COMPUTER SECURITY, FALL 2015

Why Technology Alone Cannot Fix Security

Dylan Phelan

12/15/2015

Abstract:

Defensive security is failing. In this year alone, organizations and countries across the globe have lost an estimated $400 million from comprised data records, as noted in Verizon's Data Breach Investigations Report[1]. This is despite decades of continuous research and remarkable advances in cryptographic systems, database management and incident detection. Many breaches are not due to the lack of a solution – though new exploits are constantly arising – but because not enough research is focused on helping folk implement those solutions.

For one, as long as citizens don't understand how simple breaches from protocol can jeopardize swaths of data, I claim most people will do whatever is simplest – and often that is what is least secure. Secondly, even if they do have that understanding, if people don't have an incentive to maintain any cumbersome habits, I claim most people will regress into what's comfortable. If these two things are correct – and I'll show examples of how crackers have exploited these behaviors – then it seems security research fails to address a critical issue: human behavior.

This paper's purpose is not to deemphasize the importance of security and its researchers; in fact, this paper's existence is predicated on the value we assign to corporate, societal and individual security. But any defensive security measures we construct will undoubtedly be broken or circumvented if people simply don't know how or don't care to use them. If our interest truly is to keep information secure and maintain privacy, we need to teach people how and why to maintain security.

[1] "2015 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.

Introduction:

Security research all too often focuses exclusively on the role of technology in a secure system, giving little attention to the face of the system itself: the user. Within a company, employees make their new passwords, control calendars, send sensitive emails, answer and forward calls, leave systems on and off – touching and operating every lever of the corporate machine. As long as there's a person in control of this information, it will almost inevitably leak – a truism that wards most researchers off in the best case from mitigating the issue, and in the worst case from even recognizing it.

It's precisely for this reason that social engineers rely on the human factor. Social engineering is, in short, "the art of manipulating people so they give up confidential information."[2] This information can then be used for financial gain, for competitive advantage across companies, for blackmail or for nothing but sensation of control[3]. Note that because the focus of these attacks is on the human factor they often require low technological sophistication, even in high impact cases.

Below we will address common techniques used by social engineers -- specifically phishing, dumpster diving and baiting – considering both fictional and real life break-ins. And this examination we will attempt to determine what specific behaviors or tendencies contributed to these breaches.

But before we continue, let's make one thing clear; we cannot be tasked to solve the problem of social engineering. This goal is juvenile and chasing it can lead to a false sense of security. Instead, we should endeavor to understand how social engineering happens and the human behaviors that contribute to these vulnerabilities. The most effective response to this problem is a persistent vigilance from individuals, married with corporate policy that recognizes and plans for our weaknesses. Without this, social engineering wins every time. With it, social engineering can at least be stifled.

---

[2] Criddle, Linda. "What Is Social Engineering?" *Examples and Prevention Tips*. Webroot, n.d. Web. 15 Dec. 2015.
[3] "2013 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.

To the Community:

Let's be honest: an in depth study of human behavior isn't sexy, and it sure isn't information security. It's natural that this feature of security, in the worst case gets overlooked, and in the best case is an afterthought. But it's precisely because of this that it's so easy to take advantage of. It should come to no surprise to anyone in the community that a) perfect security is a pipe dream, and b) so long as there is a human being in charge of a system, they themselves will be a point of exploitation.

But this doesn't mean we should ignore the issue. We need to investigate exactly what features of our behavior are so prone to exploitation, and how exactly to use this knowledge to better inform current and future security systems. Our inability to do that has left us in the hole we are in right now, where 29% of attacks are due to phishing schemes, dumpster diving and other social tactics[4]-- problems we have the solutions to, but solutions that just haven't stuck yet.

After major break-ins that are socially engineered we can hear the community sigh through their tweets and posts on other social media. The simplicity of the tactics makes the tragedy seem so avoidable. We ask ourselves, "Who could still fall for a phishing attack?" and "Why didn't they shred that before throwing it out?!", moving back to *real* security work – solving the niche and complex problems. But the fact that the simple problems are still around deserves more attention. After all, how much hope can we have for future research if we can't even implement the simplest of solutions in an effective way?

[4] "2013 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.

Issues:

Phishing

Carl Something sits down at his desk, returning from a late lunch, and hops back onto his desktop. One finger on the mouse and the screen comes back to life; his ears perk to the sound of a new email – looks like it's the lead engineer at his company, asking him to take a look at a new project spec. So Carl downloads the attachment, a .pdf, and within minutes a worm is crawling across not only his computer, but across all systems on the network.

This is an example of what is known as phishing; an attacker sends one or more users an email designed to fool them into revealing sensitive information in the form of direct input or in the form of access to a system[5]. Attacks can be both mass spread, usually poorly written but sent to so many people that it's worthwhile, and targeted to particular individuals. Often people who use computers have both heard of and avoided phishing attacks in their lifetime. That said, these attacks are still remarkably successful. As of Verizon's 2015 Data Breach Investigation Report (DBIR) 23% of recipients would open phishing messages, and 11% would open attachments[6].

Carl's above scenario was an example of a targeted attack. The email seemed to be from an internal official of high importance, jargon was used within the email that seemed like something the lead engineer would say. These details take much longer to craft than those used in mass-spread attacks, which are often scraped together quickly, laden with typos and logical errors, but which only rely on a fraction of a fraction of the recipients opening.

But hypotheticals, while useful, aren't necessary to demonstrate the impact of these attacks. In 2011, RSA SecurID had a major breach that led to upwards of $66 million dollars in losses.[7] This is a company that literally builds security products for a living – token generators that are used in two factor authentication systems[8] – and their internal teams fell for a phishing scheme, ultimately giving crackers remote access to their servers and everything on them.

---

[5] Rouse, Margaret. "What Is Phishing?" *TechTarget*. N.p., n.d. Web. 15 Dec. 2015.
[6] "2015 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.
[7] Schwartz, Mathew J. "RSA SecurID Breach Cost $66 Million." *Dark Reading*. N.p., 28 July 2011. Web. 15 Dec. 2015.
[8] "About RSA SecurID." *RSA SecurID*. N.p., n.d. Web. 15 Dec. 2015.

But why do these attacks succeed so often, even among security professionals? There are a plethora of human tendencies that can be exploited in phishing attacks, but among the most common are ignorance, curiosity and laziness. It's our curiosity that leads us to open emails from foreign senders in the case of mass spread attacks, and to open suspicious emails from familiar faces in the case of targeted attacks. Ignorance of how much damage Excel spreadsheets and .pdf files can do to our computers in the way of malware makes people careless about clicking on links and opening attachments. And general laziness leaves most of us unwilling and unprepared to be suspicious of the emails we have to sift through on a daily basis.

Dumpster Diving

Phishing isn't the only social tactic that is influenced by these behaviors. Dumpster diving is another social engineering stunt that contributes to major theft every year; a 2015 report by BakerHostetler reported that almost one in every five breaches involved some sort of paper records[9]. One of the easiest ways for external agents to gain access to these records – and legally if done right[10] – is through dumpster diving.

As the name suggests, dumpster diving generally involves sifting through trash to find some bit of useful information. This technique can be valuable directly, revealing things like credit card and routing numbers, or indirectly, unearthing information that can serve as a tool in other social engineering attacks. Either way, the upshot is that improper disposal of company property can have devastating consequences.

Though it's not headline breaking, one security researcher Steve Hunt wanted to see how much information he could uncover in a few minutes of diving. Investigating the trash bins of a bank revealed checks, SSN's, credit card numbers, signatures, addresses, bank numbers, employee ID numbers, business identification numbers and entire laptops full of undeleted,

[9] McLellan, Melinda L. "2015 BakerHostetler Incident Response Report Shows One in Five Breaches Involved Paper Records." *Data Privacy Monitor*. N.p., 01 June 2015. Web. 15 Dec. 2015.
[10] Legal limits of dumpster diving are still a point of contention, but for more information on that see the following. http://freegan.info/what-is-a-freegan/freegan-practices/urban-foraging/diving-and-the-law/

unencrypted information on individuals and the businesses they worked for.[11] All of this in one dumpster, for one bank, on only one day.

Like the previous example, laziness and ignorance factor in largely here. Shredding documents is a time consuming process, especially for banks where almost all their information is confidential and needs to be destroyed. While it might seem that this urgency would encourage sensitivity, it's easy to imagine how such sensitivity fades over time. The first time you forget to shred paperwork you worry profusely, and typically receive no backlash unless there's a system of checks and balances. The second time, you're nervous still, but aren't surprised when there's no consequence. What was a single incident can quickly become a habit if there's no negative feedback for breaking protocol; and in such a scenario, negative feedback can come too late.

As for ignorance, many people don't know how to dispose of digital information or how it gets handled. The relative novelty of technology often means we have terrible intuitions as to how it works. Deleting files doesn't actually delete the files, a broken monitor or a virus-laden computer doesn't mean that the hard drive is destroyed, and a variety of reasons that might motivate us to dispose of a computer don't require us to wipe the computer's memory beforehand. Our inability to recognize the immediate or indirect value of this information can lead to oversight on the user end and, ultimately, an easy exploit for the social engineer.

Baiting

There's one more attack we'll consider: baiting. This is somewhat similar to the phishing attack mentioned above, but leverages curiosity more than laziness. In 2006 Steve Stasiukonis, a security consultant and founder of Secure Network Technologies Inc., was hired by a credit union to assess the company's security policies and employee diligence. As part of the process, security auditors infected 20 flash drives with Trojans – a virus that disguises itself to seem harmless – scattered the sticks about the company premises, and waited. The viruses were programmed to send logins, passwords and machine information back to the team upon opening

[11] Goodchild, Joan. "A Real Dumpster Dive: Bank Tosses Personal Data, Checks, Laptops." *CSO Online*. N.p., 2009. Web. 15 Dec. 2015.

a file that seemed innocuous. By the end of the day, 75% of the drives were found, and 100% of those drives had their viruses opened.[12]

Baiting is exactly what it sounds like. Attackers bait their victims into downloading or activating malware by enticing them with something intriguing. It doesn't necessarily have to be tangible like the example above; malicious, downloadable files on peer-to-peer sharing websites are another classic example of baiting. But either way, baiting pries on our tendency to be overly curious, a general ignorance of how malicious software can be and a laziness that can leave us vulnerable even if we know the possible consequences.

The employees at this credit union had no business opening those flash drives. There wasn't any obvious sign that the drives belonged to the company or that they were safe to use. In fact, the lack of any signs at all was exactly made them so appealing. If there's no indicator of what it contains, the sky's the limit: credit card numbers, incriminating photos, passwords, business documents… and, of course, malware.

That's where the ignorance and laziness fit in. As was the case with email attachments, I maintain most people don't fully understand the possible consequences of plugging in a USB drive. If people knew that excel spreadsheets could give someone access to their passwords and usernames, they might be more diligent with when opening them. Then again, for those of us that do know this, many cannot be bothered to investigate the contents of the file with care – not when curiosity is calling. The process of being secure can be time consuming, and if we're in a rush or on a deadline we might sacrifice best practices for time efficiency.

[12] Stasiukonis, Steve. "Social Engineering, the USB Way." *Dark Reading*. N.p., 7 June 2006. Web. 15 Dec. 2015.

Action Items:

Of course, the behaviors I've described above are, right now, nothing more than conjecture. Understanding why these and similar attacks happen is key to preventing them in the future, but we need an experimentally oriented approach to determine how accurate these conjectures are. Once we have a solid and well supported idea of what human behaviors are easy to exploit, we can work on these two prevention strategies.

The first is a better general education. Though computers keep our financial, healthcare, transportation and legislative systems running 24/7, many of the people who operate within these spheres have never taken so much as an introductory computer science course. If people had a better idea of how malicious attachments can be, how worms can spread from one computer over a whole network, how common it is for crackers to connect to computers remotely, and how easy it can be to break simple passwords, we might be inclined to be more diligent in our privacy practices. In the long term, this can happen by introducing core computer science concepts into public school curricula; but in the short term, offices and employers can introduce security seminars to give their employees insight into how people often get exploited in their line of work.

Secondly, we can build more robust policy within corporate and legal arenas. If we can construct a system that isn't so prone to neglect and laziness, one that provides incentives to fight that laziness and that launches internal audits, companies will have a better concept of how often these break-ins occur and under what conditions they happen. Are phishing scams more successful around deadlines? Are new employees more likely to mishandle sensitive trash, or do the veterans members lead to more dumpster diving incidents? Once that understanding is developed, policy can be set up to account for those. If dumpster diving is an issue, remove trash bins and put shredders at people's desks. If phishing is a problem, launch an internal audit and offer free lunch to people who don't fall for them. These are just a few ideas that can try to incentivize proper security practices and make improper practices impossible by virtue of corporate structure.

Moving Forward:

Future research in the security community should not only take into account how to solve a problem, but also how to spread this solution among the public. Once accessibility becomes a concern in the mind of the researcher, the efficacy and the diffusion of their work will be closer to reaching its true potential. Similarly, we users who turn this research into a reality need to be aware of our shortcomings.

The desire to be curious, the tendency to be lazy, a lack of computer science education: these are only a few things that might leave you and me vulnerable to social engineering. And the first step in overcoming these faults is being aware of them. But these behaviors I've cited are hunches at best. Only by consulting with other disciplines, those who focus in human behavior, can we determine exactly what features of the human condition are contributing to these exploits. And once we've done this research with the aid of the Psychology and other communities, we can develop an understanding of what practices and policies can mitigate these behaviors in the long term.

References:

1. "2015 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*, N.p., n.d. Web. 15 Dec. 2015.
2. Criddle, Linda. "What Is Social Engineering?" *Examples and Prevention Tips*. Webroot, n.d. Web. 15 Dec. 2015.
3. "2013 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.
4. "2013 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. N.p., n.d. Web. 15 Dec. 2015.
5. Rouse, Margaret. "What Is Phishing?" *TechTarget*. N.p., n.d. Web. 15 Dec. 2015.
6. "2015 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions,* N.p., n.d. Web. 15 Dec. 2015.
7. Schwartz, Mathew J. "RSA SecurID Breach Cost $66 Million." *Dark Reading*. N.p., 28 July 2011. Web. 15 Dec. 2015.
8. "About RSA SecurID." *RSA SecurID*. N.p., n.d. Web. 15 Dec. 2015.
9. McLellan, Melinda L. "2015 BakerHostetler Incident Response Report Shows One in Five Breaches Involved Paper Records." *Data Privacy Monitor*. N.p., 01 June 2015. Web. 15 Dec. 2015.
10. "Dumpster Diving and the Law." *Freeganinfo*. N.p., n.d. Web. 15 Dec. 2015.
11. Goodchild, Joan. "A Real Dumpster Dive: Bank Tosses Personal Data, Checks, Laptops." *CSO Online*. N.p., 2009. Web. 15 Dec. 2015.
12. Stasiukonis, Steve. "Social Engineering, the USB Way." *Dark Reading*. N.p., 7 June 2006. Web. 15 Dec. 2015.