Abstract

Known Unknowns

Phil Cracknell
FBCS, CISSP, Former Cabinet Office Cyber Security Advisor and Award-winning CISO across 8 separate roles and 30 years

Abstract:

TCybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Security can only be accurately assessed, if ways of managing 'non-knowledge' are taken into account. Anyone attempting to measure an organisation's security posture finds that metrics are difficult to collect and don't show the full picture. We also tend to protect against what we know and what we think we know. Knowledge does not come in volumes offering certainty to security decisions. Instead it is an incremental process in which the data reflects but never quite captures the changing security landscape. A steady conversion of unknowns to knowns! Anticipating Blind-Spots! Organisations face complex and uncertain situations every day, but the most challenging circumstances are often completely unexpected, because we never even knew to look for them. Organisations should make efforts to anticipate blind spots. We can never completely eliminate our blind spots, but they can be reduced to improve performance and prevent the mistakes that in hindsight should have been obvious.

Biography:

Phil is regarded as one of Europe's leading information security experts. He has held several CISO (Chief Information Security Officer) roles spanning five different industry sectors and thirty years.

His experience has been gained in a variety of high-profile technology and security management roles, enabling him to offer a unique and captivating insight to the world of information security, cyber-threats and risk management. As national publicity on the subject of 'Wireless security' peaked in 2002, Phil became somewhat of a cyber-security celebrity with appearances on Sky TV, BBC News and in national and industry press. Phil remains highly technical with a hands-on security capability not normally present with someone of his seniority in the industry. He has vast amounts of project success, technical

deliverable experience and can operate at any level. Serving as Group Security & Risk Advisory to Arriva Plc.(2015), Advisor to the Board at Camelot UK (2016/17), a board advisor retained by HomeServe plc (2017-18) and more recently the cyber security lead for the government health checks working for the Cabinet Office (2018-2019). He was the founder and chairman of the non-profit ClubCISO group – www.clubciso.org, is also a non-executive director of the Cloud Security firm Everycloud – www.everycloud.co.uk and board advisory for IP Performance www.ip-performance.co.uk.

Publication of speakers:

1. Significant cyber-intelligence experience with UK Intelligence Services (1993-1995 and 2001-2003) and consulted for recent government cyber-crime initiatives

2. Phil has worked extensively with UK government departments and CESG on the design, implementation and operations of new connections to the government network (GSI/PSI) and ISO 27001 compliance and HMG standards

3. Guest lecturer at Royal Holloway on Fred Piper's Information Security Degree course for several years (2001-200

4. Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: a) Input parameter validation, b) User/Role Authentication & Authorization, c) Session management, parameter manipulation & exception management, and d) Auditing and logging.

5. Former non-executive director for a Scottish investment company - 2016