Chapter 7 – Information Systems Security

7.1 Security Defined

Most consumers think of security from a superficial technical perspective. When the average person is asked what they think of "computer security" or "information security," their responses will involve descriptions of antivirus software, vague notions of hackers, and hiding their passwords. While these are important and valid concerns, they present a shallow understanding of what security really involves, especially from an organization's perspective.

An individual's personal security should involve protecting their hardware, access to data, and their own identity. It is generally common knowledge that this involves maintaining up to date antivirus software, not sharing one's Social Security Number (SSN), not sharing or writing down any passwords, password protecting their computer or mobile device, and choosing effective passwords for all of their logins. The effective password rule would be especially true for sensitive data such as financial organizations.

Organizations have a far more complicated job maintaining security. An individual does not necessarily provide data services to large sets of people. All individuals must concern themselves with is protecting one person. Most organizations provide service to multitudes of people and this opens them a number of security concerns. With their data sitting on a public portal, the Internet, it is now vulnerable to any number of targeted attacks. To complicate matters further, the organization likely has thousands of weak points within the organization: their human employees. Humans are notoriously unreliable for maintaining any semblance of security within an organization. Antivirus programs and password protections do not scratch the surface of tackling these complex problems.

Bringing the focus back to the individual consumer, one might wonder why an organization's overall security is of any concern to them. One need not look any further than one of the thousands of widely

publicized security breaches that happen on a regular basis. From 2013's Target data breach to 2014's Home Depot data breach to 2014's JP Morgan data breach, millions upon millions of consumers have had a direct impact by lacking security in organizations.

7.1.1 The Traditional Model

The CIA triad is a venerable model of security. The acronym stands for Confidentiality, Integrity, and Availability. It has been around for decades. At its core, the focus of this model is exclusively on the data itself. The data is the core of any system so there is a valuable applicability within this model. Ultimately, an organization must protect its data. One of the main criticisms of the model is that it oversimplifies the security issues organizations face. Since the data is contained within a technical bubble, the only needed solution, from the perspective of CIA, are technical in nature.

For example, Confidentiality is concerned with keeping data hidden and protected from those who should not access it. One of the easiest ways to implement this is to enact some sort of authorization or access control with the data. If an organization simply requires a password for accessing their data then they are ensuring the confidentiality of that data. For many years, this is exactly what most organizations thought was sufficient. The problem comes in when you have users writing their passwords down because they can't remember them. Now the value of the password has been dramatically decreased since it would be much easier for someone to find it. Passwords are also vulnerable to cracking software that can break password systems as well as other forms of bypass such as SQL injection.

Integrity refers to the data not being modified in an unauthorized or undetected manner. This can be implemented with access control, file and folder permissions, data backups (in case integrity is breached), and auditing (to detect a previously undetected breach). It is clear that Integrity is closely related to confidentiality. Data must first have its confidentiality breached before integrity violations can

occur. Notice as well that the main proactive approach to protecting integrity, access control, is the same as the only control for confidentiality. It is vulnerable to all of the same issues with password protection as Confidentiality. The other items listed are all reactive, after the fact methods.

The final component of the CIA triad, Availability, refers to the data being available to those who have authorization to access it. This is reliant upon functioning computers, software systems, and communications infrastructure. This can be dealt with by utilizing power backups (generator or battery powered), strategies for dealing with Denial of Service (DOS) attacks, and planned system redundancies.

7.1.2 The Managerial Model

In light of some of the deficiencies in the CIA triad, standards organizations such as the International Standards Institute (ISO), Organization for Economic Co-operation and Development (OECD), and the National Institute for Standards and Technology (NIST) developed more holistic and encompassing security guidelines. For example, in 2002 the OECD released the Guidelines for the Security of Information Systems and Networks. In this, nine principles were proposed: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. In 2004, NIST released the Engineering Principles for Information Technology Security standards report which proposed 33 security principles.

As security breaches continued to plague organizations, despite implementation of many of the technical tools called for with the CIA triad, the need for a new approach was palpable. Organizations took these standards and implemented them in a variety of ways. In a general sense, there was a need to understand the threats individual organizations faced, a need to implement a plan to handle these threats, a need to plan for the lifecycle of the security plan, a need to handle disasters, and a need to adhere to the ever increasing regulations handed down by government entities.

The first of these, understanding the threats, is implemented by an organization conducting a Risk Analysis. In a Risk Analysis, an organization identifies the assets, threats, vulnerabilities, impact of breach, and controls. It is simply a pre-audit of the assets an organization has, and determining what could steal or violate those assets. Organizations then determine how vulnerable a given asset is to a given threat and how much of an impact it would have if that asset was violated. For example, if it is determined that customer information is an asset and an external hack is considered a threat, how much would it hurt the organization if the customer information was stolen?

A Risk Analysis can inform the formulation of an organization's security policy. The policy is the formal plan for an organization's information security. It addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Two other components of the managerial approach are strategic in nature. One is the security development lifecycle. This refers to the continual cycle of analysis, policy formulation, and policy implementation. Security threats are constantly changing and organizations are also under continual change and flux. Performing one round of risk analysis and policy creation would be detrimental to an organization's security. Organizations should have a strategy in place to plan for this lifecycle of security development.

The second strategic component is business continuity. This is a strategy for how an organization plans to to continue operations if a place of business (such as an office, work site or data center) is affected by adverse physical conditions, such as a hurricane, tornado, fire, earthquake or crime. This plan explains how the business would recover its operations or move operations to another location. For

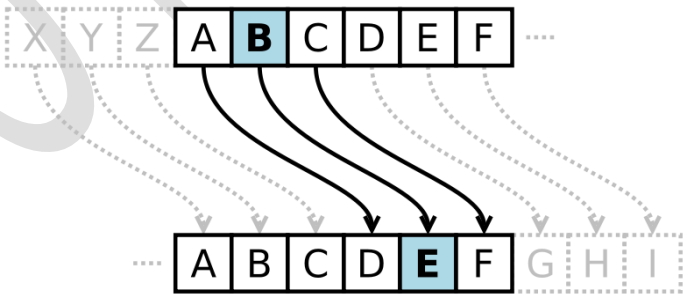
example, if an earthquake destroys an office building or data center, the people and business or data center operations would relocate to a recovery site. Creating this type of strategic plan forces a business to think outside of normal business operations and carry through the necessary steps to be able to recover in case of an emergency.

7.2 Historical Context

7.2.1 Ancient Applications of Data Security

In its earliest form, data security had limited application since data was limited to tangible hard copy and no computer systems or networks existed. The most common application was within the domain of military operations. When a message was sent between two points, it was done with a messenger who carried the message. If the messenger was intercepted, the enemy would have a distinct advantage with the new intelligence. Therefore, it became necessary to begin encrypting the messages.

One of the earliest known encryption schemes was the “Ceaser Cipher.” This encryption involved shifting the letters of the alphabet by a set amount in order to scramble the message. This can be seen in the following image:



For example, if the letters were shifted by one character, the message “Class is cancelled” would be encrypted to the following message: “Dmbtt jt dbodfmmfe”. Unless the interceptor knew the type of encryption used, the message would look like a jumbled mess. Over time, this encryption method

became well known and far less useful. In order to decrypt the message, one only has to attempt every possible combination of character shifts. Over “n” number of messages, the average number of attempts is only 13. Since there are only 26 letters in the alphabet, there are only 26 total combinations of encrypted strings. Assuming an equal number of attempts of encryptions among the different combinations, the average number of attempts will be 13.

Since this encryption method declined in usefulness, other methods took its place on the ancient battlefields. One well known method was the use of a scytale. A scytale was a cylinder with a strip of parchment wound around it on which is written a message. The message would be written vertically along the length of the rod. If someone intercepted the message, the letters would appear in apparent random order. Unless they knew it was written with a scytale and had with them an appropriately sized rod, they wouldn’t be able to decrypt it. The recipient used a rod of the same diameter on which he wraps the parchment to read the message. The “key” in this method was the diameter of the rod used to write the message.

7.2.2 Recent Historical Security Context

In 1957, Joe Engressia, a blind seven year old boy mistakenly discovered that whistling a certain tone would stop a dialed phone recording. He eventually learned that this tone was actually a control tone for the automatic circuit switches that had recently come into use for the telephone system. Joe befriended a man named John Draper who eventually learned that a whistle out of a box of Cap’n Crunch cereal made the same tone. They had essentially hacked the phone system. They were able to make international calls without being charged and the phone company was none the wiser. This early hacker group grew in numbers and soon the group were devising new ways to gain access to telecommunications infrastructure.

Over time, this group became known as phone phreakers. With pitch perfect whistling, Cap'n Crunch whistles, and eventually a tone generating blue box, they roamed the early telephone network with impunity. As ARAPNet and NSFNet expanded and Personal Computers became more widely available, early hackers found new areas to explore. Computer networks provided vastly more opportunities for exploitation. Instead of being restricted to various sounds and frequencies, they now had access to a command line where they could fine tune their commands.

The early computer networks also provided the opportunity for easy electronic gatherings via Bulletin Board Systems (BBSs). A BBS is software that allows users to connect and log into a remote centralized system using a terminal (command line) program. Once logged in, a user can do various functions such as exchanging messages with other users, uploading and downloading software and data, reading news and bulletins, and direct chatting. Originally BBSs were accessed directly over a phone line using a modem, but by the early 1990s some BBSs allowed access via Telnet, a terminal program that connects via packet switched network. There was now an easy to access community of like minded individuals that persists to the current day.

7.2.3 Public Perception of the People Involved

When a member of the public hears the term "hacker," it is generally interpreted in a pejorative fashion. Stories of security breaches at organizations are usually described as hacking by mainstream media outlets. This likely affects public opinion and perception of what hacking is. What many don't realize however is that hacking comes in many flavors.

The types of hackers that the public is thinking about are called "Black Hat" hackers. A "black hat" hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain. These are people who form the illegal groups that are often portrayed in popular culture. Their motivations are not always. Sometimes, there is a clear financial incentive while other breaches seem to

be only for the sake of chaos and mayhem. Within the community of hackers, black hat hackers are often referred to as crackers.

On the other end of the spectrum are “White Hat” hackers. A white hat hacker breaks security for non-malicious reasons. These reasons might include testing their own security system or working for a security company which makes security software. The term ethical hacker has been used to describe white hat hackers. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement with an organization. There is actually a security certification called “Certified Ethical Hacker” that one can test for that is designed to prove oneself as a capable but ethical hacker.

In between white hat and black hat are grey hat hackers. They generally are not malicious like black hat hackers but do not always take the most ethical route in their activities. For example, a grey hat hacker might illegally break into a computer network just to see if they can. Upon breaching the network, they may just leave and do nothing or they might let the organization know so that they can patch the vulnerability.

Within the culture of hacking there are subgroups that fall into the one of the three hats described above. There are also subgroups that are not easily categorized. For example, there are “elite hackers” who are the most skilled and widely known among the hacking community. They regularly discover new exploits and methods of attack. Some of them are white hat and some are black or grey hat. There are “script kiddies” who are the lowest of the low in the hacking community. They use pre-packaged automated tools to perform break-ins with no understanding of the underlying concept. Script kiddies are almost exclusively black hat and are generally neophytes. Most tend to tire of their activities after a limited time and move on and away from their hacking activities.

Another recent phenomenon is hacktivism. This is a hacker who utilizes technology to publicize a social or political message. An infamous hacktivist group is Anonymous. They were responsible for several high profile attacks including attacks on the Church of Scientology, Sony, Visa, the US Department of Justice, the FBI, the Motion Picture Association of America, North Korea, the National Security Agency (NSA), and Israel. Most of these attacks were simply aimed at either shutting down the target's website or taking over the target's website. If a site was taken over, it was usually replaced with whatever message the hacktivists were trying to convey. Depending on one's perspective, their actions could be considered black hat, grey hat, or white hat.

7.3 Should Security be a Concern?

7.3.1 Contemporary Anecdotes

Data breaches have occurred on a regular basis for as long as there have been computers and networks. The public tends to ignore these unless they are large scale, affect them personally, or are part of national media coverage. Several recent breaches have ticked all three of those boxes: the December 2013 Target breach, the September 2014 Home Depot breach, and the July 2014 JP Morgan Chase breach.

In December of 2013, the retail store Target discovered that is Point of Sale (POS) devices had become compromised with malicious software (malware). By the time of the discovery, the software had been running undetected for many weeks. In this time, more than 40 million debit card and credit card numbers had been stolen. Furthermore, 70 million consumers had their personal information stolen. As a result of this, Target is dealing with at least 200 lawsuits, $148 million in direct costs, and a decline in sales of 10%. Of far greater concern for Target is the potential for permanent damage to their reputation.

Home improvement retailer, Home Depot, found a similar type of breach in September of 2014. Their POS devices had become compromised and millions of credit and debit card numbers had been stolen. The duration of this breach was at least six months so a far greater number of consumers were affected. As of this writing, it is unknown exactly how many people were hit. It is estimated that Home Depot will be on the hook for billions of dollars.

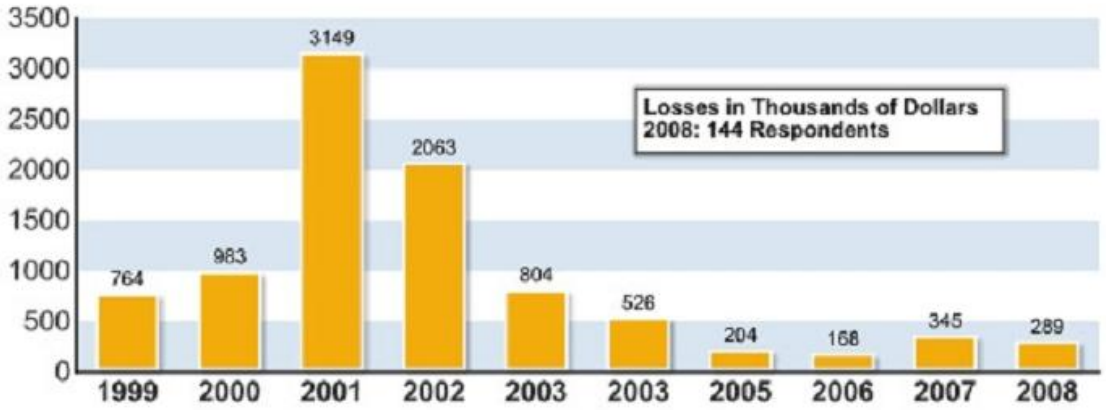
A final contemporary anecdote is the July 2014 discovery of a major data breach at JP Morgan Chase. Hackers had gained access to the internal servers at the bank and had this access for many months. It is still unclear how they got in. In this time, 76 million households were hit. No money was stolen but personal information, including Social Security Cards were stolen. It is likely that identity theft and social engineering will result from this theft. Like Target and Home Depot, this organization has faced serious damage to their reputation.

These anecdotes illustrate the critical nature of security in organizations. These are all well established large organizations with a large cadre of security personnel on hand. Despite their adherence to long standing security protocols and methods, the organizations still faced major breaches that damaged their reputation and cost millions of dollars.

7.3.2 Broader Trends

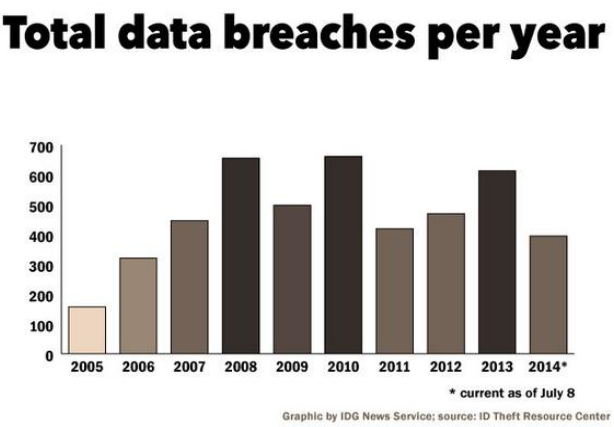
While anecdotes are useful for illustrative purposes, data trends are more useful for seeing a bigger picture. One such set of data is the FBI/CSI yearly computer security survey. One of the survey questions asks for direct monetary loss as a result of security breach. In the following image, one can see a spike in 2001, followed by a decline and eventually a steady state up to 2008:

Figure 14: Average Losses Per Respondent



The 2001 spike is clearly a result of 1000s of companies establishing an online presence during the peak of the "dot-com" boom. With so many companies putting their networks and data on a public portal like the Internet, breaches were bound to happen. As organizations refined their security to come in line with basic security standards, the breaches and monetary loss declined to a steady state. Note that the data only goes until 2008. This is because organizations became less willing to share information (even anonymously) about financial loss around this time. The data trickles to almost nothing after 2008.

Other data show some alarming recent trends that are demonstrative of a changing landscape in the security world. The following image shows the total number of data breaches per year and contains data up until 2014. While this does not show actual monetary loss, as the previous chart, the information about breaches is indicative of a worrisome trend. Since 2005, breaches have increased dramatically. Some of them result in monetary loss, others in information theft. Damage to the organization's reputation is likely consistent despite the type of breach.



Though organizations are becoming more secretive, it is clear that security is and should be a major concern for all organizations. From internal threats, to hackers breaking in from the outside, to accidental leakage, lost or stolen computers, organizations are under constant peril. The real victim and actual target in most of these attacks is really the consumer though. They are the ones who have to deal with stolen identities and fraudulent financial transactions.

7.4 Attack and Control

7.4.1 Technical Attack Vectors

7.4.1.1 Malware

There are countless attack vectors that hackers can take on the technical front. There are always vulnerabilities embedded within code and it's only a matter of time before these vulnerabilities are discovered by those with a desire to invade a system. With that said, there are widely known and reoccurring attacks that companies have had to deal with for decades. One of these is malicious software (malware).

Malware can take the form of viruses, Trojan horses, worms, or spyware. Viruses are software that replicate by inserting copies into other computer programs. When this replication succeeds, the affected

areas are then said to be "infected". Viruses often perform some type of damaging activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

Viruses currently cause billions of dollars worth of economic damage each year due to systems failure, wasting computer resources, corrupting data, and increasing maintenance costs. In response, free, open-source antivirus tools have been developed, and a multi-billion dollar industry of antivirus software vendors has cropped up, selling virus protection to users of various operating systems. The lingering problem is that virus protection software is only as good as its library. Virus libraries are updated when viruses in the wild are discovered and logged. Considering the fact that there are always viruses in the wild, virus libraries are perpetually out of date. Thus, the danger remains no matter how vigilant an organization is at maintaining their antivirus software.

Trojan horses are similar to viruses in that their function is generally harmful to the infected computer. The primary difference is in delivery. A virus is generally a standalone malicious program that is run unintentionally (for example by opening a Word document attached to an email that happens to have a macro attached to it). A Trojan horse hides inside of software that appears to be useful in order to persuade victims to install them on their computer.

Worms differentiate themselves from Trojan horses and viruses by what they target. While a Trojan horse or virus target a single machine, a worm replicates itself on the network. They consume bandwidth simply by continuous replication. Sometimes there is a payload in a worm that attacks a host system by deleting files or installing a backdoor on the system. The backdoor can then be used to create a zombie computer that is under the control of the attacker.

Finally, in the malware category there is Spyware. This is software that a person installs that gathers information about that user and reports back to the software provider. This is typically done without the consumer's knowledge. A common use of spyware is to track a user's web browsing activity in order to send targeted advertisements to that user in the form of pop up windows. Some Spyware will reroute the user to specific websites in order to maximize commercial utility. Unlike viruses and worms, Spyware does not self replicate. It is designed to run by itself. The delivery method is typically similar to Trojan horses in that the spyware is installed along with a seemingly useful piece of software.

7.1.1.2 Denial of Service Attacks

Another common attack vector is the Denial of Service (DOS) attack. A DOS attack simply makes a computer or service unavailable to its intended users. Most DOS attacks are on web servers. A variation of the DOS attack is the distributed DOS (DDOS) attack. While DOS attacks come from one source, DDOS attacks stem from many sources. These sources can be other attackers working in coordination or an army of zombie computers under the control of a single person. Another type of DOS attack is a permanent DOS (PDOS) attack. This is known as phlashing and damages a system so badly that the hardware needs to be replaced. An attacker does this by exploiting Operating System vulnerabilities to flash a system's firmware with modified firmware. This permanently destroys the hardware and renders it incapable of providing service.

The way a DOS attack works is by saturating a target machine with communications requests to the point that the machine cannot respond to legitimate traffic. These attacks can eventually lead to server overload and shutdown. In most cases DOS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address.

The previously described hacker group, Anonymous, uses this attack vector regularly to shut down services to companies. Most of their attacks are of the DDOS variety. Sometimes DOS attacks can be by accident. For example, if a large news aggregate site like reddit.com shares a site with its millions of users, that site can be flooded with their legitimate clicks. If the site is only designed to handle 10,000 users in a given day and 10,000,000 users hit the site within an hour, the site's host will shut access to the site off.

DOS attacks are very difficult to protect against. Public portals are intended to be open by their very nature. If an attacker is using some sort of IP spoofing to shift their location with each hit of the server, there's no way for a system's administrator to pinpoint where the attack is coming from. Some sites have been shut down for very long periods during sustained attacks. One example of this is the Sony PlayStation network. It was shut down for several months in 2011 due to an extended DOS attack from Anonymous.

7.1.1.3 SQL Injection

SQLi takes advantage of SQL to exploit web servers with a database backend. SQL is a declarative language used to query, create, update and read delete data in databases. Unlike many conventional programming languages such as Python or Java, SQL is not an imperative language and does not specify logic in terms of step-by-step procedures. Instead, SQL facilitates the defining and manipulating of data through specifying the desired end results as queries composed of algebraic-like operators. Internal database algorithms then interpret and execute these queries to accomplish the desired outcome. SQL supports sophisticated querying through selection, grouping, and table-join operators as well as set-based operators such as union, intersection, difference, and Cartesian product. Typical operations inuses of SQL include building tables, populating the rows in tables, querying tables, deleting tables, updating records, and deleting records.

The primary form of SQLi consists of inserting code into user-input variables that are subsequently concatenated with SQL commands and executed. The technique takes advantage of a common software developer technique of dynamically building SQL statements. The most common example of this in action is when a user logs into a webpage. In order to authorize access, the system will compare what the user entered for the username and password against the set of usernames and passwords in the database. If the both the username and password are present, the user is granted access. The previous paragraph described how SQL is not a procedural language. In order to create the logic needed to do the comparison of user input and existing data, the SQL is embedded in procedural language like PHP or ASP. This code builds the appropriate SQL statements in a string variable based on the user input.

For example, if a user enters “bobsmith” for the username and “hunter2” for the password, PHP code might build the string variable $sqlstring as “select * from user_table where username = userinput1 and password = userinput2”. Within PHP, userinput1 would contain the substring “bobsmith” and userinput2 would contain the substring “hunter2”. The system would then run the SQL query. SQL queries utilize Boolean logic and this can be used by an SQLi attacker to their advantage. Note that in the SQL string just described, the two conditions (username and password) are connected with an AND operator. This means that both conditions must be true to return a result. If an SQLi attack found a way to embed a OR operator then the power of ANDing multiple conditions loses its significance.

This is exactly what SQLi attackers do. In one of the user input fields, they inject a fragment of an SQL query that contains the OR operator. They couple this with a condition that is always true, like 1 = 1, so that the query returns results no matter what else is entered. The fact that they entered a incorrect username and password is now irrelevant since the Boolean OR will override this and cause the query to return the results. They will have, in effect, bypassed the entire login authentication.

Another important aspect of SQLi is how databases interact with websites. Websites interact with databases via a three-tier architecture. At the top level, there is the web-based interface seen by the user. This is generally coded in Hypertext Markup Language (HTML) and is viewed within a web browser like Mozilla Firefox, Google Chrome, or Apple Safari. When a user interacts with a form on a website, the form calls the second level which is a server-side script. Recall that SQL is not procedural so SQL commands are typically nested within a language that is procedural (e.g., within an Active Server Page (ASP) script). The server-side script is referred to as "server-side" because it is procedural code that resides on the server rather than on the user's computer. Examples of server-side scripts include Microsoft's ASP, Adobe's ColdFusion, and the open source PHP.

SQL commands are embedded in server-side scripts, which then update, delete, or retrieve records from the database. Developers embed SQL commands within server-side scripts because server-side scripts make update, delete and retrieve SQL command dynamic. Rather than using a static SQL statement to retrieve or update records in a database, developers, by embedding SQL statements into server-side scripts can base a query on user input.

An example of a static SQL statement might look like this: SELECT * FROM employee-table WHERE employee-ID = 72. While this statement might work to return the employee who has an ID of 72, that's all it can ever do. It is not a practical thing for actual usage. On the other hand, if a developer embeds an SQL statement in a dynamic script, the ID could change depending on what the user needs at any give time. For example, there might be PHP code that looks like this: $sqlstring = "SELECT * FROM employee-table WHERE employee-ID = ". $_POST['employeeID-input']; In this code, the static part of the sql string is everything inside of the double quotes. Since this shouldn't ever change, it's fine to leave it hard coded. At the end though, there is a input variable that will change based on the user's input. The period

between the static string and the variable will join the two strings together. Now, a user can enter and search any of the employees in the employee table.

While incorporating user input into SQL commands allows developers to create dynamic SQL commands, users could also inject malicious SQL commands, thereby bypassing username and password authentication. By utilizing the simple nature of SQL, a malicious user could add on different types of SQL commands to their input fields. An example of SQL injection to bypass a password control would be the following:

- Username field: type “Admin” (assuming a valid username is “Admin”)
- Password field: type “1 or ‘1=1’”

In this case, the dynamically built SQL statement would read as (assuming a table name of tblEmployee):

Select Username, Password from tblEmployee where UserName=’Admin’ and password=1’ or ‘1=1’”.

This SQL statement would bypass the password control because username equals “Admin” (assuming a valid username is “Admin”) and while the password does not equal “1”, the second statement of 1=1 is true, so the entire where clause evaluates to true, thereby returning a record count of one. A record count of one implies that a record with the username and password has been found and allows a hacker to authenticate as the admin. Admin rights may allow a hacker to steal corporate data, change corporate data, or deface the website.

While many examples of SQLi exist, one of the most prolific hackers who used SQLi was Albert Gonzalez. Between 2005 and 2007, he and his co-conspirators used SQLi attacks to steal 170 million credit cards. His targets included Dave & Busters, CardSystems Solutions, and Heartland Payment. It is not known exactly how much money he made by reselling the cards, but when he was eventually

arrested, authorities confiscated 2.7 million dollars in cash, a luxury car, laptops, firearms, a diamond ring, and Rolex watches.

7.4.2 Controls for Hardware and Software Based Attacks

There are well established sets of controls for hardware and software based attacks. These include virus scanners, access control, firewalls, encryption, and intrusion detection systems (IDSs), and secure development practices. Many of these provide a base level of security but as can be seen from the previous anecdotes and continued attacks, they leave a lot be desired.

As previously described, antivirus software is software that runs on a machine and scans for malware that might have infected that system. While this software is effective at keeping out 99% of the existing malware, it will always be vulnerable to zero day attacks. Zero day exploits are malware that have not been identified and catalogued by virus scanning libraries.

Like virus scanners, access control (authentication or username/passwords to access a system) are critical base levels of protection. Authentication only allows in those who should have access to a particular system and keeps out those who should not. Of course there are a good number of vulnerabilities that organizations should be aware. For example, a previously compromised system might have leaked the database containing the username/password data. A hacker could utilize social engineering (discussed in the following section) to trick a user into providing their username and password. The threat could originate from inside the organization with an employee who already has authentication to access the system. Passwords are not necessarily failsafe mechanisms in terms of protecting an organization's technology infrastructure.

Firewalls are software that controls the traffic coming in and out of a network. They are set up to keep out targeted attacks and only allow legitimate data in and out of an organization. Unfortunately

this is susceptible to attack. For example, an attacker can use a “brute force” attack to overwhelm a firewall. A brute force attack is similar to a DOS attack in that a flood of packets are sent at a target in order to flood its buffer and potentially cause it to shut down. Once the firewall is shut down, the network would be completely open. Another potential threat comes from viruses that users unwittingly execute from within the network (perhaps as an email attachment). These viruses can open up ports in the firewall.

Encryption involves the process of encoding messages or information in such a way that only authorized parties can read it. In encryption, the message, referred to as plaintext, is encrypted using an encryption algorithm and ciphertext is generated that can only be read if decrypted. In the historical context section of this chapter, early examples of encryption including the Ceaser Cipher and Scytale were described. People who purchase items over the Internet use encryption when sending their Credit Card number over the Internet. Encryption algorithms are advanced enough whereby they are virtually impossible to break. It is considered a best practice to encrypt all sensitive data that is in transit or at rest within a system.

An Intrusion Detection System (IDS) is software that monitors network or system activities for malicious activities or policy violations and either takes action or produces reports to systems administrators. An IDS evaluates suspected intrusions within a network and signals an alarm if one is detected. This is usually achieved by examining network communications, identifying heuristics and patterns or signatures of common computer attacks, and taking action to alert administrators. These are effective tools in the arsenal of protection for an organization’s network.

Secure Development practice refers to the embedding of security principles within the development of software. For example, the SQLi attacks described in the previous section can be easily stopped by using secure development practices. If developers were made aware of the threat and included code to

protect against SQLi, the system would be protected. Beyond SQLi attacks, secure development would minimize vulnerabilities that hackers use to attack systems. Poor code writing opens up a system to untold problems.

7.4.3 Sociological Attack Vectors

People based attacks are actually more vexing than technological attacks. When a technological attack becomes widely known, most organizations will move to protect their technology infrastructure from whatever the vulnerability is. People, on the other hand, are not predictable and not easy to train out of common habits. The four most common methods of people based attacks are social engineering, phishing, insider attacks, and physical theft.

Social Engineering involves the psychological manipulation of users by an external entity in order to divulge sensitive information. A common target of this information is the login credentials of the target in question. This is typically done by way of a quid pro quo, meaning the attacker offers help for some made up problem (such as a technical problem with the target's account) in exchange for some information. If an attacker calls enough people at an organization, they are likely to run into a person who has a legitimate problem. This increases the likelihood that this person will see the call as valid. This scenario is usually not needed. Research has found that roughly 90% of office workers will give up their password in exchange for a cheap pen or chocolate.

Another common form of social manipulation is phishing. This involves casting a wider net than you would with the individual calls for a quid pro quo. It is typically implemented with an organization-wide email that pretends to come from a legitimate source. This could be a business partner, technical support company, etc. Another form is to act on the gullibility and greed of the individual. The phishing attack might pretend to be a notification from a lottery or a wealthy individual looking to distribute his or her money.

One of the most infamous of phishing is the Nigerian 419 scam. This is a widely perpetrated scam that involves a fraudster promising a target a large sum of money. After trust is established, the attacker will require an upfront payment in order to release the promised money. A variation of this has been seen recently in tight housing markets like New York City. The scammers will post attractive apartment rentals to sites like Craigslist. During the initial communication, they say that they live out of the country and would like to sign the lease, receive the deposit, and send the key via mail. If the victim agrees, they will lose the deposit money since the apartment never actually existed.

A final major category of people based attacks is the insider threat. This is considered a people based attack since, by definition, all of the technical controls will already have been bypassed. The insider threat can come from a disgruntled employee or a simple opportunist. There is a large amount of research that points to the insider threat as the most serious threat facing organizations.

7.4.4 Controls for Socially Based Attacks

There are three major strategies for dealing with socially based attacks: security training, regular psychological screening, and auditing. Training and screening are intended to be proactive in nature and aim to prevent the problem before it happens. IT auditing is reactive and aims to determine if a problem occurred after the fact.

Training typically occurs when an employee starts employment at an organization and might be repeated on a yearly basis. Regular training is most effective as security threats evolve over time and to refresh the employee's exposure to the concepts at hand. Most training involves helping the employee become familiar with the security protocols of the organization. These protocols cover both the technical and social issues. For example, an employee would likely be instructed to never give their username and password to any person on the phone. The attempt is to avoid the problems associated with social engineering.

Psychological screening is usually reserved for employees that handle sensitive data. For example, a Systems Administrator has access to the entire set of company data. They could cause catastrophic damage if they were so inclined. It is in the company's best interest to ensure that these types of employees are on the level. Unfortunately, this type of invasive screening is not normally applied to higher level employees like executives. They too can and have destroyed large companies as a result of greed and bad decision making. Screening might have caught their activities before it was too late for the company.

The final piece in the puzzle in terms of controlling for social based attacks is the use of IT and financial auditing. The best one can hope with this technique is to determine if a problem has already occurred within the organization. IT auditing involves reviewing the server logs for unusual activity in terms of file access, data manipulation, and control adherence. IT audits can include analysis of the systems and applications, IT facilities, systems development, enterprise infrastructure, and network software and hardware.

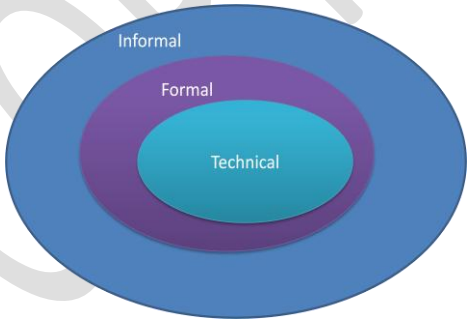
7.5 The Future of Security within Organizations

This chapter has covered two broad views of security: the technical and the managerial. At the core of any security plan, organizations should ensure that their technical controls are in place. Protecting the data with authentication, encryption, virus protection, network control (firewalls), Intrusion Detection Systems, and secure development practices is crucial. Ignoring any of these tools is leaving the organization open to attack.

It is as important to wrap these technical tools in a blanket of managerial protection as well. Performing a risk analysis, formulating and implementing effective security policy, and strategizing for an effective security lifecycle are as critical as the technical tools at the core. Like the technical tools, ignoring any of these higher level managerial tools will leave the organization vulnerable.

Recent research by Lapke and Dhillon[1] has uncovered yet another area that should be considered moving into the future. While the technical and managerial (or formal) layers offer a solid layer of protection, there are missing pieces. These revolve around the cultural and power relationship changes that occur as the result of security policy implementation. By its directive nature, security implementation affects existing power relationships within an organization. This can lead to problems with the implementation and ultimately a weaker policy within the organization.

This research indicates that a third area should be considered when discussing information systems security at organizations. As seen in the figure to the right, this new layer, the "informal" layer surrounds the managerial or "formal" layer. The formal layer surrounds the core of security at the organization: the technical. Analyzing and understanding the informal aspects of security implementation at an organization informs how the risk is analyzed and how the policy is formulated and implemented. The policy implementation directly impacts how the technical tools are implemented at the lowest level.



This holistic and complete view of security should be considered as organizations move towards the future. As was seen in the previously described anecdotes and data trends, problems and issues in security will continue to plague organizations indefinitely. It is in the organization's best interest to maximize their efforts in security their organization.

[1] Lapke, M and Dhillon, G, "Power Relationships in Information Systems Security Policy Formulation and Implementation" (2008). ECIS 2008 Proceedings. Galway, Ireland.