Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches

John W. COFFEY
Department of Computer Science
University of West Florida
Pensacola, FL. 32514, USA

ABSTRACT

A great deal of effort is expended on technological protections against cyberattack. Still, dangerous vulnerabilities and large-scale systems intrusions disrupt organizations with dismaying regularity. Much of the mayhem stems from human error. Much of that human error is on the part of end-users. A large portion of the effort to address cyber security concerns focuses on the hardening of technological infrastructure while placing less emphasis on the role of humans in creating system vulnerabilities. This article is about the interplay of humans with technologies in both causing and potentially ameliorating cybersecurity threats. It addresses the role of errors individuals make in the use of technology that open vulnerabilities, and the roles of both technology and training to protect systems from vulnerabilities created by the people who use them.

Keywords: CyberSecurity, human error, technological solutions, training

1. INTRODUCTION

The growth of utilization of the Internet and World Wide Web as tools for commerce, collaboration and social interactions continues to be explosive and to some degree, fraught with danger. At the end of 2016, one can look back on the multi-million dollar costs associated with cyber breaches of large corporations, the possible role of the successful hack of the Democratic National Committee in determining the outcome of the 2016 U.S. Presidential election, and on countless other smaller losses, both personal and financial, caused by successful cyber security exploits.

Accordingly, cybersecurity concerns are pervasive in contemporary discussions of and research pertaining to technology. Much emphasis is focused upon technological solutions to cyber security concerns, often at the expense of considering important human issues in both creating and ameliorating cyber security vulnerabilities. This short paper will provide a brief overview of issues on both sides of this equation – human sources of vulnerabilities and the exploitation of technological capability and the modification of human behaviors to address cyber vulnerabilities. The remainder of the paper will address the role of human error in creating cyber security vulnerabilities, the use of technology to protect humans from themselves, and the role of heightening security awareness and training to prevent human error.

2. HUMAN ERROR AND CYBERSECURITY

Research results pertaining to the root causes of successful cyber security attacks are somewhat variable, but all major reports point to a significant human error component. Daugherty [9] summarizes BakerHostetler's 2015 and 2016 Data Security Incident Response Reports. The 2015 report reads that 37% of incidents involved human actions or errors and that successful phishing/malware attacks contributed to 25%, accounting for 62% of all incidents. Successful phishing attacks fall in the category of human error as they depend upon duping a user into trusting untrustworthy sources. The 2016 report placed phishing and malware as most common (31%) with employee actions and errors second at 24%. BakerHostetler's reports are based upon breaches the firm helped to manage and included approximately 300 incidents.

According to a IBM's Security Services 2014 Cyber Security Intelligence Index, human error played a role in more than 95% of all security breaches [1] as opposed to those caused strictly by unanticipated vulnerabilities in system security. IBM's report is based upon nearly 1000 clients in 133 countries and literally billions of events per year. IBM reports that human errors include those made by IT professionals such as improper system security configurations and poor patch management, and those made by end-users such as weak or shared passwords, loss of devices containing sensitive information, and the single most prevalent: opening an

unsafe attachment or accessing an unsafe URL. The report describes a typical human error involving the use of social media to initiate an attack. A scenario described is that the attacker contacts a user inside an organization via social media and directs the user to a malicious website or gets the user to open a malware attachment in email. Since the user is using organizational resources, the entire organization is potentially exposed to the exploit.

Howarth [2] describes a range of human errors, again involving end-users inside organizations who do stupid things. Howarth concludes that organizations that implement strong technological security procedures still often pay insufficient attention to human sources of vulnerability, and strongly advocates for enhanced security training. Armerding [8] cites a report that indicates that 56% of workers who use the Internet on their jobs receive no security training at all.

Verizon [4] reports that 63% of confirmed data breaches were facilitated by stealing legitimate passwords that were weak, default or stolen. Point of sale attacks frequently occur and they are often caused by people who use point of sale machines for other uses including web surfing and email [6], and in the process opening an avenue for malware to get into the machine. Verizon estimates that only 3% of phishing attacks are reported by targets of the attacks. The Dridex strain of malware has been used for years to steal usernames and passwords in banking-related phishing attacks [7] and successful attacks depend upon human error.

Social Engineering attacks are those that involve tricking people into bad behaviors such as the IBM scenario described above. One of the most common forms of social engineering attacks is phishing, and surprisingly, phishing attacks still frequently succeed. Modern phishing attacks are much more sophisticated than the old days of "I have 10,000,000 US dollars I am trying to move into the United States" schemes to extract money directly. Modern phishing attacks typically aim at installing malware on targets' machines. Spear phishing attacks are highly sophisticated, being based upon fraudulent emails that appear to be from trusted sources or businesses with which the target of the attack has legitimate interactions.

The preponderance of the literature indicates that attacks (and the human errors that facilitate them) are inevitable and improvements in the ability to minimize impacts through damage control and forensics is critical. Although this is obviously true, one could argue that excessive emphasis is placed upon training to detect and ameliorate the damaging effects of attacks rather than on technologies to minimize the occurrence and effects of human error and on training to minimize human error. The next sections address these concerns.

3. TECHNOLOGICAL SAFEGUARDS

Verizon [4] reports extensively on forensic data pertaining to data breaches. Verizon's report recommends careful analysis of the threat landscape, the formulation of an amelioration strategy, and the prioritization of threat mediation strategies. van Duersen [10] describes a wide range of human errors that expose information systems including improper system configuration and deficient management of security patches, poor authentication procedures including use of default userid/passwords, weak passwords, and sharing passwords, physically losing devices with protected data on them, staying logged in when leaving accessible computers unattended, accessing unsafe websites and opening unsafe emails, and inadvertent sharing of confidential data by sending it to the wrong email address.

Technological safeguards can help with many of these problems. Enforcing encryption of sensitive data at the system level can ameliorate many problems. If data that is on a lost device or inadvertently sent in an improperly addressed email is strongly encrypted, damage is minimized. Encryption entails some time/response penalty that causes users not to want to use it, but it is a very important safeguard. Stringent password management is critical. Technologically enforceable aspects of password management include mandatory (and hopefully frequent) periodic changing of all passwords and checking passwords for strength. Websites are available [11][12] that allow users to check the strength of their passwords, but password management systems can and should be implemented that only allow strong passwords.

Automatic standby locks on computers which turn on after only short periods of inaction are good safeguards for unattended, accessible machines. These locks must be enforceable at the system level because user resistance to them is pervasive. All of the first results of a quick search on "automatic standby lock" describe ways to remove such locks from locally administered machines. Controls over group policies and access, domain trusts, and access roles such as those specified by Flexible Single Master Operation (FSMO) are as

important as they are difficult to administer [13]. Unfortunately, these technological safeguards are only as good as the humans who administer them, which again allows human error at a different level. Built-in operating system-level auditing may be too cumbersome and time-consuming. Dedicated tools to administer these access issues are available and hold some promise of making their implementation more efficient and effective.

4. TRAINING AND OTHER HUMAN-CENTRIC SAFEQUARDS

Training and the building of a security-oriented culture must address those areas where people might accidentally or deliberately circumvent technological safeguards, and areas where no automated safeguards are possible. Users must be made aware of the implications of sharing passwords, the importance of routine encryption of sensitive data, the implications of removing standby locks, etc. van Duersen [10] lists several approaches to human-centric safeguards that range from positive reinforcements for good behaviors to basic awareness campaigns to the threat of termination for bad behaviors. She describes creation of security checklists, making policies and procedures high-profile, creating explicit disciplinary measures for lax security practices and even raising the threat of litigation as measures that can be taken to encourage or coerce people into better security practices.

Woodhouse [15] states that organizations need much more than annual awareness training to modify behaviors of end users. He states that the answer lies in cultivating an information security culture with active participation in good security practices. As is the case with so many papers on the subject, Woodhouse's article is long on platitudes but lacking on details regarding how to cultivate such a culture. SanNicolas-Rocca, Schooley, and Spears [17] conducted an interesting study regarding practices that improve IS security awareness. They found that people who participated in workshops to develop security policies were more likely to apply security measures and to communicate knowledge of such policies to others. Cost-benefit analyses that are difficult to quantify before the fact of a major security breach might shed some light on how much effort an organization should put into such programs.

Nothing about cyber security appears near the top level of the author's university's website. A request for cyber security-related resources at the author's university yielded a link to a university website that contains links to the FBI, DHS, Department of Defense (DOD), and European Network and Information Security Agency (ENISA) sites. Of these, only ENISA was totally focused on cyber security. Of all the information on the university's cyber security website, the National Cyber Security Alliance page had the best practical information, assuming one took the time to find it.

The Department of Homeland Security (DHS) has a clearinghouse website for Cyber security training [14]. Topics include training for cyber security professionals but nothing pertaining to end-users. The National Security Agency (NSA) and DHS have created the designation "Center for Academic Excellence in Cyber Operations" (CAE) for university-level technical programs that contain mandatory knowledge units they specify [16].

The slate of topics in the CAE training is extensive: low-level programming languages, software reverse engineering, operating systems, networks, mobile devices, discrete math, overview of cyber defense, security fundamental principles, vulnerabilities, and legal issues. The curriculum contains nothing pertaining to educating end-users. It is a mystery why, with human error, particularly among end-users, playing such a critical role in cybersecurity attacks, more information is not available regarding how to make rank-and-file people more security-conscious.

5. CONCLUSIONS

Cyber security is enhanced both by improving preventative measures and by improving the efficacy of responses to successful attacks. Two separate reports pertaining to causes of successful attacks were reviewed and they corroborate each other regarding the pervasive role of human error in opening the door to a successful attack. Still, one can find little in the literature with specific recommendations regarding how to implement end-user training to prevent human.

Some literature exists regarding basic topics that might be addressed but efficacy studies regarding the nature of such training – for instance regarding content and frequency – is difficult to find. Future work will involve redoubled efforts to find more regarding more detailed information on the types of human error by various group classifications. Additionally, characteristics of successful programs including content and frequency and on how to foster security awareness in day-to-day activities will be examined.

6. REFERENCES

[1] IBM Security Services 2014 Cyber Security Intelligence Index. Online. Available: https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

[2] F. Howarth. The Role of Human Error in Successful Security Attacks. Online. Available: https://securityintelligene.com/the-role-of-human-error-in-successful-security-attacks/

[4] Verizon. 2013 Data Breach Investigations Report. Online, available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[5] L. Hummer. Security Starts with People: Three Steps to Build a Strong Insider Threat Protection Program Online, Available: https://securityintelligence.com/security-starts-with-people-three-steps-to-build-a-stronginsider-threat-protection-program/

[6] J. Grunzweig. Understanding and Preventing Point of Sale Attacks. Online. Available: http://researchcenter.paloaltonetworks.com/2015/10/understanding-and-preventing-point-of-sale-attacks/

[7] A. Hern. What is Dridex, and how can I stay safe? Online, Available: https://www.theguardian.com/technology/2015/oct/14/what-is-dridex-how-can-i-stay-safe

[8] T. Armerdeing. Security training is lacking: Here are tips on how to do it better. Online, Available:http://www.csoonline.com/article/2362793/security-leadership/security-training-is-lacking-here-are-tips-onhow-to-do-it-better.html

[9] W. R. Daughterty. Human Error Is to Blame for Most Breaches. Online, Available: http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-mostbreaches.htm

[10] N. van Deursen. How to Reduce Human Error in Information Security Incidents. Online. Available:https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/

[11] The Password Meter. The Password Meter. http://www.passwordmeter.com/

[12] UIC Academic and Communications Center. Password Strength Test. Online. Available. http://www.uic.edu/apps/strong-password/.

[13] netwrix. Audit Changes and Prevent Security Breaches or Failed Compliance Audits. Online. Available:https://www.netwrix.com/audit_changes.html

[14] Department of Homeland Security. Cybersecurity Training and Exercises. Online, Available: https://www.dhs.gov/cybersecurity-training-exercises

[15] S. Woodhouse. Information Security: End User Behavior and Corporate Culture. Proceedings of the Seventh International Conference on Computer and Information Technology. IEEE. DOI 10.1109/CIT.2007.186. pp 767-772.

[16] National Centers of Academic Excellence in Cyber Operations. Online. Available: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/requirements.shtml

[17] T. SanNicolas-Rocca, B. Schooley, and J. L. Spears. Designing Effective Knowledge Transfer Prectices to Improve IS Security Awareness and Compliance. Proceedings of the 47th Hawaii International Conference on Systems Science. IEEE. DOI: 10.1109/HICSS.2014.427. pp3432-3441.