LIBERTY UNIVERSITY

Strategic Informer: Student Publication of the Strategic Intelligence Society

Volume 1 | Issue 3 Article 2

September 2013

The Effect of Human Error on Modern Security Breaches

Devin C. Streeter
Liberty University, dstreeter3@liberty.edu

Follow this and additional works at: http://digitalcommons.liberty.edu/si

Recommended Citation
Streeter, Devin C. (2013) "The Effect of Human Error on Modern Security Breaches," *Strategic Informer: Student Publication of the Strategic Intelligence Society*: Vol. 1: Iss. 3, Article 2.
Available at: http://digitalcommons.liberty.edu/si/vol1/iss3/2

This Article is brought to you for free and open access by DigitalCommons@Liberty University. It has been accepted for inclusion in Strategic Informer: Student Publication of the Strategic Intelligence Society by an authorized administrator of DigitalCommons@Liberty University. For more information, please contact scholarlycommunication@liberty.edu.

Operational Security and Cyber Security

The Effect of Human Error on Modern Security Breaches

By Devin C. Streeter

The United States is entering into an era characterized by technological innovation and increased networking and connectivity. This new norm has opened up new vulnerabilities in the realm of cyber security. These weaknesses, however, are increasingly typified by human error and a failure of operational security (OPSEC) that costs the United States and the world massive amounts of financial capital. These errors are typified by a lack of information on security policies, a failure of safe use of social media, misuse of company computers, and repeated use of weak passwords. Potential solutions should be developed with minimal third party intervention and with a focus on informing personnel on internet security.

Operational security has been a concern of U.S. military operations since the Revolutionary War.[1] George Washington personally noted that small details of information must be hidden in order to run an efficient military apparatus.[2] However, with increases in technology, the exploitation risk of private materials grows.[3] With every new technology, from telegrams, to radios, to telephones and the Internet, the convenience of information sharing has opened up fresh weaknesses in the U.S. security and intelligence community.[4]

The United States has seen an escalation of cyber assaults on its military, defense, and technological infrastructures.[5] Reports show that criminals, foreign governments, and private entities have heavily targeted these public and private sectors.[6] Studies show that approximately 28,765 breaches have been reported in the United States in 2013,[7] with 64% (18,410) of breaches occurring in the business sector, 14% (4,027) of successful attacks occurring against the United States government, with the final 12% (3,452) targeting educational centers and 10% (2,877) focusing on the medical industry.[8]

The costs of these attacks are staggering, bleeding the United States approximately $5,403,644 annually and the world around $28,814,844 U.S. dollars per year.[9] When the costs of scams, sabotage, and damages from these attacks are included, the costs become exponential, to the point of costing 1% of the United States GDP.[10] This is a transnational and extremely damaging reality.

The impacts of cyber espionage are grim and devastating in both the private and public sectors.[11] However, the root of all cyber breaches stems from the compromise

[1] LTC Robert G. Michnowicz, "OPSEC in the Information Age," Strategy Research Project, March 8, 2006, 2, accessed October 21, 2013, http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil427.pdf.
[2] Ibid.
[3] NSA, "Purple Dragon: The Origin and Development of the United States OPSEC Program," United States Cryptologic History, Series VI Volume 2, August 22, 2007, accessed October 21, 2013, http://www.nsa.gov/public_info/_files/cryptologic_quarterly/purple_dragon.pdf.
[4] Ibid.
[5] DSS, "Targeting U.S. Technologies, a Trend Analysis of Cleared Industry Reporting," October 1, 2013, accessed October 21, 2013, http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf.
[6] Ibid.
[7] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," Semantic White Paper, May 2013, accessed October 23, 2013, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.
[8] Rapid 7 Corporate Headquarters, "Data Breaches in the Government Sector," May 31, 2012, accessed October 23, 2013, http://www.rapid7.com/docs/data-breach-report.pdf.
[9] "2013 Cost of Data Breach Study: Global Analysis."
[10] Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage," McAfee Security Report, July 2013, 3. accessed October 23, 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.
[11] "Data Breaches in the Government Sector."

of sensitive information.[12] The Center for Strategic and International Studies writes:

> *The most important area for loss is in the theft of intellectual property and business confidential information—economic espionage*.[13]

Similarly, the government has experienced a record increase of attacks targeting "personally identifiable information" in 18 of 24 major federal agencies.[14] This information can be used to steal funds, access classified information, and complete acts of cyber-espionage.[15]

The United States General Accounting Office summarizes the size and scope of the cyber threat thusly:

> *Computers are crucial to the operations of government and business…* [but] *many computer systems and networks were not designed with security in mind… As a result our critical infrastructure is riddled with vulnerabilities that could enable an attacker to disrupt operations or cause damage.*[16]

The reality is that cyber security is a very vulnerable part of both public and private sectors. If not properly protected, the cyber realm offers a vulnerability that can be very easily exploited with minimal effort and consequences on the part of the attacker.[17]

However, there is a much more easily exploited side to cyber security that has been largely unseen in the greater conversation over securing cyberspace: the element of human error and traditional espionage.[18] Human error in cyber security manifests itself in various levels of threat: (1) lack of information on security policies, (2) a failure of safe use of social media, (3) misuse of company computers, and (4) repeated use of weak passwords.[19] These errors come to fruition through poor OPSEC and failures in screening procedures.

Human error is a major contributing factor to cyber breaches. Sources show that human error accounts for 35% - 53.5% of cyber breaches caused by preventable employee error[20] or sabotage from within a company in both the public and private sectors.[21] Simultaneously, the Phenomenon Institute noted that of the 72% of cyber breaches, 35%[22] can be directly traced to individual failure while 37%[23] can be boiled down to acts by "criminal insiders (employees, contractors or other third parties)".[24] These trends are verified by the Defense Security Service (DSS), which noted a staggering 458% increase in the targeting of overseas, U.S.-cleared personnel for information,[25] and a further 43% increase of those seeking employment for the purpose of illicit information acquisition.[26] Simply put, humans can be the weakest link in cyber security.[27] As one professional cyber consultant succinctly states: "Amateurs hack systems, professionals hack people."[28]

---

[12] Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage," McAfee Security Report, 8.
[13] Ibid.
[14] "Data Breaches in the Government Sector."
[15] United States General Accounting Office, "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," United States General Accounting Office Report, May 2004, 1, accessed October 26, 2013, http://www.gao.gov/new.items/d04321.pdf.
[16] Ibid, 26.
[17] Ibid.
[18] IT Governance, "Boardroom Cyber Watch Survey," IT Governance 2013 Report, 8, accessed October 26, 2013, http://www.itgovernance.co.uk/download/Cyber-Watch-Survey-Report-FINAL.pdf.
[19] Kenneth Geers, "Strategic Cyber Security," NATO Cooperative Cyber Defense Center of Excellence, 2011, 40, accessed October 26, 2013, https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.
[20] "2013 Cost of Data Breach Study: Global Analysis."
[21] "Boardroom Cyber Watch Survey," 8.
[22] "2013 Cost of Data Breach Study: Global Analysis."
[23] Ibid.
[24] Ibid.
[25] "Targeting U.S. Technologies, a Trend Analysis of Cleared Industry Reporting."
[26] Ibid.
[27] The Economist Special Report, "The Weakest Link," *The Economist*, October 24, 2002, accessed October 27, 2013, http://www.economist.com/node/1389553.
[28] Ibid.

Of these types of breaches, the poor handling of sensitive information on the internet arises from a misconception of OPSEC.[29] Research Specialist LTC Michnowicz properly articulates the problem with OPSEC procedures in saying:

> *Current OPSEC policy and regulations appear outdated and in need of revision in order to successfully deny US adversaries the ability to gain information… computer technology and communication advances require a renewed internal effort by the United States government to curtail vulnerability in the critical areas of unclassified open source communication networks.*[30]

Social media, the Internet, and the increased connectivity of modern life have transformed cyber space into an OPSEC nightmare.[31]

The reality is that many individuals will not commit cyber espionage personally, but almost all of them will use social media and some facet of the internet for communication.[32] These sites are prime areas for potential cyber criminals to watch for posts on work, policy, and family life.[33] This information is then a primary target of hackers, identity thieves, and foreign intelligence agents.[34] This is a widely acknowledged and serious problem in both the public and private sectors.[35]

It is worth noting that the government sector sets out strict regulations on how to handle the internet and network safely.[36] Army regulation specifies that military personnel must:

> *Consult with their immediate supervisor and their OPSEC Officer for an OPSEC review prior to publishing or posting information in a public forum. This includes, but is not limited to letters, resumes, articles for publication, electronic mail (e-mail), Web site postings, web log (blog) postings, discussion in Internet information forums, discussion in Internet message boards or other forms of dissemination or documentation.*[37]

Many private sector groups have similar stipulations.[38] However, both the Department of Defense (DOD)[39] and private sector[40] acknowledge that security procedures are not adhered to and that there is a general lack of common sense when it comes to internet and technology use.[41] Both public and private sector indicate a deficit of "knowledge about their security strategy"[42] and that many groups lack a cohesive plan for protecting their information.[43]

Part of the problem lies in simple posts on social media, blogs, and websites that can be used for nefarious purposes.[44] The Al Qaeda handbook specifically notes that social media can reveal "Government

[29] Michnowicz, 1.
[30] Ibid.
[31] Geers, 107.
[32] US Army, "OPSEC and Safe Social Networking," US Army Briefing Packet, October 2013, accessed October 27, 2013, http://www.lewis-mcchord.army.mil/des/OPSEC%20Training/SocialmediaandOPSECbrief1.pdf.
[33] Operations Security Professionals Association, "Operations Security," OSPA Briefing Packet, October 2009, accessed October 28, 2013, http://www.opsecprofessionals.org/training/OPSEC_Training.pdf.
[34] "OPSEC and Safe Social Networking."
[35] United States Department of Defense, "Operations Security (OPSEC)," Department of the Army, April 19, 2007, accessed October 28, 2013, http://www.fas.org/irp/doddir/army/ar530-1.pdf.
[36] "OPSEC and Safe Social Networking."
[37] "Operations Security (OPSEC)."
[38] David Sims, "Survey Finds Manufacturers Afflicted with a False Sense of Cybersecurity," Industry Market Trends, October 2, 2013, accessed October 29, 2013, http://news.thomasnet.com/IMT/2013/10/02/ survey-finds-manufacturers-afflicted-with-a-false-sense-of-cyber-security/.
[39] US Army Public Affairs, "Army Operations Security: Soldier Blogging Unchanged," US Department of the Army, May 2, 2007, accessed October 29, 2013, https://www.fas.org/irp/agency/ army/blog050207.pdf.
[40] Sims.
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] "Targeting U.S. Technologies, a Trend Analysis of Cleared Industry Reporting," 53.

personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited)."[45] Electronic capabilities such as geotagging, facial recognition, and global positioning systems (GPS) can also easily reveal locations, activities, and coworkers.[46] Simple things such as privacy settings,[47] user license agreements,[48] and use of plug-ins,[49] can all contribute to a cyber breach if not properly addressed.[50]

Similarly, use of computers in downloading unauthorized materials that can contain spyware, malware, Trojan Horses, and other hacking tools of the trade is a serious problem.[51] Those who download files without confirming their origin run the risk of crashing their system.[52] This is a grave problem in both public and private sector, and has been the cause of multiple cyber breaches.[53]

Yet another easily preventable error in cyber security is reuse of weak passwords.[54] A study released by the U.S. Computer Emergency Readiness Council shows that 89% of web users feel that they use safe password habits.[55] However, the same study notes that 61% of internet users reuse passwords on multiple accounts, 54% have only 5 passwords or less, 44% change their passwords less than once a year, and 21% of those polled have had an account compromised.[56] These statistics fly in the face of safe internet practices.[57] Simultaneously, those who reuse passwords are more likely to use passwords that are easy to guess and are more likely to reveal them to others.[58] This kind of sloppy OPSEC can result in increased susceptibility to phishing.[59] Phishing, the creation of a false webpage to capture username and password, is a very easy and often used tactic.[60] However, weak password security can make a minor inconvenience a catastrophic security breach, giving the attacker access to multiple accounts and a wealth of secure information.[61]

All of these factors are of the utmost concern when it comes to OPSEC practices and cyber security. As noted before, many of these issues are addressed in security protocols.[62] However, there is a steep divide between what institutions teach and what their employees practice.[63] This problem exists despite the weight of evidence and existing barriers; therefore a different focus is key to rectify the damages of poor OPSEC.[64]

However, this reform is best carried out within the existing system and limiting third party involvement.[65] Involving third parties, even those with proper clearance,

---

[45] "OPSEC and Safe Social Networking."
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] "Operations Security."
[51] Geers, 42.
[52] Thomas J. Harvey, "Battling Employee Sabotage in the Wired Workplace," The Center for Association Leadership, November 2001, accessed 30 October 2013, http://www.asaecenter.org/Resources/whitepaperdetail.cfm?ItemNumber=12167.
[53] "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," 24.
[54] Alexa Huth, Michael Orlando, and Linda Pesante, "Password Security, Protection, and Management," U.S. Computer Emergency Readiness Team, December 2012, accessed October 30, 2013, http://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf.
[55] CSID, "Consumer Survey: Password Habits, A Study of Password Habits Among American Consumers," CSID White Paper, September 2012, 3, accessed October 30, 2013, http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf.
[56] Ibid.
[57] Huth, Orlando, and Pesante.
[58] "Consumer Survey: Password Habits, A Study of Password Habits Among American Consumers," 3.
[59] "Dinei Florencio and Cormac Herley, "A Large-Scale Study of Web Password Habits," Microsoft Research, 2007, 8, accessed October 30, 2013, https://research.microsoft.com/pubs/74164/www2007.pdf.
[60] "Consumer Survey: Password Habits, A Study of Password Habits Among American Consumers," 2.
[61] Ibid.
[62] "OPSEC and Safe Social Networking."
[63] Michnowicz, 1.
[64] Ibid.
[65] "2013 Cost of Data Breach Study: Global Analysis."

can greatly increase costs,[66] increase the risks of further breaches,[67] and expand the leaking of further sensitive information.[68] However, the GAO highly recommends that if a third party must be involved, that these companies have cleared personnel, a good reputation in the defense community,[69] and under no circumstances should a company from a foreign country be included, even if they are allies of the United States.[70] Third parties should be avoided when looking for an OPSEC solution, but if they are used they must be from within the United States.[71]

That being said, the bulk of evidence agrees that a successful OPSEC program has been established by the United States.[72] However, the strict enforcement and adaptability of this policy can easily be called into question.[73] Training and enforcement of safe OPSEC is far from ideal due to the fact that it implicitly relies on the "entrusted soldier to practice OPSEC."[74] Serious personal mistakes will always be a problem with both the military and the private sector. However, with increased focus on the threat posed by poor OPSEC in the cyber realm, a greater sense of responsibility may be instilled in employees.[75] The only solution to this particular brand of threat is in constant reemphasis on dangers posed by poor cyber OPSEC.[76]

However, some authors recommend updating OPSEC protocols in both private and public sector to better enforce cyber security.[77] The reality is that while OPSEC has been fiercely defended in the past, 21st century threats require greater adaptation with an emphasis on evolving technology.[78]

In essence, personnel will remain the weak link in United States cyber defenses. The evolution of modern warfare has opened new weaknesses in U.S. infrastructure and industry, but the reality is that traditional espionage will remain a serious threat even in an age characterized by cyber attacks. Human error and OPSEC will remain of the utmost concern, as failure on these fronts will cost millions more dollars in damages and incalculable compromising of classified information. These errors are typified by a lack of information on security policies, a failure of safe use of social media, misuse of company computers, and repeat use of weak passwords. Potential solutions will avoid third parties and will reemphasize the ultimate danger of an individual's poor cyber practices.

---

[66] Ibid.
[67] "Operations Security (OPSEC)," 36.
[68] "Targeting U.S. Technologies, a Trend Analysis of Cleared Industry Reporting."
[69] "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," 181.
[70] "Targeting U.S. Technologies, a Trend Analysis of Cleared Industry Reporting."
[71] Ibid.
[72] Michnowicz, 6.
[73] Ibid, 8.
[74] "Army Operations Security: Soldier Blogging Unchanged."
[75] "Operations Security."
[76] Ibid.
[77] Michnowicz, 1.
[78] Ibid.