CORNELL HR REVIEW

A NEW ROLE FOR HUMAN RESOURCE MANAGERS: SOCIAL ENGINEERING DEFENSE

Scott Seidenberger

The general risk of social engineering attacks to organizations has increased with the rise of digital computing and communications, while for an attacker the risk has decreased. In order to counter the increased risk, organizations should recognize that human resources (HR) professionals have just as much responsibility and capability in preventing this risk as information technology (IT) professionals.

Part I of this paper begins by defining social engineering in context and with a brief history of pre-digital age attacks. It concludes by showing the intersection of HR and IT through examples of operational attack vectors. In part II, the discussion moves to a series of measures that can be taken to help prevent social engineering attacks. In all, this paper aims to accomplish two goals:

1. Provide a general overview of why HR managers should be involved in social engineering defense.
2. Highlight three specific areas in which HR managers can affect positive change. These are managing corporate culture (with an emphasis on the physical workspace), proactive incentive management, and smart use of penetration testing.

Part I — Problems

Human Resource Departments are Lucrative Targets

Social engineering attacks have become an ever-increasing and potent threat to the information security of organizations. Because these attacks aim to infiltrate information technology systems, the responsibility of defending against them has fallen on IT departments. However, it is actually human resource departments that have been increasingly the target of malicious actors. A SANS Institute white paper from 2008 identified HR departments as highly vulnerable targets of social engineering attacks and states that they "should be highly trained" to make sure they do not become the victim of an attack.[1]

One reason that HR departments are attractive targets is that they hold lucrative information that attackers seek, such as information on all employees and detailed company directories. Additionally, HR departments and managers are constantly engaging with those outside the organization, especially when recruiting. Hackers have been able to use recruitment web services such as CareerBuilder and Monster to deploy malware on weakly defended HR computers.[2] While groups such as SANS have emphasized the need for human resources departments to become less vulnerable to social engineering, they rarely recognize that HR departments are also

uniquely positioned to improve security throughout the organization. This paper calls for social engineering defense to be included as a new role for the HR manager.

Definition and History

Human brains have evolved to process an incredible amount of sensory data in an attempt to make sense of a dynamic and complex world. To add yet another layer of complexity, humans are social animals who have also evolved mechanisms for interacting with one another to form sophisticated relationships. To date, the human brain is the most efficient data processor of its size, able to complete an unimaginable number of operations per second, with less energy consumption than a dimly lit lightbulb.[3] Similar to machines, however, there is a limit to the ability of the human brain. We have limited cognitive resources, which, like the processors and memory of a machine, can be overloaded, misallocated, or underutilized.

The brain would easily become overloaded if it tried to fully process every bit of information that it was given from sensory input. At its core, social engineering is the systematic process of exploiting the vulnerabilities of our learned sociality. It is a process of psychological and social manipulation that takes advantage of the shortcuts of our brain, known as heuristics, to process information efficiently. It also relies on taking advantage of cognitive biases that arise from our constructed social reality.[4]

Social engineering has existed for thousands of years under different names. The word "engineering" in social engineering takes on multiple meanings depending on the context. First, it could mean that the deception was specifically crafted for a specific target or set of targets, custom-tailored for a specific effect. Secondly, it could mean that the deception is one part of a complex process with many steps. In either case, engineering does not imply that these concepts are limited to technological systems, but rather it does show that social interactions can be engineered to have, or be more likely to have, certain outcomes. In order to understand how contemporary social engineering attacks are successful and how they can be mitigated, we look to the great social engineers outside of the technology sector.

The "Old School"

Before the advent of computing and networked information systems, social engineers, or "human hackers" constructed elaborate ruses that took advantage of human nature to achieve their goals. For example, one of the most recognizable tales from ancient Greek history is of Ulysses and the Trojan Horse.[5] The Greek army played to the curiosity and naivety of the Trojans, and were able to achieve their military victory without having to face the outward defenses at all. Regardless whether this is myth or fact, it emerged as a precautionary tale about the potency of manipulating others' psychological failings.

Trust and confidence became such crucial concepts to understanding how social engineering works that in the mid-1800s in America, the term "confidence man" was coined after the schemes of William Thompson.[6] Thompson would approach those of the upper class and would strike up a conversation, pretending that he knew them. He was skillfully able to create a false air of authority where he gained the trust of his target. He would then directly ask his target: "Have

you the confidence in me to trust me with your watch until tomorrow?" This direct approach seems like it would not be effective, but it illustrates the fact that even a small amount of earned trust is incredibly powerful.

Social and psychological manipulation schemes still capture mainstream media attention today. We can look to the likes of imposters like Frank Abagnale and James Hogue, and the Ponzi-scheming Bernie Madoff. These criminals all relied on building relationships with their targets; they were charismatic and were experts in creating an artificial level of transparency and authority with their victims. From these historical examples, one can see that successful social engineering techniques have focused on exploiting a trust relationship. Now, we look at how trust relationships have changed or stayed the same today.

The "New School"

Information technology has significantly changed the way social engineering is conducted. The "New School" of social engineering is about exploiting the same human failings as in the "Old School," but with the aim of compromising information systems at the expense of the end users of those systems. Information technology has not changed the incentives or motives, but it has changed risk calculations in important ways. Risk can be defined as a product of the frequency, rate of success, and severity of social engineering attacks.

$$Risk = Frequency * \ Rate\ of\ Success * Severity$$

There are at least two ways in which information technology increases the threat, or frequency, of social engineering attacks. For one, attackers can now automate many attack vectors, such as spear phishing, to cast a much wider net in search of victims. Instead of having to focus on a single target or organization, now attackers can attempt to exploit hundreds, if not thousands of victims using a single program. Furthermore, social relationships and networks are increasingly mediated through the internet. Because of this, we are more able than ever before to connect with people that we have never met, and will never have to meet, in person. This creates new possibilities for online deception, where sites like Facebook and LinkedIn can serve as both information gathering tools, as well as attack vectors to contact people with a degree of anonymity. The ability to have greater anonymity on the web has also decreased the overall risk for attackers, as it is easier to evade detection and mitigate the consequences of being detected.

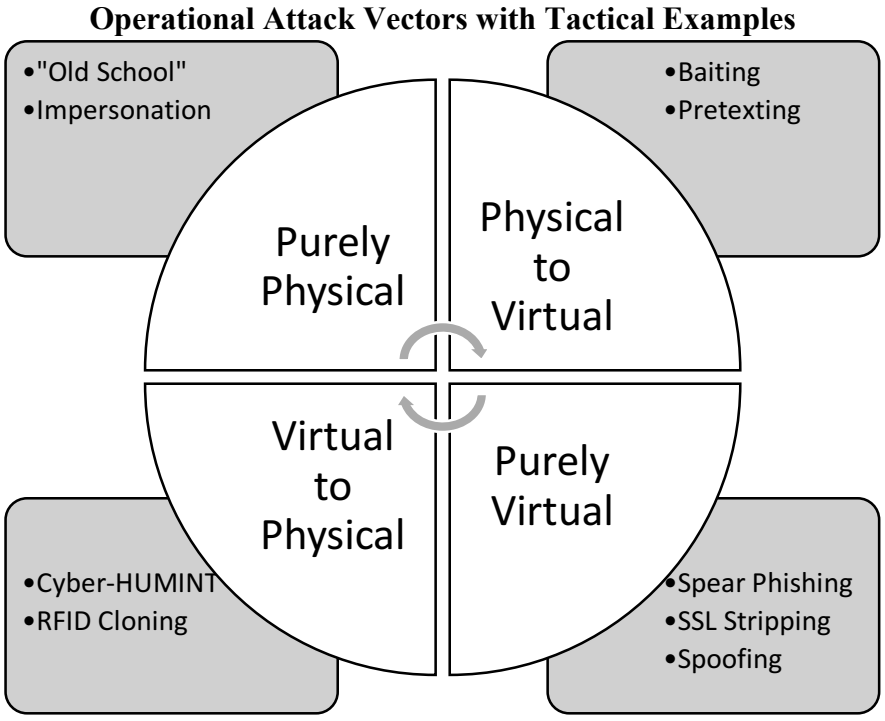
The chance of a specific threat compromising its target has also increased. The speed of information technology is to an attacker's advantage, in that mistakes made by the victims have instantaneous consequences. As a society that is largely dependent on the efficiency and speed of computers, we are more likely to make mistakes and become victims of social engineering attacks because we act more quickly than we should in many cases.[7] Especially as an individuals' familiarity with computers increases, they may become less likely to question the things they encounter on the internet, or even ignore certain security warnings, thinking that they are too smart to be duped.

The above points describe an increase in the opportunity and probability for attack, but once an attack is successful at compromising a target, the impact of that attack then must be taken into

consideration. Information technology increases the total potential consequences, or damages, from a successful attack. If an attacker gains access to a digital information system, they can much more quickly steal vast amounts of data. Getting away with this much information, while also not being caught, was much more difficult when data was stored physically in filing cabinets. Many networks have been integrated and connected for the sake of efficiency, typically meaning that those networks are not well segmented. Because of this, it is easier to get a breadth of data from many locations on the network just by penetrating one part of it.

Avenues for Attack

A social engineering attack is an attempt to gain access to an information system through a social engineering attack vector. An attack vector is an avenue through which an attack is facilitated. Social engineering attack vectors are not always purely physical or purely virtual; they often are both. The following diagram shows several attack vectors as well as tactical implementations of those vectors. It illustrates not only the complexity of vulnerabilities, but also that attack vectors can be physical, virtual, or a combination.



(The above diagram illustrates the various attack vectors that can be exploited.)

Baiting**:** A popular technique where an attacker will plant a physical media device, such as a flash drive or SD card, in the hope that a target will plug it into his or her computer in order to discover its contents. The devices are typically made to seem legitimate with labels, such as "Layoffs 2015," or even through strategic placement, such as in the parking spot of a high-ranking company official. According to a recent Department of Homeland Security study, about 90% of people tested would plug an unknown USB drive into their computer if it had an official

looking logo on it.[8] Through this, hackers can get victims to install malicious software on their computers by preying on their curiosity. Sophisticated firewalls, antivirus software, and passwords can all be bypassed by tricking the user into running the malicious software from an inconspicuous USB drive. HR managers should make sure to have policies and procedures in place to make sure that there is an efficient procedure for employees to get these found drives to IT professionals, as well as communicate to employees that this is one such way they can be active participants in the cyber defense of their firm.

Pretexting: This is the practice of pretending to be a legitimate source of help or authority, and then using this false pretext to gain helpful information such as login information or personally identifiable information. Employees should be educated on proper verification techniques to make sure that they do not inadvertently divulge useful information to an attacker that they would have originally considered routine or trivial.

Spoofing & SSL Stripping: Both of these concepts relate to an attacker redirecting traffic on a network to their malicious site, where they can steal information such as credentials. It is a form of a man-in-the-middle attack that is typically carried out on unprotected Wi-Fi networks.

Cyber-HUMINT: This is the process of gaining information on a subject by analyzing his or her digital footprint. The information collected can then be used to supplement other intelligence collection methods.

RFID Cloning: Many offices use RFID enabled cards in order to secure doorways and access to restricted areas. The data that is put on an employee's card typically contains simple information, such as name, employee ID, and organizational unit. If an attacker were able to gain this information, then he or she would be able to create a clone of the employee's legitimate card in order to gain physical access to the workplace.

Regardless of the specific vector, all of them include the interaction between the end users and the information technologies themselves. Therefore, in order to create proper defensive strategies, there must be unity between the various units within an organization that have both the *authority* and *capability* to tackle the issues. It is the direct responsibility of HR managers to put defensive mechanisms in place to help protect their organizations from social engineering attacks.

Humans as the Weakest Link

Information technology systems and networks have become ubiquitous and critical to the operation of firms in all sectors. As organizations continue to increase spending on IT, the need to secure those systems has become a great challenge. There is not only the need to protect the company's employees, intellectual property, and safe operation of corporate IT assets, but also to protect consumer data. In response to the security problem, companies have been hiring more and more developers, system administrators, and architects. They have also been dedicating more of the IT budget to hardware and software solutions to security. While these are important to shielding a network, there is very little strategic emphasis placed on the end users of the systems. In fact, by 2007 social engineering had emerged as the top method to gain information from company insiders.[9]

In many ways, humans have the greatest potential to be the weakest links in a security chain. If a vulnerability is found in software or hardware, it can be patched or redesigned. However, the

same vulnerabilities of our sociality and personalities have remained unpatched from the distant past until now. IT administrators *and* HR managers should understand the implications of this observation and endeavor to create not only protocols, but also a *joint* strategic approach to security.

The security community understands a lot about how social engineering works. Recent literature has focused heavily on generating taxonomies[9, 10] as well as case study analyses of times where organizations were penetrated by social engineering efforts.[11] Tactics and techniques of clever social engineers have been trending topics at conferences like DEF CON© and Black Hat®. However, there are few resources for how to practically apply what has been learned to real-world, complex organizations. In particular, the role that HR managers can and should play in mitigating the risk of social engineering attacks has been wrongfully neglected. HR managers must take on the role in their organizations of social engineering prevention because they are in the best strategic position to understand and influence the people of their organization.

Part II — Solutions
Managing Corporate Culture—an Example with Open Workspaces

HR managers and strategists have significant power in shaping the way a company or organization operates. For instance, they have the ability to shape organizational culture, which is critical to creating high performance work systems. To the strategic HR leader, culture is not a nebulous, uncontrollable concept, but rather a tool that when properly wielded can have tangible effects on a company's bottom line. HR managers can influence culture through several means, such as through the design of the compensation scheme, workplace policies, and even the design of the physical workspace.

Technological innovations, along with the influx of young professionals of the millennial generation, have ushered in a movement for more open workspaces. Especially characteristic in the technology sector, these open workspaces tear down the walls—literally—between coworkers. In fact, these open workspaces are big talking points for companies, both large and small, in attracting potential employees. In fact, the majority of companies listed on the Forbes list of top employers have large, open workspaces.[12]

This type of physical workspace setup has benefits of increased camaraderie and idea generation,[13] but it also presents a security challenge. Consider the following potential security issues that arise when a social engineering attack is successful in an open workspace:

- The attacker and an accomplice impersonate two construction managers by wearing hardhats, khakis, polo shirts, and having clipboards. They use this disguise to successfully convince one employee who has direct access to the workspace that they are there for a routine maintenance check. The attackers can now roam the workspace, with their camera phones, snooping out information on what kind of hardware is used, how it is configured to the network, and what written information can be of use.
- More collaboration means more sharing. In an open workspace, it would be much easier to conduct baiting attacks by planting "loose" hardware such as a labeled flash drive in the office. There are more plausible opportunities for people to plug in devices into office computers that they are not fully aware of the contents.

- A successful spear phishing attack can install malware on a computer that provides it access to built-in webcams and microphones. In an open workspace, an attacker that has a live stream view into the office would conceivably be able to gain more intelligence on the company and employees than if the space were not as open.
- The same successful phishing attack could lead the attacker to gain information about the employee such as their name, employee ID, and date of birth such that they could create a copy of the employee's RFID tag. Using the "cloned" RFID tag, they could gain access to the workspace.

These examples call into question some of the security implications that come with the open workspace trend that is supported by many HR managers today. In fact, in a 2011 study, Matthew Davis reviewed over 100 different workplace studies that found that compared with more traditional offices, employees in open workspaces experienced more uncontrolled interactions, higher levels of stress, and lower levels of concentration.[14] Stress, uncontrolled interactions, and low levels of concentration directly hurt efforts to create a more security aware culture in the workplace.

However, the trust fostered within an open workspace should be leveraged as a security asset instead of becoming a weakness. For one, coworkers could help each other identify potential security risks that arise in the workspace by communicating new threats in "real-time." Additionally, managers and coworkers can hold everyone more accountable to being security aware when they are in same physical space, and have the ability to check-in with one another (e.g. "Did you just send me an email with a link to this site?").

The implications of creating a security aware culture and putting restrictions on the open workspace are profound: depending on how it is managed, trust can become both an asset and a liability. Exploiting trust is central to social engineering, but trust is also leveraged to increase collaboration, innovation, and productivity among work teams. According to the Human Capital Institute, trust is "the willingness to put oneself at risk based on another individual's actions."[15] There seems to be a tradeoff to be made, then, between trust and security. This requires a complex solution, which requires working relationships between IT and HR, driven by HR leadership.

Proactive Incentive Management

Despite the fact that end users not only affect the security of information systems, but also in many cases are the weakest links in the security of those systems, IT managers have little control over the end users themselves. The HR managers have the most influence over workflow, workplace policies, and compensation of employees. HR managers, in coordination with input received from the IT team, should incentivize employees to maintain appropriate cyber hygiene.[16] Currently, the burden of defending networks lies squarely on the IT department. When a breach does occur, the blame is typically either attributed to a lack of good IT, or that the attacker was so sophisticated that the breach was inevitable.

Performance bonuses are common in corporations both large and small, and can be leveraged to incentivize cyber hygiene in the workplace. Regular and innocuous penetration tests could assess

the susceptibility of employees to various forms of social engineering attacks, such as spear phishing. New online tools, such as *Phish.io,*[17] can provide quick and easy mechanisms for HR managers to conduct spear phishing simulations on entire organizations. It is a free service, and can be very powerful for an HR manager to begin to develop a social engineering prevention program. According to their website, "this tool allows the user to send harmless phishing emails to your friends, family, and coworkers to test their security awareness."

The results of these tests can easily be tied to small incentive bonuses, so that employers can reward good cybersecurity behavior. More generally, HR managers should be responsible for including the results of such tests as part of their analytics. They would then be able to track both individuals' and the organization's progress over time. Cyber hygiene effectiveness should be included as critical information in HR analytics.

Researchers at the Center for Internet Security are currently exploring options for how to effectively measure cyber hygiene. Coined the Cyber Hygiene Effectiveness Score, it is a "framework, modeled after the FICO credit score" that seeks to quantify an employee's cyber hygiene.[18] It combines several factors such as education and training, past behavior, social risk, and role risk in order to come up with a quantifiable metric to help in assessing risk. Applied to an entire organization or unit, this can be an effective tool for developing and then measuring the progress of a social engineering prevention program. However, as noted by the researchers, one of the challenges facing this framework is in "adapting the CHE score across organizations and industries." This challenge is an opportunity for HR managers to lead in proactively staying abreast of the changing dynamics and threats of the workplace.

Smart use of Penetration Testing

In order to test a security program, especially one that aims to defend against social engineering attacks, there must be routine and robust testing. Security professionals and researchers alike recommend penetration testing as an effective risk mitigating measure.[19, 20] Many HR and IT managers alike are accustomed to different forms of security audits, such as with HIPPA and PCI respectively. However, there is a significant difference between security audits in the traditional sense and penetration testing. A primary difference between audit and penetration test is that in the latter, the tester assumes the tactics, techniques, and procedures of a real attacker. Unlike in an audit, where systems and processes are tested against a specific set of benchmarks and tests, a pentest aims to break into a system through whatever means, creative or not.

Because social engineering involves manipulating people, running penetration tests can be destructive to the work environment. A delicate balance must then be struck between realistic penetration tests and respect for the normal operation of the workplace. There is recent research that has developed different techniques for mitigating the harmful effects to employees during a penetration test.[21] Two of these mitigating factors include extensive record keeping and selective debriefing. Those conducting the test should maintain appropriate logs, and records should be matched to an employee's file to make sure that the employee is not negatively impacted by the tests. The research also suggests that the conductors of the penetration test should only debrief those who experienced greater than "minimal harm" during the test.

However, in the discussion of the implementation of such techniques, current literature makes no mention of directly including human resource managers in the process. HR managers specialize in dealing with all concerns related to the workplace and employee relations, and failing to recognize this expertise is not good strategy. An HR manager should be directly involved in the planning, execution, and debriefing of a social engineering penetration test, as they are most suited for navigating many difficult labor-management relationships and workplace policies.

Conclusion

At the Microsoft annual Convergence of 2015, CEO Satya Nadella spoke of the importance that technology, the internet, and interconnectedness will have on the entire economy: "Every business will become a software business, build applications, use advanced analytics and provide SaaS[22] services." Information technology will only become more integrated in all corporate divisions, and therefore it is vital that organizations leverage all of their personnel in its defense. Social engineering is a specific attack vector that preys upon people and their sociality. As it is one of the most critical security risks to companies today, HR managers must take a proactive role in preventing social engineering attacks. They have a unique perspective and specialized training in dealing with the people of their organizations, and therefore are in the best position to make meaningful change. א

Scott T. Seidenberger is an honors graduate of the ILR School at Cornell University, where he specialized in human resource studies. His research interests and professional activities center on the intersection of technology and human resource management. He has delivered a TEDx talk on the issue of cyber culture and technical talent management in the military. *He extends his thanks to Rebecca Slayton, Ph.D. who has served as an invaluable advisor and for her help in manuscript preparation.*

---

[1] Kee, J. (2008). Social engineering: Manipulating the source. GCIA Gold Certification.
[2] http://www.esecurityplanet.com/network-security/hr-a-hot-target-for-cybercriminals.html
[3] Fischetti, M. (2011). Computers versus brains. Scientific American, 12.
[4] Bless, H., Fiedler, K., & Strack, F. (2004). Social cognition: How individuals construct social reality. Psychology Press.
[5] For complete story, see Virgil's The Aeneid Book II at http://www.poetryintranslation.com/PITBR/Latin/VirgilAeneidII.htm#_Toc536009309
[6] See a *New York Herald* article from 1849 here: http://lostmuseum.cuny.edu/archive/arrest-of-the-confidence-man-newyork-herald
[7] Several companies have made business models by use of *clickbait*, which is intentionally attention-grabbing headlines and images with the intent of getting people on the internet to impulsively click on a link.
[8] See the Bloomberg Business story for a summary of the important aspects of the report: http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy
[9] Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), 183-196.
[10] Patel, R. S. (2013). Kali Linux Social Engineering. Packt Publishing Ltd.
[11] Winkler, I. S., & Dealy, B. (1995). Information Security Technology? Don't Rely on It. A Case Study in Social Engineering. In USENIX Security.
[12] http://www.forbes.com/sites/kathryndill/2014/12/10/the-best-places-to-work-in-2015/
[13] For a full report on the subject see http://m1.ethisphere.com/resources/survey-on-the-influence-of_workplace-design-and-practices-on-the-ethical-environment.pdf

[14] To see the distilled argument along with many other cited studies about the problems with open workspaces, see http://www.newyorker.com/business/currency/the-open-office-trap. The original study can be found here: http://onlinelibrary.wiley.com/doi/10.1002/9781119992592.ch6/references
[15] From *Building Trust 2013* http://interactionassociates.com/sites/default/files/research_items/Building%20Trust%202013.pdf
[16] See the INFOSEC Institute's piece on cyber hygiene for more information: http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/
[17] http://www.phish.io/ by the INFOSEC Institute.
[18] See the Center for Internet Security online at https://www.cisecurity.org/cyber-pledge/index.cfm for more information about the Cyber Hygiene campaign.
[19] Northcutt, *Penetration Testing: Assessing your Overall Security Before Attackers do*. (2005) SANS Institute.
[20] Barrett, Neil. *Penetration testing and social engineering: hacking the weakest link.* Information Security Technical Report 8, no. 4 (2003): 56-64.
[21] Dimkov, *Two methodologies for physical penetration testing using social engineering*. (2010) Distributed and Embedded Security Group.
[22] Software as a service is a software-licensing model in which use of a platform or product is licensed out to a client, with the computing accomplished in the cloud. It has become common delivery model for many business applications across industries.