EMPLOYEE AND INSIDER DATA BREACHES: VULNERABILITY OR THREAT VECTOR?

Barry S. Herrin, JD, FAHIMA, FHIMSS, FACHE
Founder, Herrin Health Law, P.C.

"Consider that, despite years of cybersecurity awareness and training, most staff's kneejerk reaction to finding a 'lost' USB drive is to plug it into a corporate PC in order to read through the files or to identify the owner."[i]

"We have met the enemy, and he is us."[ii]

Introduction

According to a 2014 IBM study[iii] cited by the Institute for Critical Infrastructure Technology in its 2016 report[iv], 31.5% of all cybersecurity incidents in 2014 were perpetrated by malicious insiders, and 23.5% resulted from the activities of non-malicious insider threats. In 2017, statistics reported by the MIT Sloan Interdisciplinary Consortium showed an increase in the likelihood of insider threats, as between 67% and 80% of cybersecurity incidents were linked to persons with legitimate access to the breached data infrastructure.[v] A 2018 Ponemon Institute report[vi] confirms that this upward trend is not abating, as 64% of successful cyber attacks resulted from privileged user negligence, with another 23% being perpetrated by malicious insiders – a total of 87% of all incidents.

Given that a paucity of effective technological controls exists to prevent persons with legitimate access to systems from clicking on attachments or responding to messages utilizing a business email compromise (BEC) gambit, and thereby becoming unwitting participants in a cyber attack, perhaps it is time to consider a change in how we view the employee who "accidentally" (read "negligently") facilitates cyberintrusions. In other words, education having failed in many instances, and with criminals becoming ever more sophisticated, perhaps employers should consider their employees threat vectors and not innocent victims in cybercrime. Doing so could change how organizations respond to the growing threat landscape without the need for an increase in technology purchasing or an increase in internal security personnel hiring. "External threats are typically addressed with perimeter defenses which have now been rendered useless against these new attack methods which leverage existing communication paths and user accounts. A new model for protecting organizations is required."[vii]

Change Your Human Resources Mindset

For organizations that wish to focus on people and processes rather than on technology in their cybercrime change management exercise, executives and risk managers have known for some time that the most significant changes organizations undertake is to change corporate mindset and culture.[viii] That same study also shows that top management sponsorship of the desired change, coupled with employee involvement, honest communication, and a corporate culture that promotes and reinforces the change, can provide a higher degree of success.[ix]

Big Decision 1: Changing Training Focus from "Threat Prevention" to "Patient Safety"

As this author previously wrote[x], changing the approach of cyber hygiene training in the healthcare environment from one of information technology (which is perceived as the "business" of the information technology department) to one of patient safety (which is perceived as everyone's business) might yield significant improvement. However, the enterprise must convince its employees that such steps are necessary to protect patients from injury. Two studies in this regard should be persuasive. First, in one study conducted using the VA health system EHR, 24 of 100 incidents surveyed caused a patient care error due either to software design conflicts, inappropriate access credentials, or to corrupted files or databases that prevented entry of diagnoses and orders or retrieval of patient information.[xi] In another study, 80,381 EHR event reports were analyzed, and 76 of those reported incidents described a patient safety issue that correlated to EHR unavailability. The majority of the patient safety issues resulted from lab order and result irregularity, with the second most common issue being medication administration and order errors.[xii]

In the healthcare environment, human resources decisions that align internal cybersecurity with patient safety initiatives could use the fall risk prevention approach that seemed very effective in the early 2000s. Components of this approach might include the following:

- Empowering employees to report suspect behavior of others[xiii];
- Providing a main emergency line to obtain response for the "inadvertent click";
- Calling a "code" when suspicious cyber activity occurs or when external actors attempt to compromise business systems with phishing, BEC, or other exploits;
- Rewarding employees who respond favorably to training[xiv]; and
- Publishing results of non-compliance with enterprise directives in the manner that patient care risk results are.[xv]

Big Decision 2: Empower Employee Surveillance

Employees who actually pose a significant insider threat may not initially draw attention to themselves; however, academic research indicates that they cannot hide their disruptive behavior for a long period of time.[xvi] Consequently, loyal employees who see what might otherwise be imperceptible shifts in behavior may be one of an employer's most critical assets in determining who may be an insider threat. Facilitating and training employees to recognize patterns of behavior or unique wrongful conduct, and providing incentives for reporting that conduct, is critical to changing the workplace environment to one of compliance and away from one of complacency.

The Office of Intelligence and Analysis of the U.S. Department of Homeland Security, in coordination with the Federal Bureau of Investigation, published a reference aid on "Insider Threat Behaviors and Mitigation Responses" in March of 2017.[xvii] Although this guidance was designed for the public sector and persons accessing government information technology resources, it is instructive to the private sector as well. The Insider Threat Reference Aid lists a series of

suspicious activities that could be evidence of an insider threat and which should be reported to management:

- Document collection, copying, or movement from one storage location on a system to another or onto portable media;
- Any use of unauthorized devices, drives, or data storage media;
- Excessive or continuous printing of documents in a manner different than previously usual;
- Carrying a computer, tablet, or briefcase when not previously required for work obligations;
- Maintaining or changing work hours in an abnormal way, such as a pattern of early mornings, late evenings, weekends, and the like when persons in similar job classifications do not have similar work expectations; and
- Excessive failed login attempts, attempts to access controlled domain architecture, multiple attempts to increase legitimate data access, and the like.[xviii]

Separate and apart from suspicious activities, potential insider threats display certain types of suspicious behaviors. These have been developed in coordination with behavioral scientists at the Carnegie Mellon University's Software Engineering Institute[xix], and include the following:

- Employees who are consistently disgruntled, angry, or perceive that workplace injustices routinely occur against them may be more likely to agree to engage in harmful behavior or may be "susceptible to exploitation by an adversary."[xx]
- Employees who constantly manifest a feeling of being undervalued, underpaid, passed over for promotion, or who are not included in activities with others of their job level or seniority will begin to demonstrate a lack of regard for the organization and their peers or may "take what they're entitled to" in violation of company policies or applicable laws or regulations or hold employer assets hostage.[xxi]
- Any persistent pattern of negative performance, such as chronic absenteeism or unexplained tardiness, inability to accept constructive criticism, rejection of or internal complaints about scheduled job performance evaluations, or the need to blame others for mistakes display inappropriate workplace attitudes that could degenerate into harmful or malicious conduct.[xxii]
- Employees who demonstrate a tendency to routinely violate workplace rules because they perceive themselves as better than their peers or "above the law," or employees who "habitually defy the commonly accepted rules of society".[xxiii]
- Employees who suddenly begin to display stress, anxiety, or anger in the workplace due to workplace or life changes (family illness, divorce, stress of remote working, etc.) can be an attractive target for manipulation or exploitation.
- Employees who exhibit changes in spending behavior or display signs of unexplained financial gain can be using customer credit card information for personal gain or could be siphoning enterprise resources to personal accounts, or could simply be selling industrial secrets to competitors or criminals.[xxiv]
- Employees with substance use, abuse, or dependency problems use stolen resources to support their habit, and knowledge of addiction can be exploited by outsiders to leverage the insider.[xxv]

Comments from the FBI in numerous presentations and encounters would simplify it this way: "Define what your 'normal' is; then look for people who are not acting 'normally'." Training workforce members on what "normal" performance in their job or environment looks like and encouraging them to report aberrant behavior – even if there may be a perfectly reasonable explanation for it – will start a culture shift away from complacency. Because security is an "inside risk" fundamentally, "insiders" need to be empowered to help solve it.

Big Decision 3: Treat Information Technology Access as a Privilege and not a Right

Because we know what some of the common behaviors and activities are for a significant number of insider threat actors (whether intentional or simply negligent), human resource policies and practices should change to screen out those risks, both at initial hire and during the person's tenure at the enterprise. Some examples of these types of screening activities would include the following:

- Thorough background checks on employees, to include prior criminal convictions[xxvi] and discussions with former employers regarding whether the potential hire displayed any of the suspect behaviors identified with higher insider risk;
- Employees with access to enterprise financial assets or customer credit card information should have credit checks at a minimum, and a fidelity bond should be considered for key employees with financial responsibilities;[xxvii]
- Apply the same screening criteria to full- and part-time employees, as well as to independent contractors;
- Define access to information technology by role, and include this role-based access in job descriptions for each position within the enterprise;
- Monitor access to information technology resources, and set reasonable employee expectations to privacy when using employer-provided assets; and
- When employees promote within the enterprise or gain new or different levels of access to information technology resources or datasets, mandatory rescreening as if the employee were a new hire should be conducted.[xxviii]

Big Decision 4: Cutting the Cord to Social "Notworking" Sites and Personal Email Accounts

The growth of social engineering[xxix]-based targeted cyberattack should make every enterprise extremely wary of employee access to social media. Information gained from social media sites can lead to targeted phishing attacks or even to criminal outsiders (or mischievous insiders) guessing an employee's passwords. Additionally, and as with any case of "cyber stalking," attackers can learn about an employee's workplace, his or her level of satisfaction with work, names of supervisors, and other information making an intrusion attempt (or an attempt to convert the employee to a willing participant in a criminal endeavor) more successful. Finally, with access to personal social media sites and individual email accounts through the enterprise's Internet channels, the enterprise's systems can more effectively be exposed to malware and to the easy ability of employees and others to exfiltrate enterprise data without much notice.

The problems of access to enterprise data systems with personal devices encountered by many actually suggests a solution to the social-networking problem in part, and that is to eliminate access

to all social media and commercial email sites on enterprise technology assets, and instead require employees to use their personal devices to access these platforms. Furnishing a separate secure Internet access point for employees also helps limit the possibility that malware and other exploits could be downloaded to personal devices or those of visitors and others without direct access to the enterprise's Internet "pipe" or data repositories. Finally, systems should be configured so that the "lazy" password problem does not continue. Seven of the top ten most used passwords from 2017 are the same as prior years.[xxx]

However, as with many cyber activities, technological controls alone do not solve the social media problem. A certain amount of what the military would call "operational security training to increase situational awareness" is required. Employees need to be taught how cybercriminals "harvest the bounty of the Internet" from social media sites to engage in socially engineered exploits, such as hacking online user forums where employees seek workarounds to employer data use restrictions or surveilling social media site public posts to determine which employees at a particular employer are disgruntled.[xxxi]

The risk to the individual employee's workplace environment based on his Internet presence should also be illustrated. The Common Sense Guide suggests a live demonstration of "ethical hacking" using publicly available employee social media information to infiltrate a system.[xxxii] Additionally, enterprises should not permit employees to use commonly available personal information to reset internal passwords – use of ZIP code, mother's maiden name, place of birth, and similar pieces of information known to be prevalent on social media sites can increase internal vulnerability if used by the enterprise to validate an employee's identity.[xxxiii] Finally, targeted phishing exercises can be used to illustrate how criminal actors gain access to systems and email accounts, thereby heightening employee awareness of the risk of "cross-pollenation" between work and personal online presences.[xxxiv]

All of the foregoing activity is dependent on robust and targeted enterprise policies on Internet and social media use and abuse. Policies should clearly describe how much online privacy an employee has when using employer IT resources, should describe how employee access is monitored and audited, should eliminate or severely limit access to personal email accounts and social media sites from employer resources, should establish clear punishments for violating or attempting to work around any employer IT restrictions, and should set parameters for what employer data (including employee-specific data) can be made public on social media sites.[xxxv]

Big Decision 5: Incorporate IT Issues into the Termination Process

Once a decision has been made to fire an employee – any employee – then the human resources, physical security, and information technology departments need to collaborate on the termination process. The exit process is more than a financial and benefits checklist. When an employee leaves the enterprise, their position as a potential cybersecurity threat will persist if they are not "offboarded" with the same care that they are "onboarded."

First, physical and cyber access to critical systems and spaces should be terminated at the time the decision to terminate is affirmed, and not during the exit interview. The old wartime admonition that "loose lips sink ships" applies inside the insular workplace environment with a vengeance,

and any rumor of termination reaching a disgruntled employee could provide the trigger for cyber-mischief. Keycards, passwords, and other tokens allowing access to employer resources should be disabled prior to the exit interview, and door keypad codes should be changed. Among other things, this will prevent the employee from exfiltrating any data on those devices prior to their turn-in or sending inappropriate emails to co-workers, clients, or customers.

Second, any trusted devices issued to the employee (laptops, portable media, cellphones) should be removed from the list of such devices at the same time as the employee's access to IT systems is removed. Employer-owned cellphones are a particular risk here, and consideration should be given whether to engage in the "lock-wipe-kill" cycle to prevent exfiltration or corruption of data.

Third, when any employer-furnished devices are collected from the employee at the exit conference, forensic examination of those devices should be undertaken immediately to determine if data was compromised or exfiltrated.

Fourth, all keys, cards, workplace identification cards and badges, uniform items, and other means used to gain physical access to the employer's spaces should be confiscated and accounted for, and – even if accounted for –certain physical locks should be considered for change.

Finally, the workforce should be informed of the employee's termination, and reception and security employees should be given a photo of the employee accompanied by instructions should the employee appear at any employer workplace location. More than one security breach has occurred because those minding the doors were not told of the employee's termination.[xxxvi]

Big Decision 6: Deciding ***When*** to Shift from Education to Punishment is Critical

Employee negligence that causes a business either financial or reputational harm is almost always dealt with in disciplinary terms in every environment except the information technology environment, and only in health care is there an external audit and oversight structure that virtually mandates employee discipline for wrongful use or disclosure of a patient's "protected health information."[xxxvii] "Every time an employee clicks a malicious link, visits a watering-hole site, opens a malicious attachment, etc., he subverts organizational cybersecurity and invites adversaries to infiltrate, compromise, and infect the network."[xxxviii] However, only in the most catastrophic circumstances are employees subject to significant discipline for violation of the enterprise's email hygiene, password, and other polices designed to mitigate the risk of insider threat.

This is not merely a conflict between the generations: studies indicate that over half of insider threat incidents are caused by employees who routinely violated known enterprise information technology policies.[xxxix] However, younger employees will perceive this as a challenge to their "way of life," and the lack of connectivity (sometimes manifesting itself as FOMO (fear of missing out) or more classic narcissistic behavior) will create awkwardness within the workplace, particularly in those that are dependent on the Internet. Nevertheless, the data now show conclusively that a systemic failure to hold employees accountable for intentionally bad or clearly irresponsible behavior can have enormous financial consequences for data-drive enterprises.

Notice here that the decision is not ***whether*** to punish continued negligence in email hygiene or in not following employer technology policies, but only ***when*** to make that shift. With over a decade of internal training on privacy, cybersecurity, typical cybercrime exploits, and the increasing prevalence of cyberattack in all industries, businesses must decide when enough truly is enough and when employees should start to be disciplined rather than re-educated (or re-re-educated) for what clearly is negligent conduct.

Change Your Mindset About "Best Practices"

A 2016 NIST report[xl] examining the use of the Cybersecurity Risk Management Framework captured responses to a Request for Information (RFI) and comments from workshop participants in April of 2016. The report stated that those involved reached consensus that the term "best practice" sharing should simply be "current practice" sharing or else merely "practice" sharing, because the moniker of "best" should be "reserved for practices that are measured and adjudicated as truly beyond others in practice" and "conferred by an impartial organization, recognized for its cybersecurity expertise."[xli]

This highlights a critical component of the intersection of cybersecurity and legal compliance: unless there is an absolute standard against which a business can be audited or for which failure to meet such can result in civil or criminal sanctions, all cybersecurity exercises are simply risk mitigation controls against financial, reputational, or performance losses. In this regard, the healthcare industry has a strange blessing in the HIPAA Privacy and Security Rules[xlii], which mandate the preservation of the confidentiality, availability, and integrity of electronic protected health information.

One other factor needs to be considered in light of this legal/technological intersection, and that is the risk incurred in holding oneself to a standard higher than that imposed by law. The typical analysis of product defect against a governmental framework is articulated in *Sexton v. Bell Helmets, Inc.*, 926 F.2d 331 (4th Cir. 1991):

> A defect can therefore be identified by measuring the product against a standard articulated expressly by government or industry or established by society in its expectations held about the product at the time of its sale. While government and industry standards are readily identifiable for a given product at a given time, the reasonable expectation of purchasers requires a factual examination of what society demanded or expected from a product. This may be proved from evidence of actual industry practices, knowledge at the time of other injuries, knowledge of dangers, the existence of published literature, and from direct evidence of what reasonable purchasers considered defective at the time. While society demands and expects a reasonably safe product, an examination of societal standards at any given point in time usually reveals an expectation that balances known risks and dangers against the feasibility and practicability of applying any given technology. …. With respect to the [seatbelt hypothetical mentioned earlier in the court's analysis], society did not consider an automobile manufactured in the 1950's defective merely because it had no seat belts. Likewise, society does not currently expect automobiles to be manufactured to eliminate all risks of blindspots when operated in reverse. Existing

> technology would undoubtedly permit rearview video cameras or beeper warnings which could operate while the automobile is in reverse. Nevertheless, the automobile would not be considered defective because it is not equipped with these devices. In short, a product can only be defective if it is imperfect when measured against a standard existing at the time of sale or against reasonable consumer expectations held at the time of sale. There is no evidence in this case that purchasers of motorcycle helmets in the 1979-81 period, when the Bell Star III helmet was designed, manufactured and sold, reasonably expected a higher level of protection than that called for by the existing government and industry standards.[xliii]

Those participating in the Framework Feedback stated that, in the absence of a verified and specifically adopted industry standard, they did not want to endorse or promulgate any practices as "best" or "recommended" for fear that they would be held to these standards in the event of a security incident.[xliv]

Conclusion

As noted in the Common Sense Guide,

> Organizations often focus too much on low-level technical vulnerabilities. For example, many rely on automated computer and network vulnerability scanners. While such techniques are important, … vulnerabilities in an organization's business processes are at least as important as technical vulnerabilities. In addition, new areas of concern have appeared in recent cases, including legal and contracting issues…. Many organizations focus on protecting information from access by external parties but overlook insiders. An information technology and security solution that does not explicitly account for potential insider threats often gives the responsibility for protecting critical assets to the malicious insiders themselves.[xlv]

Even the FBI acknowledges that it is impossible to perfectly "profile" an insider threat. No single behavior or series of suspicious actions can definitively identify a rogue employee or a continuous screw-up. "Detecting and mitigating insider threats will almost always rely on the identification of concerning workplace behaviors in combination with select types of suspicious activity."[xlvi] Technological savvy and deploying good monitoring tools are certainly part of the solution; however, the use of trained employees to gather the "human intelligence" necessary for risk managers to spot and interdict the insider threat remains critical for overall cybersecurity success. Human beings[xlvii] remain "the weakest link" in the cybersecurity chain of defense for all organizations, and, as can be seen from the above, global cybercrime relies on employees continuing to do the wrong thing inside critical information systems to make cyberattacks successful and costly. Pogo had it right.

Barry S. Herrin, JD, FAHIMA, FACHE is the founder of Herrin Health Law P.C. in Atlanta, Georgia. Herrin has over 25 years of experience practicing law in the areas of healthcare and hospital law and policy, privacy law and health information management, among other healthcare-specific practice areas. He is both a Fellow of the American College of Healthcare Executives and a Fellow of the American Health Information Management Association and holds a Certificate in Cyber Security from the Georgia Institute of Technology.

---

[i] "In 2017, The Insider Threat Epidemic Begins," James Scott and Drew Spaniel, Institute for Critical Infrastructure Technology, February 2017 (hereinafter the "ICIT Report), p. 13.
[ii] Pogo Possum, written by Walt Kelly on his famous Earth Day poster, April 22, 1970.
[iii] "IBM 2015 Cyber security intelligence index," 2015. [Online]. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03278USEN&attachment=SEJ03278USEN.PDF&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US.
[iv] ICIT Report.
[v] Remarks by Stuart Madnick, Co-Director, at the 2017 HIMSS Healthcare Security Forum ("Madnick Remarks").
[vi] Ponemon Institute LLC, "2018 Cost of Insider Threats: Global", April 2018
[vii] David McNeely, Vice President of Product Strategy, Centrify, quoted in the ICIT Report.
[viii] "Making Change Work Study: Continuing the Enterprise of the Future", IBM Global CEO Study, 2008, p. 12, available at http://www935.ibm.com/services/us/gbs/bus/pdf/gbe03100-usen-03-making-change-work.pdf
[ix] Id. At p. 13.
[x] http://www.healthcareitnews.com/blog/what-can-anti-phishing-efforts-learn-fall-prevention-strategies
[xi] https://academic.oup.com/jamia/article/21/6/1053/2909293/An-analysis-of-electronic-health-record-related?searchresult=1
[xii] http://www.beckershospitalreview.com/healthcare-information-technology/5-study-insights-into-patient-safety-events-when-ehrs-go-down.html
[xiii] More on this below.
[xiv] https://www.csoonline.com/article/2132618/phishing/social-engineering-11-tips-to-stop-spear-phishing.html.
[xv] http://www.hhnmag.com/articles/6404-Hospitals-work-to-prevent-patient-falls. The article specifically mentions a hospital posting the results of fall risk compliance of staff members by name in employee workspaces.
[xvi] Journal of Strategic Security; vol IV, issue 2; Summer 2011; "Modeling Human Behavior to Anticipate Insider Attacks"; https://scholarcommons.usf.edu/jss/vol4/iss2/3; accessed on 15 SEP 16.
[xvii] Hereinafter the "Insider Threat Reference Aid."
[xviii] "Protecting Your Organization from Insider Threats," Georgia Institute of Technology Applied Research Corporation, March 30, 2017, p. 115.
[xix] Common Sense Guide to Mitigating Insider Threats, Fifth Edition (CMU/SEI-2016-TR-015). Retrieved May 22, 2018, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484738 (the "Common Sense Guide")
[xx] Insider Threat Reference Aid p.2. These threats can be either competitors, criminals, or foreign intelligence agencies or assets.
[xxi] As reported on www.sfgate.com in October of 2003, a woman in Pakistan doing remote coding for the UCSF Medical Center threatened to post patients' confidential files on the Internet unless she was paid more money. This was the first recorded use of cyberextortion in the healthcare industry following the adoption of HIPAA. It has not ceased.
[xxii] Ninety-two percent of insider threat cases studies in a 2016 CERT report were preceded by a negative workplace event. http://www.digitalgovernment.com/media/Downloads/asset_upload_file133_5604.pdf.
[xxiii] https://www.metrostarsystems.com/cyber-security/common-behaviors-insider-threats/, citing the Common Sense Guide. Also, see http://www.digitalgovernment.com/media/Downloads/asset_upload_file133_5604.pdf, which reports that fifty-one percent of employees involved in an insider threat scenario had a pattern of routinely violating enterprise information technology policies.

[xxiv] The Common Sense Guide, p. 38. Movie buffs will remember Richard Pryor's character in *Superman 3* transferring all of the business's rounding errors into a separate account and then purchasing a Ferrari with the stolen funds.
[xxv] https://insights.sei.cmu.edu/insider-threat/2018/04/substance-use-and-abuse-potential-insider-threat-implications-for-organizations.html. In healthcare, the deliberate insider threat seems to be concentrated on physicians engaging in typical drug diversion behavior, such as selling prescriptions, self-prescribing through strawmen, or fraudulent insurance billing for imaginary visits in exchange for issuing prescriptions to addicts.
[xxvi] Criminal background checks may only be used to screen employees for crimes that are reasonably related to the scope of work or that would indicate an increased risk to the employer. https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm#VIII. A conviction for misdemeanor marijuana use, for example, would not disqualify someone from performing financial transactions work, particularly if the employer also maintains a drug free workplace and could test employees for drug use post-employment.
[xxvii] The Fair Credit Reporting Act requires employers to obtain permission from job applicants and existing employees. 15 U.S.C. Section 1681(b)(3)(B).
[xxviii] NIST Special Publication 800-53, Identification & Authentication Control IA-11. "In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii) when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically."
[xxix] "Social engineering may be defined as obtaining information or resources from victims using coercion or deceit. During a social engineering attack, attackers do not scan networks, crack passwords using brute force, or exploit software vulnerabilities. Rather, social engineers operate in the social world by manipulating the trust or gullibility of human beings." Common Sense Guide, p. 53, citing Raman, Karthik et al. Ch. 19, "Social Engineering and Low-Tech Attacks." Computer Security Handbook, 5th ed. John Wiley & Sons, Inc., 2009.
[xxx] http://mentalfloss.com/article/522128/here-are-most-commonly-used-passwords-2017. The top four passwords are "123456", "password"/"Password", "12345678", and "qwerty."
[xxxi] Common Sense Guide, pp. 53-54.
[xxxii] Common Sense Guide, p. 54.
[xxxiii] Id.
[xxxiv] NIST Special Publication 800-53, Identification and Authentication Controls, IA-4, Control Enhancement (1): "The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts."
[xxxv] A list of social media policies and templates are available at http://socialmediagovernance.com/policies.php
[xxxvi] See as an example http://www.dailymail.co.uk/news/article-2766868/Ex-UPS-employee-walks-company-warehouse-shoots-two-former-workers-dead-turning-gun-himself.html and https://www.aol.com/article/news/2017/06/05/multiple-fatalities-in-workplace-shooting-in-orlando-florida/22126385/
[xxxvii] 45 C.F.R. Section 164.530(e)(1).
[xxxviii] ICIT Report, p. 13.
[xxxix] http://www.digitalgovernment.com/media/Downloads/asset_upload_file133_5604.pdf.
[xl] "Cybersecurity Framework Feedback: What We Heard and Next Steps," National Institutes of Standards and Technology, U.S. Department of Commerce, June 9, 2016 (the "Framework Feedback")
[xli] Framework Feedback, pp. 3-4.
[xlii] 45 C.F.R. Parts 160 and 164.
[xliii] *Sexton v. Bell Helmets, Inc.*, 926 F.2d 331, 337 (4th Cir. 1991).
[xliv] Framework Feedback, p.4.
[xlv] Common Sense Guide, p.47.
[xlvi] Insider Threat Reference Aid, p.4.
[xlvii] Lovingly referred to by some of my security colleagues as the "organic chair-keyboard interface."