Curriculum Development for Fraud, Identity Theft, and Identity Management Content in Graduate Level Information Assurance Programs

Dr. Kevin Streff
Kevin.streff@dsu.edu
Dakota State University

Nick Pullman
nick.pullman@citi.com
Citigroup, Inc.

Abstract

Fraud, identity theft, and identity management is an important topic as part of an information assurance curriculum. Identity theft and identity fraud continue to grab headlines with high profile breaches causing significant losses to consumers and businesses. This paper will discuss the curriculum for a self-contained class on the topic of fraud, identity theft, and identity management. In addition, the paper will discuss the relevance of the topic to the financial services industry. In this paper we present key topics such as the drivers behind fraud, and identity theft; the regulations and regulators of financial services and other industries, identity theft and identity fraud attacks such as phishing, pharming, and skimming; and identity and access management concepts such as provisioning, password management, single sign on, and access control.

Keywords: Identity Management, Access Management, Information Assurance Curriculum, Security, Privacy

1. INTRODUCTION

According to the 2003 FTC report on Identity Theft, identity theft and identity fraud cost businesses an estimated 47.6 billion dollars in 2002 with 9.9 million cases of identity theft and identity fraud (Federal Trade Commission, 2003). Identity theft continues to grow, and according to data tracked by the Sentinel database maintained by the FTC, complaints of identity theft and fraud rose from 542,656 in 2003 to 686,683 in 2005 (Federal Trade Commission, 2003). The importance of security practices to combat identity theft and identity fraud is clearly important to not only protect businesses from direct monetary losses, but also from the potential loss of goodwill.

Identity management is another area of information assurance that is important for students to understand. Regulations such as Gramm-Leach-Bliley for financial data and HIPAA for medical data require that organizations protect the privacy and integrity of their customers' data (Gramm-Leach-Bliley Act, 1999, (U.S. Department of Health and Human Services, 2008). In order to prevent unauthorized access to this data, strong identity and access management processes must be implemented. Students must have an understanding of the requirements of protecting the confidentiality and integrity of consumer data and how to secure it from unauthorized disclosure.

It is clear that there is a need for students studying information assurance to have a strong understanding of the problems caused by identity theft and identity fraud as well as ways to protect against them. Students must understand how to secure the consumer data that they process, transmit, and store, and they must understand how to protect the privacy of that data. This paper provides a proposed curriculum for a stand-alone class which discusses fraud, identity theft, and identity management. The paper discusses the format of the class, provides a course outline, describes the course content, and provides conclusions on the topic.

2. COURSE FORMAT

The format of the class will include approximately 35 hours of in-class discussion and lecture. The class will include significant discussion where problems will be given to the students and then the class will discuss some of the possible solutions. There will be a strong research and critical thinking component to the class with four minor assignments and one semester long research project. The four assignments will be 3-5 pages in length and ask the students to survey and analyze current issues and solutions for fraud and identity theft and to survey identity and access management topics. The major project will be 6-10 pages in length, research oriented, and chosen by the student. Each project will be different and each student will present their topic at the conclusion of the course.

There are some considerations that need to be made for distance or on-line learning. For distance or on-line learning, the presentation at the end of the course is not feasible and would be removed. Much of the discussion and lecture will take place on a university hosted message board with students expected to contribute and students will be graded on their participation.

3. COURSE OUTLINE

This section provides an outline of topics addressed in the course. It also serves to help set up the syllabus, select the appropriate text and plan the content of this course relative to other courses in your information assurance program.

I. Introduction to Fraud, Identity Theft, and Identity Management
    a. Definitions
        i. Identity Theft
        ii. Identity Fraud
        iii. Credit Card Fraud
        iv. Privacy
        v. Identity Management
        vi. Access Management

II. Fraud, Identity Theft, and Identity Management Drivers
    a. California SB 1386
    b. GLBA
        a. OCC
        b. Federal Reserve
        c. FDIC
    c. HIPAA

III. Identity Fraud
    a. Phishing
    b. Pharming
    c. Skimming

IV. Identity Theft
    a. Identity Theft vs. Identity Fraud
    b. Laws fighting identity theft

V. Identity Management
    a. Identity Management Lifecycle
    b. Proliferation of user identities
    c. Identity stores
        i. LDAP
        ii. Databases
        iii. Flat files
    d. Identity consolidation, aggregation, and synchronization
    e. Provisioning/Deprovisioning
    f. Workflow
    g. Password Management

VI. Access Management
    a. Role Based Access Control
    b. Single-sign on
    c. Auditing

VII. Authentication
    a. 3 Factors
        i. Something you know
        ii. Something you have
        iii. Something you are
    b. Multi-factor authentication
    c. Biometrics
        i. Physical
            1. Iris

2. Retinal
3. Facial
4. Fingerprint
5. Hand Geometry

ii. Behavioral

1. Signature Analysis
2. Voice Analysis

Each of these sections is further described in the next section: Section 4. Course Description.

4. COURSE DESCRIPTION

The course content will first discuss the issues in depth, and then discuss possible solutions both at a large national level and at a lower level such as an individual business. The following sections describe the major content of the proposed security curriculum.

Fraud, Identity Theft, and Identity Management Drivers

There are many reasons why organizations should want to protect the privacy and confidentiality of the customer data that they process, transmit, and store. For example, if customer data is disclosed to unauthorized parties, then the reputation of the company could be affected which as a result could cause the company to lose current and future customers. This possible negative affect to the reputation of the company occurs because many companies are required to notify customers when their personal data has been breached. California SB 1386 was the law enacted in California in 2003 that required notification to the customers for any data breaches containing their unencrypted personal information (Jepson, 2006). SB 1386 was really the beginning of this type of legislation, numerous other states have passed their own breach notification laws, and now there are numerous federal bills being proposed that essentially mimic SB 1386, but at the federal level (Jepson, 2006).

In addition to the fear of losing goodwill, organizations in certain sectors are required to protect the confidentiality and integrity of its customers' data. Two of the main pieces of data that must be protected are financial information and health information. Financial information has to be protected by banks because of the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), and any organization that processes credit card transactions needs to protect that financial information due to the Payment Card Industry Data Security Standard (PCI DSS).

The GLBA Safeguards rule requires that financial institutions protect the confidentiality and integrity of its customers' data. Organizations must create and implement a security program to prevent unauthorized disclosure or update (Gramm-Leach-Bliley Act, 1999). The three main bodies that ensure compliance with GLBA are the OCC, Federal Reserve, and FDIC. Depending on whether the financial institution is federally chartered, state chartered, a FDIC member, or a Federal Reserve member determines which regulatory body, or bodies, will ensure compliance (Spong, 2000). The PCI DSS is a security standard which protects credit card specific data. The standard requires that any company, not just financial institutions, that processes, transmits, or stores credit card data must protect that data (PCI Security Standards Council. 2006). Financial information is very important data to protect, and so it is necessary to understand GLBA and PCI DSS drivers behind protecting this confidential information.

Another important form of customer information is health information. The Health Information Portability and Accountability Act of 1996 (HIPAA) required national standards to be created to protect the confidentiality of individuals health information (Centers for Medicare and Medicaid Services, 2008). The basic structure of HIPAA and GLBA are quite similar with both regulations having requirements for privacy and security.

There are a number of drivers behind protecting users' personal information; some are legally required while others are not. Securing consumers' confidential data is an important function no matter what the drivers are behind it. Both financial data and health data are very critical to the well-being of individuals and so it's important for organizations to be sensitive to the confidentiality and integrity needs of the data and appropriately secure that information.

Identity Fraud

Identity fraud is a term that is often confused with identity theft. Identity fraud is when malicious individuals make fraudulent charges to a victim's account such as a checking or credit card account (Pastore, 2004). There are a number of ways in which malicious attackers can go about obtaining the necessary customer accounts such as phishing, pharming, and skimming. Attackers use these techniques to attempt to steal credit card numbers and bank numbers to commit fraud.

Phishing is the more common attack with approximately 10,091 unique phishing sites in August of 2006 (Phishing Activity Trends Report Q1 2008, 2008). Phishing refers to an attack which uses social engineering and technical subterfuge to compromise confidential information such as credit card numbers (Phishing Activity Trends Report Q1 2008, 2008). There are numerous types of phishing attacks, but the two main forms of phishing attacks are deceptive attacks and malware attacks (Emigh, 2005). Deceptive attacks are attacks where the attacker attempts to trick the victim into providing his/her confidential information. The most common example of this is a phishing email with a hyperlink to a spoofed website (Emigh, 2005) (or embedded html within the email); a spoofed website is a website which attempts to look authentic but is fraudulent forged website. The spoofed website looks real and requests the victim to provide their confidential information such as credit card numbers, usernames/passwords, or Social Security numbers (Emigh, 2005). Malware phishing on the other hand relies on Trojan horses, viruses, or other malicious software to obtain confidential information from the victim (Emigh, 2005). For example if a victim browses to a malicious website or is tricked into clicking on a link in a malicious email, a malicious piece of software may be downloaded to his/her computer. This could be any number of different malicious pieces of software such as keyloggers, screenloggers, session hijackers, or web Trojans (Emigh, 2005). The main purpose of this software is to collect the victim's confidential information. For example, if a victim's computer gets infected with a keylogger, the keylogger can record the victim's username/password when he/she logs into his/her bank's website.

Pharming is very similar to phishing, in that the user is tricked into providing their confidential information, usually to a spoofed website. The difference between phishing and pharming is that phishing is an attack on the user typically through malware or deceptive tactics. In phishing, the user has to click on a fraudulent link or redirected to the spoofed website. Pharming, in contrast, attacks the Domain Name System (DNS) in order to redirect the victim to the spoofed website (Schipke, 2006). In this case, even though the user types in the correct URL into the browser, they will be redirected to the spoofed website. DNS works by resolving domain names, such as google.com, to IP addresses. All hosts on the Internet have a unique IP address which is like an address for that host. Since IP addresses are difficult to remember, we use domain names instead of IP addresses and we use domain name servers to obtain the IP address for us (Wikipedia, 2008). If the domain name server is attacked and a fraudulent IP address is associated with a domain name, for example "citibank.com", then every person who uses that domain name server and visits "citibank.com" will be redirected to the spoofed website instead of the official website. Depending on how much that particular domain name server is used, a large number of users could be affected.

Skimming is a tactic that is used to obtain credit card or ATM numbers and/or make a copy of the card (Mohsberg, 2007). The attacker can then either use those numbers in "card not present" transactions such as those over the phone or Internet or make a copy of the card and use it as if it were their own card. Skimming occurs in a number of different ways ranging from very sophisticated to fairly simple. A very simple example would be a restaurant waiter/waitress who takes a credit card to the back room and processes the valid transactions, but then swipes the card through a second reader which stores the magnetic data from the card (Cleaver, 2003). The magnetic data stored on the skimming device can then later be retrieved and then used to create copies of the credit card. More sophisticated schemes involve ATM cards. In some of these scenarios, small card readers are placed over the top of the actual reader on the ATM machine and capture the magnetic data as the card passes through. A small camera may be placed above the keypad in order to capture the PIN number (Cleaver, 2003). The transaction proceeds normally, but what the victim doesn't know is that his card data was stored on the skimming device that was placed over the actual ATM card reader and their PIN was captured on camera.

Identity fraud is no doubt a difficult problem. Banks lose a lot of money due to fraud; however, according to Michael Pastore, in general banks believe that they have made great strides to containing fraud by using technology to detect patterns and anomalies (Pastore, 2004). Banks have been dealing with fraud for a long time and understand that fraud is a part of doing business. Security students need to have an understanding of the types of fraud is and what can be done to mitigate the problem from both a consumer perspective and a business perspective.

Identity Theft

Identity fraud and identity theft are two terms that are used to describe any crime that in which someone wrongfully obtains and uses another persons data for fraud or deception (United States Department of Justice, 2008). The two terms are very similar, but there is a distinction. Identity fraud really refers to fraud such as credit card fraud and check fraud, where the attacker is making some kind of fraudulent charge to the victims account. Identity theft, on the other hand, is when somebody steals the victim's identity to fraudulently open new accounts, buy houses, take out loans, or obtain false documents (Pastore, 2004). The distinction is that identity fraud is when an attacker commits fraud by using another individual's information such as using the victim's credit card. Identity theft is when an attacker steals the victim's identity and acts on behalf of the victim such as opening a new credit card account. Another distinction that can be made is that with identity fraud, the attacker typically has information such as the victim's credit card or bank account number, but with identity theft, the attacker has to have more information such as the victim's Social Security Number, phone number, date of birth, and address. The two terms identity theft and identity fraud are related, but there is a distinction and it is important for students understand the difference between the two.

There are laws that aim to reduce the prevalence of identity theft by imposing strict penalties for anyone who commits these crimes. These laws focus on punishment for those who commit identity theft and those who produce and/or transfer fraudulent documents. The Identity Theft and Assumption Deterrence Act was passed in 1998 and has a maximum penalties of up to 15 years in jail and a maximum fine of $250,000 (Koerner, 2006). The Identity Theft Penalty Enhancement Act, was enacted in June of 2004, and increases the penalties that can be levied against the fraudsters (Social Security Administration, 2004). These two laws aim to directly deter ID theft by imposing strict penalties on anyone who knowingly commits ID theft. In addition, laws like Gramm-Leach-Bliley and HIPAA attempt to limit what information must be protected and how it can be used. These laws, while they don't directly attempt to thwart identity theft, attempt to protect consumer data which makes it more difficult for identity thieves to succeed. In the end, the combination of the data confidentiality laws and the identity theft deterrence laws make an effort to protect customer data from identity thieves and to punish identity thieves when they do commit a crime help to deter identity theft, but it isn't a complete solution.

Identity theft is obviously an issue and recent attempts, such as the Identity Theft Penalty Enhancement Act, to curb the issue have been relatively unsuccessful. Some of the recent studies show that identity theft continues to be a huge problem. For example, a 2003 survey performed by the Federal Trade Commission found that 4.6% of the respondents were victims of identity theft which equates to approximately 10 million cases of identity theft (Federal Trade Commission, 2003). In addition, a 2004 study performed by the FDIC lists identity theft as the fastest growing type of consumer fraud (Federal Deposit Insurance Corporation, 2004). Identity theft continues to be an issue that doesn't have an easy fix, but students need to be aware of the scope of the problem and the measures that have been enacted to try to protect against it.

Identity Management

The course content discussed so far has been about large national issues such as fraud and identity theft, but those are far reaching problems that while difficult to solve on a national level, organizations can implement safeguards to protect its customers' data from identity thieves. Organizations need to take a layered approach to information security and identity and access management is one of those layers. Organizations must understand who is using their systems and what functions the users are performing on those systems. In addition, one of the largest threats to an organization is not from the outside, but from inside of the organization. According to the 2005 E-Crime Watch Survey, 64% of the theft of intellectual property was caused by insiders and that 54% of unauthorized access to systems was caused by insiders of the company (US-CERT Coordination Center, 2005).

Identity management is concerned with how to manage identities within an organization, including users and their accounts. Identities can be employees, consultants, or business partners and in a looser sense even accounts on individual systems. In order to understand identity management, you must understand the following concepts which make up identity management: the identity management lifecycle; the proliferation of user identities; identity stores; identity consolidation, aggregation, and synchronization; provisioning / deprovisioning; workflow; and password management.

The identity management lifecycle is the basic process that a user account follows; the account is created, used, maintained, and then deleted. In addition, the entire process is encased in an audit function which reviews the account information and access (Smith, 2005). These accounts should be unique to the user and should not be shared so that there is individual responsibility for the user accounts. The identity management lifecycle lays the foundation for the rest of the concepts in identity and access management by providing the framework to discuss the issues and solutions at each phase of the lifecycle.

User accounts are created often within an organization and in a large organization it wouldn't be uncommon to find more than 100 different identity stores which store user account information (Microsoft Corporation, 2006). The problem with this is that organizations tend to operate in silos with each application or system managing its own set of user accounts, i.e. identities. This makes managing all of those accounts, not only difficult and time consuming, but all of this overhead causes account information to possibly become out of synch which continues to contribute to the problem. In addition, with so many accounts, it becomes difficult to audit the users to determine what entitlements they posses and becomes increasingly difficult to link users to the accounts that they own. For example, in a large organization, there may be ten "John Smiths" which makes it difficult to manage all of their accounts on many different systems since it is difficult to determine which accounts belong with which user. This makes having a unique employee identifier important; it can be used as the link between the user and their specific accounts.

Identity stores are directories, databases, or flat files that store identity information (Microsoft Corporation, 2006). Since each system/application often maintains its own identity store, as was mentioned before organizations tend to operate as silos, security administration becomes more difficult and complex. LDAP is one possible solution to try and curb this issue since LDAP has become common and can be used as an external identity store for multiple systems or applications. Using an external identity store such as an LDAP directory allows the organization to consolidate the identity stores; this makes administration and synchronization of user accounts simpler (Microsoft Corporation, 2006). Rather than each individual system/application having its own identity store, it can use an external identity store which will authenticate the users.

There are many cases where consolidation just doesn't make sense or is too difficult to implement, so the organization should attempt to keep those identities synchronized so that there isn't conflicting information and to aggregate them in order to get a unified view of the accounts. Two ways that this can be accomplished are with a meta directory or a virtual directory. A meta directory is a directory which contains data that is synchronized, copied, from multiple other directories (Sullivan, 2004). This allows data to be synchronized to a central location, the meta directory, and then that data would be synchronized back down to all of the other directories. This also gives a unified view of user accounts since they can all be seen from the meta directory. A virtual directory is similar to a meta directory, but instead of data getting copied to a centralized directory, the virtual directory provides a real-time logical view of the data; no synchronization is typically done with a virtual directory (Sullivan, 2004). Using these two technologies allows an organization to simplify user account maintenance with synchronization and improves the audit ability of the organization by having a single repository for identity information.

Provisioning is the process of creating user accounts and granting their entitlements, which can be time consuming if done manually (Sullivan, 2004). The process of deprovisioning accounts is the opposite of provisioning and the account entitlements must be removed and/or the account deleted, such as the case with a terminated employee (Microsoft Corporation, 2006). The issue with provisioning is that is it can be resource intensive and time consuming to perform. To remedy this, some form of automated provisioning can be employed; either HR provisioning or self-service provisioning. With HR provisioning, accounts are created or modified based on attributes that are stored on the individuals HR data; such as job title. Self-service provisioning, on the other hand, is requested by the user or the manager themselves and after an approval process or workflow the account is created or changed appropriately (Microsoft Corporation, 2006). A workflow is really just formalized business and security rules. The workflow, most likely implemented through a web based/email based application, provides the logic that must be followed before security actions are taken, such as management approval being obtained before the account is created (Microsoft Corporation, 2006). An automated provisioning application along with workflow can help organizations reduce the cost of manual administration of accounts

Password management is an area of identity management that is highly critical to the security of the organization and often has a high maintenance cost. The trade-off with password management is security and usability. If passwords aren't complex enough then the can be brute-forced attacked and if they are too difficult to brute-force, then they are typically hard to remember which causes security help-desks an undue number of calls. When selecting a password policy for determining how complex a password should be, the organization must weigh the security against the usability of the passwords. A typical password policy might be: a minimum of 6 to 8 characters; both alpha and numeric characters; a minimum of 1 upper-case character; and a minimum of 1 special character (Swanson & Guttman, 1996; National Institute of Standards and Technology, 2006). In order to help reduce the cost of help desk calls from password resets, organizations may want to implement a password self-service solution which lets users manage the password for their own accounts. These solutions typically require a user to "register" with the application by answering a series of questions, and then if the user forgets his/her password, he/she can authenticate to the application by correctly giving the answers to the questions that they registered with. The user can then manage their own passwords from within the application (Microsoft Corporation, 2006).

Identity management is a critical area for students studying security to understand. There are just as many risks to organization from inside of the firewalls as there is from the outside. Organizations must know who is accessing their systems and what they have access to on those systems. Students graduating with a security Masters Degree need to understand the issues with managing identities in an organization and possible solutions to solving those issues.

Access Management

Access management is an area of security which focuses on ensuring that users have only the access that they need to perform their job function. This is the concept known as least privilege (Microsoft Corporation, 2006). The users go through a three step process when they get access to a resource or perform a function: authentication, authorization, and auditing (Campbel, Calvert, & Boswell, 2003). First, the user is authenticated to the system. Second, the user attempts to perform the function or access a resource and the system/application checks to ensure that the user is authorized for that function or resource. Finally, the user performs the function or resource, and an audit record may be created as a record of the event. The resource or function can be protected at any of these three stages either proactively with authentication and authorization or reactively with auditing. The best method is a combination of all three of these.

It is important to minimize the access of the individuals in relation to their job function; they should have the least amount of privileges needed for their job. There are different methodologies that organizations can follow for managing account entitlements, but Role Based Access Control (RBAC) is the most common and important methodology to understand. RBAC is a methodology of grouping entitlements first into a group based on a role or job function and then connecting users to the groups based on their role or job function within the organization, which effectively gives the users those entitlements (Hitachi Id Systems, 2008). Most current systems have the ability to group entitlements together and so a RBAC implementation for a single system is fairly straightforward. Implementing RBAC across multiple systems in an organization is more difficult, but is essentially the same process with a role, rather than equating to a group, equates to multiple groups that are on multiple different systems; the scope of the role has merely increased. RBAC helps the organization to manage entitlements efficiently since they are logically grouped based on a role or job function within the organization.

We can effectively manage the resources that an individual is authorized to use by implementing RBAC. In order to effectively minimize the number of times that individuals have to authenticate to a system or application, single sign on (SSO) can be implemented. SSO is basically a process that will authenticate the user, and then every subsequent time that a user attempts to access an application that requires authentication, even across domains, the SSO application will automatically supply the necessary credentials (Pohlman, M, 2003). In today’s organization, it is not feasible to create a truly SSO environment, so a more appropriate term is reduced sign on. Reduce sign on is similar to single sign on but is more accurate because it takes into account the fact that organizations and technologies are too complex to be completely integrated.

Being proactive and limiting entitlements and authentication is very important; however, auditing the systems and their logs is just as important. Organizations need to understand what functions are being performed on their systems and which resources are being utilized. This is a requirement through HIPAA, GLBA, and Sarbanes-Oxley, but is absolutely critical even without the regulatory requirements. Three critical types of log reviews for access management are violations reporting, security changes reporting, and entitlements reporting. Organizations must review logs for violations to ensure that users aren’t abusing the system. Security changes reports must be reviewed to ensure that unauthorized changes weren’t made on the system and that authorized changes followed the correct procedures. Entitlement reports must be created and reviewed to ensure that accounts have the minimum privileges needed to perform their job functions. Auditing the logs of systems is a reactive process, but is absolutely essential to the security of the organization.

Access management is absolutely critical for students to understand. The risk from insiders is just as great as risk from outsiders and ensuring that user accounts only have the entitlements that are absolutely necessary for their job function is arguably the most important thing that an organization can due to mitigate risks from the inside. User accounts should only be created on systems where it is necessary and entitlements for resources should only be given where it is required. In addition, processes such as RBAC, SSO, and auditing help organizations to better organization and manage their environment.

Authentication

Authentication is the process of verifying the identity of the user that is attempting to login to a system or application (Campbel, Calvert, & Boswell, 2003). Authentication is the most important part of the three step process, authentication, authorization, auditing, that users go through when they get access to resources. The reason that authentication is so important is because if the authentication is not trusted, both the authorization and auditing cannot be trusted since they rely on the fact that the authentication was correct. For example, if an attacker somehow authenticates as an insider of the company, then the authorizations and audit logs are based on the fact that the actions are taken by the insider and not the attacker. There are three factors that can be used for authentication; something the user knows, something the user has, and something the user is (Campbel, Calvert, & Boswell, 2003). Multi-factor authentication is when two or three factors are used as the authentication mechanism; for example ATM cards require the user to both have the card and know the pin number (Committee on National Security Systems, 2006). Strong authentication in contrast is the use of multiple authenticators in order to verify the identity of the user; they may or may not be different factors. For example, if a website requires a username/password and a Passphrase, this would be strong authentication since it uses multiple authenticators, but is not multi-factor authentication because both authenticators use the same factor; what the user knows.

There are numerous forms of authentication that are available, but it is important to know a few of the more common ones; passwords/Passphrases, Kerberos, digital certificates, security tokens, and biometrics. Passwords are the most common form of authentication. The user has to provide the correct password along with their username in order to authenticate to the system. The problem with passwords is that they are easily attacked using brute force and dictionary attacks. A Passphrase is similar to a password, but instead of being single word or set of characters, it is usually a longer phrase or complete sentence. Passphrases are more secure, but aren't as commonly used (Campbel, Calvert, & Boswell, 2003). Kerberos is a network authentication mechanism which allows users to authenticate to services, such as a print server, over a network. Kerberos uses an authentication server to create encrypted tickets which are used to authenticate the user (Campbel, Calvert, & Boswell, 2003). Digital certificates are another way in which users can authenticate and are used extensively in Internet transactions. With digital certificates, Certificate Authorities (CAs) issue the certificates, after verifying the identity of the user or organization. These certificates are then used for public key cryptographic transactions such as SSL (Campbel, Calvert, & Boswell, 2003). Security tokens are small devices which provide one-time passwords for the user to authenticate with. These devices are synchronized with the servers that the user is trying to authenticate with, usually either by using a counter or by time (Campbel, Calvert, & Boswell, 2003).

Biometrics is another form of authentication and has shown some great potential for improving how users authenticate, but has not gained widespread use or acceptance. There are two main types of biometrics, physical and behavioral. Some examples of physical biometrics include fingerprints, hand geometry, retinal scanning, iris scanning, and facial recognition (Campbel, Calvert, & Boswell, 2003). Some examples of behavioral biometrics include signature verification and voice authentication (Campbel, Calvert, & Boswell, 2003).

Fingerprint biometrics look at the patterns on the tips of the finger as a means to authenticate the user. The devices are relatively inexpensive and the use of fingerprints is more common than other forms of biometrics. Hand geometry looks at different measurements of the hand such as the topography and shape. Hand

geometry, however, is not as accurate as some other biometrics and the scanning devices are fairly large (Campbel, Calvert, & Boswell, 2003). Retinal scanning and iris scanning both use the eye for authentication. Retina scanners look at the blood vessels at the back of the eye whereas iris scanners look at the patters of the colored part of the eye (Campbel, Calvert, & Boswell, 2003). Retina scanners are very expensive and are very intrusive because you have to position the eye very close to the scanner. Iris scanners are less expensive, using a normal camera, and users don't have to be as close to the device (Campbel, Calvert, & Boswell, 2003). Facial recognition biometrics analyze the different facial features in order to authenticate users. It is not yet commonly used and its accuracy can be reduced in low light environments (Campbel, Calvert, & Boswell, 2003).
Behavioral characters can also be used as a biometric authenticator. Unlike physical biometrics which is part of the makeup of an individual, behavioral biometrics analyze how an individual performs an action such as signing their name or saying a specific phrase. Behavioral biometrics are typically not as accurate as physical biometrics due to the fact that peoples' tendencies and environment can affect the way in which they perform certain actions. With signature verification, the speed and pressure of the signature along with the final shape of the signature are used to authenticate the individual (Campbel, Calvert, & Boswell, 2003). Voice authentication captures a person's voice characteristics such as harmonic and resonant frequencies in order to authentication the individual (Gilhooly, 2003). This technology can be hampered by noisy environments and is more complicated to enroll users than other biometrics (Campbel, Calvert, & Boswell, 2003).

Authentication is one of the most important concepts to understand in security and students must have a strong understanding of the issues and solutions for ensuring accurate and secure authentication. Organizations must limit who can use their systems or applications and must ensure that only the authorized individual are allowed access to the systems/applications. There are numerous ways to authentication individuals and organizations must understand which technologies are appropriate. Organizations should also consider strong authentication or multi-factor authentication in order to improve the security of their environment.

5. CONCLUSION

Identity management is important to everybody's daily life. Students should be aware of the problems of identity fraud and identity theft and what current measures are being implemented to curb the prevalence of identity crime. The same problems for authenticating individuals in everyday life, such as with check or credit card purchases, also occur within an organization. Large organizations can find it difficult to manage and secure the user accounts of its employees, consultants, and business partners. Organizations must understand the identity management lifecycle and what actions or safeguards are required at each stage in order to maintain the confidentiality, integrity, and availability of its critical assets.

Efficiently and effectively managing user identity and entitlements is not an easy task, but is critical to the security of the organization. Students entering the field of information security need to understand the difficulties and importance of effectively managing users and their entitlements. In addition to security, the cost of identity management and access management can be very high if not managed correctly. There are numerous regulations that aim to ensure the confidentiality and integrity of customer information, and identity and access management is not only critical to meeting that requirement, but is also important for the overall well-being of the organization.

6. REFERENCES

Campbell, P, Calvert, B, & Boswell, S, 2003. Security+ guide to network security fundamentals. Thomson Course Technology.

Centers for Medicare and Medicaid Services, 2008. Medical Privacy – National Standards to Protect the Privacy of Personal Health Information. Retrieved June 2008. Available: http://www.cms.hhs.gov/SecurityStandard/

Cleaver, N. Skimming and its side effects. SANS Reading Room. 2003. Retrieved June 2008. Available: http://www.sans.org/reading_room/whitepapers/threats/1342.php

Committee on National Security Systems, 2006. CNSS Instruction No. 4009, 2006. National Information Assurance Glossary. Retrieved July 2008. Available: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Emigh, Aaron, 2005. Radix Labs. Online Identity Theft: Phishing Technology, Chokepoints, and Countermeasures. 2005. Retrieved May 2008. Available: http://www.antiphishing.org/Phishing-dhs-report.pdf

Federal Trade Commission, 2003. Federal Trade Commission – Identity Theft Survey Report. Synovate. September, 2003. Retrieved April 2008. Available: http://www.ftc.gov/os/2003/09/synovatereport.pdf

Federal Deposit Insurance Corporation. December, 2004. Putting an End to Account-Hijacking Identity Theft. Retrieved May 2008. Available: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

Gramm-Leach-Bliley Act, Pub.L.No. 106-102(1999).

Gilhooly, Kym, 2003. Voice Authentication: Making Access a Figure of Speech. ComputerWorld. Retrieved July 2008. Available: http://www.computerworld.com/securitytopics/security/story/0,10801,86897,00.html

Hitachi Id Systems, 2008. Identity Management Terminology. Retrieved June 2008. Available: http://idsynch.com/docs/identity-management-terminology.html

Jepson, K. Hush, 2006. Is it Ever All Right Not To Tell Members About A Security Breach. *The CU Journal Technology Report*, 10(3), 15. 2006. LexisNexis

Koerner, B., 2006. The Identity Theft and Assumption Deterrence Act of 1998. Retrieved March 2008. Available: http://idtheft.about.com/od/currentlaws/p/FEDIDLAW.htm

Microsoft Corporation, 2006. Microsoft identity and access management series: identity aggregation and synchronization. Retrieved April 2008. Available: http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/default.mspx?mfr=true

Mohsberg, Margot, 2007. American Bankers Association, 2007. ABA Encourages Consumers to Protect their Debit Cards from Skimming and Scamming at the ATM. News Release 2007.

National Institute of Standards and Technology, 2006. An introduction to computer security: the NIST handbook. National Institute of Standards and Technology. Retrieved June 2008. Available: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Pastore, Michael. Fraud Often Mistaken for Identity Theft. 2004. Retrieved June 2008. Available: http://www.insideid.com/idtheft/article.php/3434361

PCI Security Standards Council. 2006. Payment Card Industry Data Security Standard. Retrieved May 2008. Available: www.pcisecuritystandards.org

Phishing Activity Trends Report Q1 2008. Anti-Phishing Working Group. 2006. Retrieved May 2008. Available: http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf

Pohlman, M, 2003. LDAP metadirectory provisioning methodology. Writer's Showcase. IUniverse.

Schipke, Rae Carrington, 2006. The Language of Phishing, Pharming, and Other Internet Fraud: Metaphorically Speaking. Technology and Society, 2006. ISTAS 2006. IEEE International Symposium. Volume , Issue , 8-10 June 2006 Page(s):1 – 6.

Smith, Michael, 2005. Identity life cycle management. Identiprise. Retrieved August 2008. Available: http://www.mser.gov.bc.ca/privacyaccess/Conferences/Feb2005/ConfPresentations/Michael_Smith.pdf

Social Security Administration, 2004. Final Passage of H.R. 1731, the Identity Theft Penalty Enhancement Act. June, 2004. Retrieved May 2008. Available: http://www.ssa.gov/legislation/legis_bulletin_062904.html

Spong, K. Banking Regulations: Its Purposes, Implementations, and Effects. Federal Reserve Bank of Kansas City. 2000. Available:

http://www.kc.frb.org/BS&S/publicat/PDF/RegsBook2000.pdf

Sullivan, D., 2004. The definitive guide to security management, ch 5. Realtime Publishers. Retrieved September 2008. Available: http://www3.ca.com/eBook/Chapters.aspx?ID=65316

Swanson, M, & Guttman, B (1996). Generally accepted principles and practices for securing information technology systems. National Institute of Standards and Technology. Retrieved July 2008 Available: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

United States Department of Health and Human Services. Medical Privacy – National Standards to Protect the Privacy of Personal Health Information. Retrieved October 2008. Available: http://www.hhs.gov/ocr/hipaa/bkgrnd.html

United States Department of Justice, 2008. Identity Theft and Fraud. Retrieved July 2008. Available: http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

US-CERT Coordination Center, 2005. 2005 E-Crime watch survey. Retrieved February 2008. Available: http://www.cert.org/archive/pdf/ecrimesummary05.pdf

Wikipdia, 2008. Domain name system. Wikipedia. Retrieved June 2008. Available: http://en.wikipedia.org/wiki/Domain_name_system