June 7, 2015

Interpersonal Aspects of Cyber Security

By Robert Axelrod[1] and Larissa Forster[2]

Computer security requires more than safe hardware and well-tested software. It also needs vigilant individuals who accept joint responsibility.

Major vulnerabilities in cyber security are individuals who see no negligence or malfeasance in others, who will hear of none, and will report none. (Figure reprinted with permission of the American Association for Justice.)

[1] University of Michigan, Ann Arbor, MI 48109, USA; e-mail: axe@umich.edu.
[2] University of Michigan, Ann Arbor, MI 48109, USA; e-mail: larissamforster@gmail.com.

Cyber security is essential for the health of the nation's economy and national security. In fact the Director of National Security, James R. Clapper, listed cyber security first among the threats facing America today.[1] The risks include financial loss, loss of privacy, loss of intellectual property, breaches of national security through cyber espionage, and potential large-scale damage in a war involving cyber sabotage.

Cyber security involves hardware, software and wetware. Wetware is the part of the system that drinks coffee. Most efforts to improve computer security focus on hardware and software, but at least as important are problems arising from wetware. Within wetware we need to distinguish between the roles of individuals as users and observers. A focus on individual aspects of wetware is important, but too narrow. The interpersonal aspects also need attention.

Wetware Failures

A specific case in which a computer system that was supposed to have extremely high security was vulnerable due to failures of wetware is DigiNotar, a company that issues trusted certificates to verify that a request on the internet is sent to the proper party. In 2011, hundreds of false certificates for domains including Google and Yahoo were authenticated through DigiNotar by an Iranian hacker. A subsequent audit showed that DigiNotar's vulnerabilities arose from several kinds of negligence, including not updating software, poorly segmenting its network, allowing passwords that were easy to guess, and not using secure logging and server-side anti-virus protection.[2]

The negligence at DigiNotar is hardly unique. A survey of data breaches in U.S. companies found that negligence by insiders was the single largest root cause, accounting for 39% of breaches. Malicious attacks, both from inside and outside, were the second most

common root cause, and systems problems came in only third.[3] The ubiquity of negligence is underscored by an audit of Department of Energy computers which found that 58% of desktop systems were more than three months out-of-date on security patches to protect against known vulnerabilities.[4]

While many attempts are made to improve hardware and software, the user still plays an essential role in computer security. Management, IT and individual employees need to understand that cyber security is best advanced in a company-wide approach. While it is often argued cyber security is best left to specialists, it is better seen as everyone's responsibility. Too many employees are unaware of the dangers and vulnerabilities that can arise from their own computer security workplace behavior. To help the individuals understand their responsibility as a user, organizations need to clearly communicate their computer security doctrine. Further, computer security systems need to make only realistic and minimal demands on its users. For example, system designers should make automatic software updating much easier, and employ new password technology to reduce the burden on the user. Moreover, the organization must minimize false alarms, reward units that do well in audits and avoid meaningless "security theater".

The Need for Peer Reporting

In addition to avoiding individual violations of security procedures, there is an under appreciated need for people who observe a vulnerability caused by a peer to report the problem. A noteworthy violation occurred in Israel's Dimona Nuclear Research Facility when an employee tried using an unauthorized USB flash drive. More alarming is that other workers knew of this breach of security protocol but failed in their joint responsibility to report it.[5] In this case, the

interpersonal control mechanism, namely one person reporting about another, failed. Failure of interpersonal control is widespread and well documented in the organizational literature. In a study of nurses, 40% of those who observed unethical behavior admitted to not reporting it.[6] A study of civil service employees who observed or had direct knowledge of wrongdoing found that 50% admitted not reporting it.[7] Worst of all, in a study of military and civilian employees of a large U.S. military base who personally observed or obtained direct evidence of wrongdoing, 82% admitted not reporting it.[8] In the realm of computer security, the failure to report vulnerabilities caused by co-workers may open the possibility of exploitation by hostile outsiders.

A useful image to teach is the Swiss-cheese model of cyber security adapted from the literature on error management.[9] The idea is that a well-defended organization has several layers of defense, but any of these layers may have vulnerabilities that can be thought of as holes in one of those layers. The layers of defense can then be visualized as slices of Swiss cheese. If the holes in each slice are numerous and big enough, there will be a path through all the layers of defense, making the organization vulnerable to an outside attack. All employees need to understand that their or their co-workers' area of responsibility for cyber security might be the last surviving layer of defense. The Swiss-cheese metaphor also helps to explain why it is dangerous to assume that other people who have observed the same wrongdoing will have already reported it.[10]

The evidence from organizational research on joint responsibility can provide helpful and novel insights for the computer world. Although it is impossible to prevent all wetware problems, let alone all security problems, one area where progress is both feasible and important is in the reporting of problems if and when they are observed. The literatures on norms,

metanorms, whistle-blowing and peer-reporting offer insights for promoting reports of cyber security problems.

1. Clarity of obligation to report. Each organization needs to explicitly communicate its security policies and procedures and detail the consequences for both violations of security protocols and for not reporting observed violations of security protocols. Failures to act according to the policies and procedures should be regarded as serious violations.[11] Rewards should be given to employees following the policies and appropriate punishments to those who breach the policy and/or fail to report an observed breach.
2. Moral obligation. Studies of peer reporting find that a sense of moral obligation is an important motivation.[12] Especially in the realm of computer security, a norm is needed that negligence and misdeeds should be reported so that they can be fixed. There also needs to be a metanorm that one should also report those who see a problem but fail to report it.[13]
3. Ease of reporting. The whistle-blowing and peer reporting literature further shows that employees need to have clear guidelines on how and to whom to report the wrongdoing. Internal tip lines, both anonymous and not anonymous depending on the issue, have been shown to encourage reporting. In fact a recent global study on occupational fraud found that the most common way fraud has been revealed has been through employee reporting encouraged by the existence of proper channels such as internal hotlines.[14] Thus each company should create and communicate proper reporting channels.

4. Protection for the reporter. The organization must guarantee any report through proper channels will not lead to punishment of the reporter, even if the outcome could be embarrassing to the organization or its leaders.[6, 15]
5. Assurance of no excessive punishment. A surprising finding is that often people do not report their peers because of the fear of *excessive* punishment of the wrongdoer.[12] To encourage reporting, clear regulations need to be in place not only to protect the tipster, but also to assure fair and appropriate treatment of the wrongdoers.
6. Assurance that corrective action will be taken. Another frequently cited reason for not reporting is the belief that no corrective action will be taken.[15] A trustful environment is essential for establishing effective reporting channels. The organization needs to make sure the employees trust that reports are pursued. When an organization visibly corrects a problem, trust in the organization is furthered, which in turn leads to a greater willingness to report problems in the future.[8]

Computer security includes technical questions involving secure hardware and well-tested software. In addition, however, there is an urgent need to motivate individuals to accept responsibility for their own part in maintaining "computer hygiene." The interpersonal aspects of wetware need to be an integral part of security protocols and procedures. There is also a need to lower the barriers to reporting negligence and wrongdoing that undermine computer security.

These recommendations are not intended to put the security burden on the user instead of on the software or hardware. They have to be complementary, because even the best software and hardware are vulnerable to failures of wetware. People must be helped to see that the stakes

involve national security and the health of the nation's economy. These computer security considerations need to trump misplaced loyalty to negligent or malicious peers.

Acknowledgements: Supported by the U.S. Air Force Office of Scientific Research through a grant to ARTIS Research & Risk Modeling. We thank David Axelrod, Steve Crocker, Stephanie Forrest, and Amy Saldinger.

[1] J. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Senate Select Committee on Intelligence, Washington, D.C., 2013).

[2] J. Leyden, "Inside 'Operation Black Tulip': DigiNotar hack analysed," *The Register* (6 September 2011); http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/

[3] Ponemon Institute LLC, *2011 Cost of Data Breach Study: Global* (Traverse City, MI, 2012).

[4] United States. *Evaluation Report: The Department's Unclassified Cyber Security Program—2012* (U.S. Department of Energy, Office of Inspector General, Office of Audit & Inspections, Washington, D.C., 2012).

[5] M. Siver, "Dimona reactor workers suspended over security breach," *Y-Net* (16 January 2013); http://www.ynetnews.com/articles/0,7340,L-4333480,00.html

[6] G. King, A. Hermodson, Peer reporting of coworker wrongdoing: A qualitative analysis of observer attitudes in the decision to report versus not report unethical behavior. *App. Comm. Res.* **28**, 309 (2000).

[7] G. Brewer, S. Coleman, Whistle Blowers in the Federal Civil Service: New Evidence of the Public Service. *J-PART* **8**, 413 (1998).

[8] M. Miceli *et al.*, Predicting employee reactions to perceived organizational wrongdoing: Demoralization, justice, proactive personality, and whistle-blowing. *Hum. Rel.* **65**, 923 (2012)

[9] J. Reason, Human error: models and management. *BMJ* **320**, 768 (2000).

[10] P. Fischer *et al.*, The Bystander-Effect: A Meta-Analytic Review on Bystander. *Psy. Bul*. **137**, 517 (2011).

[11] M. Kabay, in *Computer Security Handbook*, S. Bosworth, M. Kabay, Eds. (Wiley, New York, 2002), ed. 4, chap. 35.

[12] G. De Graaf, A Report On Reporting: Why Peers Report Integrity and Law Violations in Public Organizations. *PAR* **70**, 767 (2010); B. Victor *et al.*, Peer Reporting of Unethical Behavior: The Influence of Justice Evaluations and Social Context Factors. *Jour. Bus. Eth.* **12**, 253 (1993).

[13] R. Axelrod, An Evolutionary Approach to Norms. *Am. Pol. Sci. Rev.* **80**, 1095 (1986).

[14] ACFE, *Report to the Nations on Occupational Fraud and Abuse. 2012 Global Fraud Study* (2012).

[15] C. M. DesRoches *et al.*, Physicians' Perceptions, Preparedness for Reporting, and Experiences Related to Impaired and Incompetent Colleagues. *JAMA* **304**, 187 (2010);United States, *A Review of the FBI's Actions in Connection With Allegations Raised By Contract Linguist Sibel Edmonds* (U.S. Department of Justice, Office of the Inspector General, Office of Oversight and Review, Washington, D.C., 2005).