society.