

THE COST OF CARELESSNESS

Security Malpractice, and How to Prevent It

Josh White

*COMP-116: Introduction to Computer Security | Tufts University
Mentor: Ming Chow*

Abstract:

It seems that, every few weeks, there are reports of high-profile security breaches from major organizations, accompanied with reassurance from those involved that they will attempt to beef up security against possible attacks in the future. The reason behind many of these attacks is often not a lack of security technology available, but a lack of will or effort in implementing it. The 2016 Democratic National Convention hack, for example, most likely started with a targeted email phishing scheme (3), and as many as 91% of security breaches begin similarly (7). In 2011, the primary damage of the Sony PlayStation Network hack came from storing customer information in unencrypted data – a basic security flaw (2). More recently, Yahoo had been reported to be engaging in poor security practices – removing funding from security teams and focusing instead on consumer-facing software and rebranding. The cost? Around 500 million accounts, and substantial losses from brand damage and lawsuits (8). The question then, is rarely “How could this have possibly been prevented?”, but instead “How could so many major organizations be so careless?”

This paper seeks to answer that question: to show the reasons behind security malpractice, and to recommend steps to prevent it. Additionally, this paper will show some of the concrete costs resulting from malpractice. Sophisticated security technology exists, but none of it matters until individuals, governments, and corporations start taking the issue seriously.

Vocabulary:

A few terms used throughout this paper need defining and explanation:

Social Engineering:

“The use of human error or weakness to gain entry to a system, despite any security technology being used.” (4)

Phishing/Spear phishing:

Phishing involves malicious email sent to random accounts, which attempt to trick the reader into clicking on a link, disclosing sensitive information, and/or downloading malware. Spear phishing is a specialized form of phishing, targeted at a particular person, and tailored to look legitimate. Often, attackers may research public information on their targets (in social media or public directories). Both methods have an alarming success rate, and government organizations are often popular targets, as much employee information is public record. (11)

Breach: Any event in which an individual’s name and information is exposed and put at risk, in either digital or physical form. (9)

Introduction:

It's well known that a significant amount of information is retrievable online. Mail, financial information, medical records, and corporate secrets are all stored digitally. When doing business with a company engaged in the information sector, a customer should have a reasonable expectation that their private information will stay private. Certainly, there is the possibility of a sophisticated attack from a state-sponsored hacker or crime syndicate, but, one expects that their information is encrypted, hard to retrieve, and largely secure.

Unfortunately, this just isn't the case. There have been over 200 major (involving 30,000 or more records) breaches since 2004 (6), which averages out to roughly 17 per year, or at least one event every month. Attacks have been increasing in the past few years, both in frequency and severity, possibly due to an increased number of people and organizations storing sensitive information online, and more web-enabled services in general. Of these attacks, nearly 91% begin with a spear phishing attack or similarly low tech method, often involving a situation as simple as a disgruntled employee.

So, what's going on here? Why are companies not taking the necessary steps to protect their customers, and what can be done about it?

To the community:

This topic was chosen because of the importance of social engineering and security malpractice. Security researchers can create highly sophisticated defenses and practices, but, ultimately, the security of a product or organization rests with the people behind it. Without an awareness of security best practices and meaningful policy changes, no security suite offers meaningful protection.

Reasons Behind Security Malpractice:

Shipping a secure product seems like it should be almost self-explanatory. Why then are major companies often caught completely disregarding even the most basic security practices? Usually, the reason is simply money. A company will try to ship a product before it's ready, as the financial and time costs for adding security features can seem too high (see Yahoo, 2016).

Organizations can, of course be the target of malicious behavior from internal sources, such as an employee attempting to “get back” at the company for a perceived slight, or an employee selling sensitive information for personal profit. In fact, 89% of attacks have a financial or espionage motive (10), and it can be difficult to predict an attack from within.

Still, this doesn’t absolve victims of sheer carelessness and, sometimes, plain incompetence that go behind a massive amount of security breaches. Basic phishing attempts are remarkably successful. In a sample of dozens of organizations in 2016, Verizon researchers found nearly 30% of phishing messages were opened by their target across all campaigns, and nearly 12% clicked on the attachment or link in the message, leading to a successful attack within a matter of minutes. Poor credentials were another too-common weakness: 63% of breaches involved a weak, stolen, or even default password. There’s also simply a lack of knowledge about security issues, as new vulnerabilities come out every day, and often, companies will continue using legacy software that they can neither patch nor understand (10).

Although the vast majority of attacks come from organized crime groups or state-affiliated hackers (10), many of the methods are basic in nature, and are effective because companies don’t take the time to create secure products, and don’t educate their employees on good security habits.

Costs

Generally, security is often a question of money. The cost of a data breach, however is approximately \$4 million, or about \$158 per record. These numbers of course fluctuate depending on the industry of the victim. Healthcare, for example, has a cost of about \$400 per record. Additionally, the cost per record is difficult to calculate for extremely large events (over 100,000 records), and there is not a strict linear relationship between records lost and cost. (1) Major breaches can involve millions, or even hundreds of millions of records. (6)

In addition to the cost of repairing damage through lawsuits, hiring expensive forensics experts, and patching what have now become major security holes, these figures account for other hidden costs. Any affected services will experience downtime while fixes are being made. This means that there could be weeks without any revenue: something that could possibly spell

the end for a small company. Companies will also have to deal with a massive PR hit, which is difficult to fully quantify for a massive security fiasco. Who wants to use an email service which just leaked millions of passwords, when switching to another is both easy and free?

It seems, then, that ignoring security cannot be worth it. So, after decades of these problems lingering, what is there that can be realistically done?

Action items

The most obvious, and perhaps, most important action which should be taken is educating people on security risks. Most of the mentioned attacks in this paper can be recognized and prevented easily enough easily enough. Employees should be trained to identify various social engineering attacks, such as phishing and be instructed on basic precautions to be taken. For example, a company could introduce a policy of a secondary confirmation for transferring sensitive data besides email, such as a phone call, in-person meeting, or verifying with a manager. This training should be mandatory for new employees, with annual sessions for all employees. Security information should be distributed regularly. For example, stories on security slip-ups and commendations could be distributed through company newsletters.

Security policy must be both meaningful and easy to understand for both technical and non-technical employees. Although employees writing code should understand best practices, everyone with proper clearance has the potential of accessing sensitive data, and should be able to easily understand how computers should be used, and how to handle and dispose of information as necessary. Employees should be screened when they are working with sensitive sections of a product, and since not everyone can be truly vetted in a company of significant size, data should be compartmentalized as necessary: not everyone needs access to the customer credential database.

Security features should be implemented into a product, as they are not expensive compared to a data breach. The cost of fully encrypting a disc is about \$200 dollars, most of which is due to productivity lost from the increased boot time of a system (7). Doing this drops the cost of breached data by about \$16 per record (1), not to mention mitigating a loss of customers or legal and forensics fees from a breach. Any organization with data of any volume

should practice encryption. Obviously, basic precautions such as virus protection and password policies shouldn't be overlooked. Better email filters, for example can prevent phishing attacks before they even happen.

Conclusion:

Most security breaches are preventable, but no amount of money or time spent in developing better defense technology will matter until people and organizations exercise good security policies. The cost of a data breach can be high, and for some organizations, even crippling, which is not to mention the responsibility of a company to protect any sensitive information they're trusted to handle by their customers. It is neither feasible nor possible that every employee in every segment of a company can be a security expert, but everyone should know how recognize email scams and social engineering schemes, and all developers should be able to write secure code free of basic security vulnerabilities like hard-coded passwords and plaintext data. As more data becomes digital, people place more trust in companies safeguarding their records. For the information economy to succeed, it is imperative that companies end security malpractice.

References:

1. "2016 Ponemon Cost of Data Breach Study." *Ibm.com*. IBM, June 2016. Web. 14 Dec. 2016. <<http://www-03.ibm.com/security/data-breach/>>.
2. Anthony, Sebastian. "How the PlayStation Network Was Hacked." *Extremetech.com*. Ziff Davis, LLC., 27 Apr. 2011. Web. 11 Dec. 2016. <<https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked>>.
3. Gallagher, Sean. "Russia-linked Phishing Campaign behind the DNC Breach Also Hit Podesta, Powell." *Ars Technica*. Conde Nast, 20 Oct. 2016. Web. 14 Dec. 2016. <<http://arstechnica.com/security/2016/10/russia-linked-phishing-campaign-behind-the-dnc-breach-also-hit-podesta-powell/>>.

4. Gulati, Radha. "The Threat of Social Engineering and Your Defense Against It." *SANS*. Sans Institute, 2003. Web. 26 Oct. 2016. <<https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232>>.
5. Kingsley-Hughes, Adrian. "The Price of Full Disk Encryption: \$232 per User, per Year." *ZDNet*. CBS Interactive, 3 Sept. 2012. Web. 27 Oct. 2016. <<http://www.zdnet.com/article/the-price-of-full-disk-encryption-232-per-user-per-year/>>.
6. McCandless, David, Tom Evans, Miriam Quick, Ella Hollowood, Christian Miles, and Dan Hampson. "World's Biggest Data Breaches & Hacks — Information Is Beautiful." *Information Is Beautiful*. N.p., 15 Nov. 2016. Web. 11 Dec. 2016. <<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>>.
7. "Over 90 Percent of Targeted Attacks Derived from Spear Phishing Emails, According to Trend Micro." *Trendmicro.com*. Trend Micro Incorporated, 28 Nov. 2012. Web. 11 Dec. 2016. <<http://newsroom.trendmicro.com/press-release/cyberthreat/over-90-percent-targeted-attacks-derived-spear-phishing-emails-according-t>>.
8. Perlroth, Nicole, and Vindu Goel. "Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say." *Nytimes.com*. The New York Times, 29 Sept. 2016. Web. 11 Dec. 2016. <http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html?_r=1>.
9. "Security Breach." *Techopedia.com*. Techopedia Inc., n.d. Web. 11 Dec. 2016. <<https://www.techopedia.com/definition/29060/security-breach>>.
10. "Verizon's 2016 Data Breach Investigations Report." *Verizon Enterprise Solutions - 2016 Data Breach Investigations Report*. Verizon, 27 Apr. 2016. Web. 25 Oct. 2016. <<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>>.
11. Zetter, Kim. "Hacker Lexicon: What Are Phishing and Spear Phishing?" *Wired*. Conde Nast, 7 Apr. 2015. Web. 25 Oct. 2016. <<https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/>>