Editorial Preface

To Speak or Not to Speak when Breeched

Kevin Curran, University of Ulster, UK

OK. You are the CTO of a large company. You are actually about to be taken over quite soon for a large amount. Your network administrator comes to you at 5pm with the news that it seems your network has been infiltrated. The question is, who do you tell? And when?

You see, the public tend to view organisations that are not able to manage customer data as less trustworthy. This is especially true for financial services, government and healthcare organizations. We expect these sectors to hold to a higher standard. They of course are simply afraid of losing precious customers as a result of going public. In fact recent reports have recorded that 8/10 people would "likely" leave a business or service provider if it committed a breach of their personal data.

There is also the factor that a large percentage of breeches are due to negligent insiders. A common percentage reported is that 4/10 organisations had a data breach resulting from a lost or stolen mobile device, including tablet computers, smartphones and USB drives that contained confidential or sensitive data. It seems it is easier to report a 'targeted sophisticated zero-day attack' rather than report a negligent employee.

Primarily it is important to report data breeches as failure to report to the Information Commissioners Office (ICO) will be considered an aggravating factor in serious cases of breeches. In fact, under the proposed EU data directive, companies that commit transgressions can be stung for 10% of their turnover. The ICO states they will impose fines on whoever commits the breach. It is also important for the community also as common means of entry are through default & weak passwords, system bugs and SQL injection attacks and reporting these through the correct channels can lead to consolidated & swift defence mechanisms being rolled out by security professionals. Ultimately, it is incumbent on all organisations to better educate their employees regarding best practices in data protection, and to meet security standards established at their national level.

The actual threshold for reporting is not an exact science but considerations should include the likelihood of damage or distress to data subjects. The higher this is, the more appropriate it will be to report. It is also crucial to take into account the number of data subjects affected. Organisations on the whole should have a breach management plan in

place. They must ensure relevant staff know what the breech plan is and where they can access it. Staff should have clearly defined responsibilities. It is vital to identify as soon as possible if the incident can recur. Steps should be taken in tandem to identify if there are gaps in policies which allowed the breech to happen. Those data subjects affected by the breech should be identified and contacted. Perhaps additional steps to secure their data can be offered at this stage. It is important to send messages to all sectors of the organisation and not just the department affected directly.

The authorities are responding to these breeches by upping the fines and widening the net on those who transgress. The proposed EU data directive, states that companies who commit transgressions can be stung for 10% of their turnover. In fact, this new EU data protection laws will require all companies and organisations to notify the national supervisory authority and affected citizens of any serious data breaches within 24 hours. The Information Commissioners Office in the UK will also impose fines on whoever commits the breach. You have been warned.

Kevin Curran
Editor-in-Chief
IJACI

Kevin, Curran BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr. Curran has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 700 published works. He is perhaps most well-known for his work on location positioning within indoor environments, pervasive computing and internet security. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to BBC radio & TV news in the UK and is currently the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Technical Expert for Internet/Security matters. He is listed in the Dictionary of International Biography, Marquis Who's Who in Science and Engineering and by Who's Who in the World. Dr. Curran was awarded the Certificate of Excellence for Research in 2004 by Science Publications and was named Irish Digital Media Newcomer of the Year Award in 2006. Dr. Curran has performed external panel duties for various Irish Higher Education Institutions. He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computing Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE) and a fellow of the higher education academy (FHEA). Dr. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He is the Editor-in-Chief of the International Journal of Ambient Computing and Intelligence *and is also a member of 15 Journal Editorial Committees and numerous international conference organising committees. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies.*