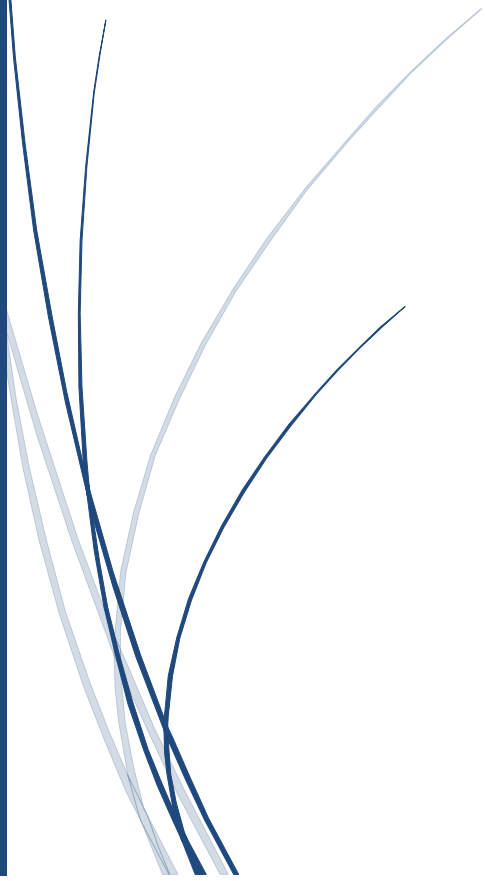
3/1/2015

# Information Security

## Fighting Fire with Fire



Taylor Jolin – Technology Solutions Consultant
JOLIN CONSULTING LLC.
300 LENORA STREET #624, SEATTLE WA, 98121

# Information Security: Fighting Fire with Fire

Taylor Jolin

Technology Solutions Consultant

taylor@jolin-consulting.com

Jolin Consulting LLC.

300 Lenora Street #624

Seattle, WA. 98121

**Information Security: Fighting Fire with Fire**

Computer hackers bring down Sony, Anonymous defaces business websites, hackers steal millions of dollars from banking systems; these are not just over dramatized headlines to facilitate the revocation of net neutrality, these are real issues that businesses face on a day to day basis. Unfortunately, as you read this, your valuable information is freely available on the internet for anyone with ill intentions to utilize at their discretion. Making this is a terrifying sentiment for much of the users in today's technology driven society. Aside from businesses, private users live in fear of having their credit ruined, personal emails stolen, or even worse, their identities stolen. Credit card numbers, social security numbers, private addresses, corporate information, and classified military documents are just a few of the numerous examples of what is freely available on the World Wide Web, making information security a crucial factor of a business's function. Securing data is an increasingly significant component of any business, resulting in curbing the ignorance of end-users, preventing the theft of crucial resources, reducing the chances of vulnerabilities being exploited, and ultimately allowing for a business to thrive while minimizing the worry of potential threats to daily operations. Sadly, the fact that much of our lives are open for the entire worlds viewing pleasure is commonplace in our culture today. Nevertheless, the advent of Facebook, Twitter, online banking, e-commerce, and mobile applications, have made the process of managing an entire catalog of private integral information nearly impossible. Additionally, in regards to managing our online lives, a few questions need be asked; how would you protect yourself? How would a business protect itself? How would a parent protect their children on the web? The answers to these questions are not as simple to understand as one would assume. Thankfully, there is a proposed solution to ease our troubled minds and allow us all to sleep better at night. Instead of demonizing hackers for the reputation

they have earned through their various exploits we should be rewarding the knowledge in which they have obtained and allow them to utilize it for the betterment of personal, business, and national security. Kevin Mitnick is undoubtedly the world's most notorious computer hacker. In the 1980's and 1990's, Mitnick masterminded a digital crime spree and eluded capture by the FBI for several years. Mitnick was charged for several offenses ranging from unauthorized access to network devices, breaking into computer systems, theft of software, and evading arrest (Penenberg, 1999). Due to Mitnick's spree of exploitation many of the country's leading technology business's had to re-engineer security practices, paving the way for a new era of information security. These larger companies had then set the standards for information system infrastructure and security practices. In hindsight, Mitnick is now employed by the same companies in which he targeted as their security consultant, ensuring they are ahead of any current trends in exploitation.

Since hackers are the primary target for most company's data protection plans, focus is rarely shifted onto the outer components of information security. Aside from hackers, companies have several other factors to ensure they are delivering unaltered products and services on time. Factors such as supply and demand, customer support, financial management, and client relations all weigh heavily on a company's ability to perform satisfactorily. However, a common misconception remains; information security is a single problem that is easily addressed when we apply virus scanning and software firewalls. Unfortunately, the reality is that there are several elements in the continually evolving wheel of information security; however, there are five integral pieces that rarely differ; physical security, data integrity, environmental conditions, vulnerability correction, and end-user awareness. Of the five pieces of information security, physical security is consistently overlooked, closely followed by the environmental conditions in

which a business or consumer stores their data. Data integrity is also a large piece of this puzzle, ensuring that data is always accurate and available. Similarly, vulnerability correction is paramount in the targeting of exploitation tactics commonly used to penetrate public or private systems in order to access secured or even unsecured data (Goldstein, 2008). Lastly, the knowledge of the policing agencies and end-users are the final key to ensuring a solid foundation for all business or private users. Consequentially, these are not easy demands to meet and to expect any business to realize these components is unrealistic and unfair. Businesses in today's digital age should never hire off-the-street self-proclaimed information technology specialists and expect to maintain a level of information security that could compete with even the least secure systems on the net. In retrospect, in order to protect a network from hackers, a business must either think like a hacker, or hire a hacker. Although hackers have a bad reputation, the common goal of all hackers is to access information for the purpose of being able to do so. Not all hackers are malicious and not all hackers are trying to steal your valuable recipes you saved in your email. Utilizing hackers could not only inform people on ways to protect themselves, but to battle-harden those curious and ready to stand their ground in their own digital fight.

As stated above, it is very dangerous to think of information security as a single tiered system that any I.T. professional can handle. Information security has several components that are crucial to securing even the least significant piece of data. Unfortunately, physically securing networking assets is commonly overlooked as a valid concern for most businesses. Several small companies are breaking ground into the fast-paced world of e-commerce and software as a service, or SAAS, without prior knowledge of networking needs or the security protocols vital to sensitive data protection (Beaver, 2012). Many start-up companies are utilizing cloud based services and running their businesses on hardware components purchased out of sync with other

needed networking and security equipment. This is a common trend in small businesses due to the lack of higher corporate financial support that would allow them to purchase and utilize the best quality hardware and software resources. Aside from the purchase of software and hardware resources, the need for co-located managed facilities to house such equipment is usually pushed to the side for other business needs. This trend could not be any more damaging by reason of misunderstanding what physical security in a networking environment really is. When we stop to analyze our own interpretations of physical security, the usual points come to mind; door locks, window locks, equipment locks, and access control (Beaver, 2012). However, most organizations put little to no thought into the location of their network resources. Unfortunately there are numerous possible vulnerabilities for all companies that are not easily thought of and corrected at first and thanks to all of our ignorance; hackers are constantly looking for them. Luckily, almost all of these vulnerabilities can be prevented or averted without breaking the bank. Unwittingly, a common point of failure for smaller businesses is the entrance, which is paramount in delivering the first impression a customer would receive; however, it is also the first impression a potential hacker will receive. Aside from showcasing a professional atmosphere, a receptionist plays a vital role in the security of a company's assets by monitoring foot traffic in and out, making sure visitors sign in or are escorted to their destination, and ensuring that vendors or delivery persons are really who they say they are. Unfortunately, the role of physical security does not end at the entrance to the company's headquarters. In the case that a hacker were to slip passed reception by either waiting for a moment of inattentiveness or impersonating a trusted vendor or employee, they would have access to a world of information laying around everywhere within arm's reach inside the company walls (Goldstein, 2008). Information posted on company bulletin boards can be a huge gain for anyone looking at creating a timeline or pattern for employees or operations at

a company. Aside from casual snooping, if the hacker has taken the risk of getting past reception, it is almost certain that they will push the envelope and attempt to steal any unsecured documents or software lying around (Beaver, 2012). Furthermore, if there are unsecured rooms, you can be almost certain that a hacker will try to see what's behind them if given the chance. This begs the question, how much security is too much? Luckily, there are numerous agencies trying to provide cost effective total security for businesses of all sizes. One of the technologies aimed at combating intrusion is biometrics, which is steadily growing more popular as time passes. Biometrics, essentially, are physiological "keys" used for access. Technologies that are readily available today are retinal scanners, fingerprint scanners, voice recognition, and in some more extreme cases; a combination of multiple physiological components (Goldstein, 2008).

Although physical security is an increasingly difficult aspect of information security to gain control of, the environmental components are usually what set a business up for failure. Both physical and logical components of a business environment are integral to the overall success of that business (Brito & Watkins, 2011). In reference to logical environmental concerns, companies have been trying to correct morale and esteem issues within a work environment for years with a great deal of success is most cases. However, there are several cases in which an employee was discharged unwillingly due to misconduct or negligence and in retaliation the former employee sabotages the company in some way. The majority of the time, the former employee will deface or vandalize company network assets due to the fact that it is virtually impossible to catch a suspected vandal in the act. It takes hours, and in some extreme cases years, to track down a hacker or digital vandal, and by the time a security analyst can pinpoint who or where they were at the time of the crime, they are long gone. On the bright side, there are numerous groups putting an enormous effort into policing the internet as well as business

intranets. Luckily, in recent development, software development companies have now discovered ways to insert code in proprietary software or company data that forces either to self-destruct once they pass a point of demarcation (Harrington, 2014). This would allow for stolen software to be destroyed in the case that an aggravated employee was trying to retaliate for an action they perceive to be unjust. Other software companies have been implementing software that would purge a former employee from all network and system databases, immediately following discharge, restricting all of their access to any company assets. Software such as the previously described, aide in the protection against the future defacement of company assets by cutting off all issued rights to company networked assets. Aside from the fear of logical environmental threats, another more common threat exists; the threat of physical environmental catastrophe. Environmental physical concerns fall into two categories; the physical conditions in which the network or system is housed and maintained, and the physical conditions in which the network must operate in. The latter of those two can be emphasized even further, for example, going as far as planning for natural environmental catastrophes such as tornadoes, earth quakes, and floods. In most cases, the focus is on the physical location of network assets due to those conditions being controllable whereas outer conditions like floods cannot be controlled. Though in retrospect, throughout my 10 years of military service as a network security analyst, a common hazard that I have corrected on several occasions was the actual location of networking equipment in open areas that allowed for virtually anyone to have unlimited and un-monitored access to valuable military data with no effort while also planning for the risk of being destroyed by natural or freak occurrences. In smaller businesses most networking equipment is housed in one central location; which is not necessarily bad, however, the choice of these locations is questionable. Due to the layout of most commercial spaces utilized by small businesses,

networking closets or server rooms are usually located in ideologically inadequate rooms that pose a physical hazard to the integrity of data. Other issues such as improper wiring of networking assets, networking hardware located too close to plumbing, improper air conditioning resulting in equipment overheating, and the overall cleanliness of data facilities all contribute to the degradation of data facilities and networking equipment. Furthermore, the majority of company employees have not been properly trained in information security tactics and almost always, are the cause for some sort of vulnerability by way of ignorance or pure laziness (Luther & Amy, 2015). Sadly, aside from the employee's lack of formal education in the matters of information security, there are still numerous outside physical risks a company can face. However, when approached with viable solutions to solving these issues, the majority of business owners still choose to finance temporary solutions rather than allowing for permanent fixes to exponentially dangerous problems. This is not due to the frugality of business owners, but a lack of awareness.

Despite the reality that the physical components of security should be the primary point of focus for businesses, an often unforeseen danger that companies face on a daily basis is data inaccuracies. Data integrity is almost always the first sign that a business has poor standards of internal security. If a business cannot maintain consistent data management practices to ensure that data is accurate, available, and authentic, then that business's days are numbered. Nowhere is data integrity as vital as it is in our nation's security. The United States, along with the rest of the world, utilizes data collected every day to ensure the security and safety of its citizens on a daily basis. By now, it is well known that our personal data such as; phone calls, texts, emails, and social media is being mined for potential threats to national security. Without the need for data integrity, agencies that maintain this sort of data in massive amounts could be contaminating

data between two different sources (Pentland, 2014). The easiest way to exemplify something like this and its after effect is to refer to two varying types of data. In the first example we have collected data on an average American, who is a business owner and who contributes to several charitable organizations. However, this average American business owner publicly posts racist or anti-democratic remarks on social media aimed at propagating hatred towards our current political situation. The gentleman in this example does not have any violent intent; he is just candid in expressing his political views. In the second example, we have collected data on an Islamic refugee, who is residing within the United States and has close ties to family in the middle-east. He sends money on a regular basis through secured means to his family and he is active in the Islamic culture within his community. Unfortunately, when data integrity is not ensured and data and document management is not taken into consideration, we receive misinformation by mixing the vastly different and numerous triggers within that data (Ramamoorti & Nayar, 2013). Due to this misinformation we now see an Islamic refugee, who publicly expresses his dislike for the United States political system. We also see that he sends money securely to organizations in the middle-east, and he is very active in local Islamic culture. With this kind of a mix-up of data we now have created a profile on someone that would potentially be a threat to our nation's security, if the data we collected was accurate and handled correctly. The mending of these two examples is an extreme case of what could happen with a lack of measures to ensure data integrity. Unfortunately, the truth is that this happens almost too often in the business world, causing business's to lose clients, lose income, and even go bankrupt.

Even though data integrity is at the core for ensuring availability, authenticity, and accessibility of data, there is a down side, the existence of data packrats. Companies and

individuals alike, all fall into the trap of being data packrats. In the techno-age we currently live, we are almost always required to house data in some way. In academics, we are always required to supplement our renditions with facts or reference. Everyday human interactions such as purchasing alcohol require authentication and verification. It would be ridiculous for every student who has written an essay or research paper to keep copies of everything they used to aid them in writing such documents. An even more ridiculous notion is to assume that every convenience store keeps a copy of an I.D. card used for the purchase of alcohol. Both of these scenarios boast unrealistic needs for keeping some sort of data. The same standard applies to business data. In most cases business data can be sorted into relevant, irrelevant, and target data; however both relevant and irrelevant data pose a threat to the security and integrity of target data (Bryner, 2014). Data such as payments received and payments sent out could be saved on encrypted sources to maintain a record of transactions, which could be beneficial for a company's tax records or financial accountability. Not only does this assist the business in maintaining accurate records of transactions, it allows them to maintain accountability of the payments a customer would make for services rendered; all of which are examples of relevant information. Information such as credit card numbers, bank account and routing numbers, or even social security numbers instantly become target data if stored in a company's personal information systems, which in reality is commonplace for the majority of businesses that host online services.

Since exploitable demographic and financial information; i.e. credit card numbers, social security numbers, or bank account numbers, are the primary target for the majority of malicious hackers, companies must be aware that there are several ways for a hacker to obtain access to this type of data. The easiest way, however, is by utilizing irrelevant data to access relevant data

which ultimately leads to target data. Irrelevant data is the data that a company would store that does not pertain to company or client interests such as; employee username and passwords for information systems, internal company emails, and company phone calls (Pentland, 2014). In most cases company employees are required to remember several passwords to a combination of in-house and cloud based information systems which can be a daunting task. To alleviate some of the stresses of the everyday workload, employees will frequently create password lists and save them to their assigned company work station. To make matters worse, some companies allow employees to work remotely through company owned virtual private networks or company provided laptops, both with scaled back security protocols in order to allow that employee to be productive while away from the traditional office.

Aside from the fact that employees are allowed to download and manipulate data freely from unsecured home networks when using company provided virtual private networks, the storage of irrelevant data is still just as dangerous. In regards to company owned networks, if a hacker gains network access and can gain access to any documents that may store passwords to access secured sources or notes to significant data stores then that hacker now has an advantage on that company. That hacker now also potentially has access to protected customer information, or target data. In the case of Sony executive Amy Pascal, hackers were able to gain access to her company emails and utilize them to sabotage her career, ultimately resulting in her stepping down as the Chairperson of Sony Pictures Entertainment Motion Pictures Group (Pascal, 2015). And in more recent news, hackers were able to endanger and potentially exploit millions of credit card numbers and other sensitive customer data from the medical insurance company Premera Blue Cross by using a combination of social engineering tactics and irrelevant information which was discovered by the hackers during reconnaissance (Shahani, 2015).

Although several of the different ways a hacker can gain access to a system have been described above, none of them are nearly as effective as common social psychological techniques. These techniques are referred to as "social engineering" and are the first layer of reconnaissance a hacker may conduct. In most scenarios, a hacker would call a company and pose as a member of the Information Technology department. In the setup of their attack they would either explain that they are attempting to install updates to that users work station and are unable to access it without that user's username and password (Garvey, 2005). In most cases the user unknowingly would give their private information to an impostor whose only goal is to gain unauthorized access to that system because they are not aware of their company's security plan or of any policies regarding password protection (El Emary, Shalhoub, Arif, Alsereihy, Shalhoub, & Al-Sahhaf, 2013). Aside from the psychological attacks that a hacker can leverage on a target, social engineering is primarily used to gain initial access to a system or network. Once an attacker gains access to a network they have a wealth of tools in which they can deploy in order to either steal information, harm the company, or both. Unfortunately, access to advanced technology is becoming easier at exponentially lower costs, which is affording hackers opportunities to penetrate systems remotely and still remain totally anonymous. Thanks to the credit card sized micro-computer known as the Raspberry-Pi, hackers can now add a fully operational remote controlled disposable packet scanner to a network, without breaking the bank at an average cost of $45. In combination with the free packet scanning software, Wireshark, the potential hacker now has a weapon of mass destruction. If a hacker were to utilize social engineering tactics and implant a Wireshark loaded micro-computer within the network they then gain virtually unlimited access to everything transmitted within that network, including any private data that may also be transmitted outside of that network as well (Hogg, 2013). Another

less common tactic that is equally as effective and even more dangerous is dumpster diving. Hackers who are unable to infiltrate the interior of a target may resort to dumpster diving in order to find information in which they can exploit and leverage to gain access to company assets. In most cases, companies that utilize stripped paper shredders or didn't bother to shred documents took the biggest hit. Hackers could locate the pieces to potentially damaging documents and paste them to boards, almost like putting a puzzle together. (Beaver, 2012).

Thankfully, in our technology driven culture we have learned to appreciate the need for certified information security analysts to fight for our overall digital protection. Information security is becoming an increasingly popular career field that pays billions of dollars annually. The side effect of supply and demand in information security is an over-saturation of technicians who may be able to quell any potential threats by formal training, but they are not skilled in proactively preventing any threats due to the fact that they do not think like a hacker. Most tools and education available to interested individuals focuses on the solutions to the problems not the root of the problems. This is not intended to discount the merit and validity of industry approved certifications, however; it is designed to challenge the mindset that companies have in regards to securing their information assets. As stated previously, training classes aimed at teaching I.T. professionals the necessary skills to mitigate network intrusions while halting vulnerability exploitation are not a one stop shop for ensuring a company's data is secure. Owners of big business, and small business alike, need to realize that in any type of intrusion scenario, the person with formal training and a deep understanding of networking concepts may be a good investment for a company's technological growth; however, they could very well be the root cause for a number of vulnerabilities. Unfortunately, in the current technological age we live in, the best way to ensure the integrity and security of information systems from hackers, is to hire

hackers to secure it. The concept is simple, fight fire with fire. However, the reality of this concept lies in the fact that hackers are part of a unique and diverse group of people who network globally. The majority of hackers belong to numerous organizations and forums which allow networking with other hackers. Unfortunately, at the end of the day, hackers are not impenetrable either and as time has shown in several cases, hackers need to brag about their exploits.

In conclusion, there are many ways in which an information system can become compromised and there are even more ways in which to protect a data system. The only true way to keep data safe from prying eyes is to not create "data" in the first place. However, in reality that is an impossible notion to impose on our technology driven society. Hackers have proven to be a formidable enemy to information technology specialists and will continue to be an enemy until the end of the digital age. In hindsight, however, hackers are also the best friend of the technology industry. Without hackers we would not understand the infinitesimal depths of electronic information security. Additionally, without hackers, we would not have the technology or software we have grown to love available today. Some of the world's most notable people were computer hackers such as; Steve Wozniak, who co-founded Apple computers with Steve Jobs, and Mark Zuckerberg the founder of Facebook. Unfortunately, if charged for computer crimes in which both individuals have admitted to committing, both Steve Wozniak and Mark Zuckerberg would more than likely be felons. Hackers have unknowingly brought the world a significant amount of convenience that we all enjoy today. Hackers have also helped to expose the darker sides of a world that attempts to appear impervious to corruption. Additionally, hackers have brought many of us a significant amount of heartache thanks to identity theft and virus distribution. However if companies wish to protect their assets from hackers, then they need to learn to fight fire with fire; or in this case, hack the hackers.

Bibliography

Beaver, K. (2012). *Hacking For Dummies.* New York, NY: Wiley Publishing.

Brito, J., & Watkins, T. (2011). The Cybersecurity-Industrial Complex. *Reason*, 28-35.

Bryner, B. A. (2014, July 15). *The Most Overlooked Data Security Measure*. Retrieved Jan 23, 2015, from The Protect IU Blog: https://protect.iu.edu/blog/2014/07/15/most-overlooked-data-security-measure

El Emary, I. M., Shalhoub, M. H., Arif, M. J., Alsereihy, H. A., Shalhoub, L. A., & Al-Sahhaf, N. A. (2013). Social Engineering and its Effective Role In Securing And Defensing The Knowledge Community. *International Journal of Academic Research*, 95-100.

Garvey, M. J. (2005). Utilities Wrestle With I.T. Security Standards. *Informationweek*.

Goldstein, E. (2008). *The Best of 2600 : A Hacker Odyssey.* Indianapolis, IN: Wiley Publishing.

Harrington, S. L. (2014). Cyber Security Active Defense: Playing With Fire or Sound Risk Management? *Richmond Journal of Law & Technology*, 1-41.

Hogg, S. (2013, October 30). *Raspberry Pi as a Network Monitoring Node*. Retrieved March 15, 2015, from www.networkworld.com: http://www.networkworld.com/article/2225683/cisco-subnet/raspberry-pi-as-a-network-monitoring-node.html

Luther, M., & Amy, V. (2015). Important Yet Overlooked Parts of Information Security. *ISSA Journal*.

Pascal, A. (2015, February 11). Hacked Hollywood Mogul Amy Pascal on Sony Attack: "All I Did Was Get Fired". (T. Brown, Interviewer)

Penenberg, A. L. (1999). The Demonizing of a Hacker. *Forbes*, 50-51.

Pentland, A. ". (2014). Saving Big Data from Itself. *Scientific American*, 65-67.

Ramamoorti, S., & Nayar, M. K. (2013). The Importance of Information Integrity. *Internal Auditor*, 29-31.

Shahani, A. (2015, March 15). *Premera Blue Cross Cyberattack Exposed Millions Of Customer Records*. Retrieved March 20, 2015, from www.npr.org: http://www.npr.org/blogs/alltechconsidered/2015/03/18/393868160/premera-blue-cross-cyberattack-exposed-millions-of-customer-records