2014 NSCP REGIONAL MEETING

Session 2a GI: 11:30 – 12:30

Cyber Security, Data Protection & Business Continuity (BC)

Glenda Bianchi Chief Compliance Officer, Cypress Wealth Management
Phone: (214) 736-8887 / E: gbianchi@cypress-wealth.com

Daniel E. LeGaye, Esq. Partner, The LeGaye Law Firm, PC
Phone: (281) 367-2454 / E: dan.legaye@legayelaw.com

DISCLAIMER

This paper is not intended to be relied upon as a final analysis in resolving legal questions. The information presented herein is intended to provide an overview of recent law and or trends. There is no substitute for a thorough review of the relevant statutes and laws to the facts of your particular situation by an experienced and competent attorney. Due to the summary nature of this paper, the level of detail necessary for a proper legal analysis of any particular situation cannot be reached.

A. INTRODUCTION

As a result of the increased dependence on digital technologies and computer hackers becoming more skilled at defeating the security features of outdated and antiquated technology, ensuring the security of customer information has become a top priority in the financial industry. In fact, Securities and Exchange Commissioner Luis A. Aguilar stated at the SEC Roundtable on Cybersecurity on March 26, 2014, that "cybersecurity has become a top concern to American companies, regulators, and law enforcement agencies. This is in part because of the mounting evidence that the constant threat of cyber-attack is real, lasting, and cannot be ignored."[i] The highly publicized security breaches that have hit big name retailers, government, social media websites and other corporate targets in recent history have pointed out the real risks inherent in the handling of the data and signals from broadband networks. The data and signals that power our personal computers, mobile devices, and local networks in our hospitals and businesses, are wide area networks that allow information sharing and business transactions across the globe. These massive grids enable critical government services, private utilities and exchanges to exist in cyberspace. In that light, protection of this all-encompassing network and the information transferred across it, is an integral part of a properly functioning financial market.

Cyber security incidents can result from deliberate attacks or unintentional events. Over the past year, there has been an increased level of attention focused on cyber-attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber-attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber-attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumventing network security or overwhelming websites, to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber-attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to individuals and companies, their customers, or other business partners. Persons and companies that fall victim to successful cyber-attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to the following:

- For individuals, cyber-attacks may result in identity theft, which can include assets being stolen, damaged credit ratings and a painful cleanup process.
- For financial companies, including broker-dealers and investment advisers.

  Firms face increased costs, which may include:

  - Remediation Costs related to liability for stolen assets or information, repairing system damage that may have occurred and potential cost of incentives offered to customers or other business partners in an effort to maintain the business relationships after a cyber-attack;
  - Increased cyber security protection costs may include organizational changes, deploying additional personnel and protection technologies, additional training of employees, and engaging third party experts and consultants;
  - Lost revenue resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
  - Costly litigation; and
  - Reputational damage adversely affecting customer or investor confidence.

B. Definitions

1. Cyberspace

Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to your friend, you could say you sent the message to her through cyberspace.

2. Cybercrime

Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Identity theft is currently the most prominent form of cybercrime in which criminals use the Internet to steal personal information from other users. Two of the most common ways this is done is through phishing and pharming. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

3. Domain Name

A domain name is a unique name that identifies a website. For example, the domain name of The LeGaye Law Firm is “legayelaw.com." Each website has a domain name that serves as an address, which is used to access the website. When you access a website, the domain name is actually translated to an Internet Protocol (IP) address, which is a 9 digit number, which directs the server to where the website located. This translation is performed behind the scenes by a service called DNS.

4. DNS

DNS stands for "Domain Name System." The primary purpose of DNS is to simplify the way we locate web-sites on the internet because web sites are actually located by their IP addresses and not the domain name. When you search for “apple.com”, your computer doesn't immediately know that it should look for Apples' Web site. Instead, it sends a request to the nearest DNS server, which finds the correct IP address for "apple.com".

5. Identity theft

It is the illegal or unauthorized acquisition, transfer, or use of another person's means of identification for criminal or fraudulent purposes. Means of identification can include a name, social security number, brokerage account number, or anything else that can be used to identify a particular person, including both physical items, like an identity document, or electronic authenticators, like a user-ID, PIN number or a password.

6. Malware

Malware is short for malicious software. Generally, it is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

7. Phishing

Phishing is similar to fishing in a lake, but instead of trying to capture fish, hackers focus on stealing your personal information. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or banking institutions. The e-mails state that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to your account.

8. Pharming

Pharming is another technique used by criminals and hackers to manipulate users on the Internet. While phishing attempts to capture personal information by getting users to visit a fake website, pharming redirects users to false websites without them even knowing it. While a typical website uses a domain name for its address, its actual location is determined by an IP address. When a user types a domain name into his or her Web browser's address field and hits enter, the domain name is translated into an IP address via a DNS server. The Web browser then connects to the server at this IP address and loads the Web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer in a DNS cache. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website.

One way that pharming takes place is via an e-mail virus that "poisons" a user's local DNS cache. It does this by modifying the DNS entries, or host files. For example, instead of having the IP address 17.254.3.183 direct to www.apple.com, it may direct to another website determined by the hacker. Hackers can also poison entire DNS servers, which means any user that uses the affected DNS server will be redirected to the wrong website.

9. Ransomware

Ransomware is a form of malware that has been around for a long time. Malware designers created ransomware to lock up the functions of an infected system and force the operating system to display a splash screen with some kind of message disguised to look like it was coming from an official agency or bureau (the FBI, NSA, CIA, etc.) that stated that due to some kind of deviant web-surfing behavior your system has been locked. By paying a fine, usually a few hundred dollars, your system would be unlocked. Historically, this ransomware had an important weakness. It could be removed without any long lasting effects to the most irreplaceable part of any system, your data.

The new generation of designers decided to change the paradigm. They didn’t design it to interrupt system function, instead they designed it to quietly seek out and encrypt as much personal data as possible in the background without the user’s knowledge. And only after the malware did that job would the user see the ransom note, which basically says if you want the key to decrypt your data, a key only the hackers now have, you’re going to have to pay again, usually a few hundred dollars. At this point the user is completely stuck. If they ever want to see their personal data again, they would either have to restore it from the backups they hopefully made, or pay up,

because even professional cyber security experts would not be able to reverse the encryption and regain access to the data once it is done.

10. Trojan Horses

Trojan Horses are malicious software programs that hide in files attached to an email or in a download from the Internet which installs on your computer. While these programs can take many forms, Trojan Horses used in identity theft scams usually take the form of keystroke loggers which are programs that log the keystrokes you type and allow criminals to find your usernames and passwords, giving them access to your online accounts. Trojan Horses have increasingly been showing up in "phishing" scams, or are being used in place of a phishing scam to secretly capture sensitive information.

11. Virus

Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

C. Regulatory Overview

1. Moving Forward

Officials throughout the Administration, including the White House, the Department of Homeland Security and the Department of Defense as well as Congress are making cyber security a priority. President Obama has expressed that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.” As a result, cybersecurity is now a top priority of regulators whose responsibility over the financial industry is to ensure the security of customer information and efficient, reliable execution of transactions.

2. Proposed Legislation & Standards

Lawmakers on Capitol Hill have been debating cybersecurity bills for many years, but opposition from industry and civil right groups have always stymied the initiatives. In 2012, the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA) despite vehement opposition from online privacy advocates and the White House. The Senate voted down a version of cybersecurity legislation, titled the Cybersecurity Act of 2012, in large part because of industry opposition.[ii]

There has been a wide variety of legislative proposals for safeguarding American computer systems and networks, but recent bills have focused on two goals. These include protecting critical infrastructure -- such as power plants, chemical facilities, communications networks, transportation networks and financial networks -- and promoting information-sharing between the government and industry. Information-sharing provisions examine ways to encourage private

companies to inform government organizations such as the National Security Agency about cybersecurity threats and responses. For affected industries, such provisions must include liability protection should they share information protected by privacy laws.

3. NIST Issues Cybersecurity Framework

On February 12, 2014, the Obama administration released the "Framework for Improving Critical Infrastructure Cybersecurity"(the "Framework") a voluntary cybersecurity framework developed by the National Institute of Standards and Technology ("NIST") in collaboration with a large number of groups and individuals from both the public and private sector.[iii] This occurred one year after President Obama signed Executive Order 13636 for "Improving Critical Infrastructure Cybersecurity,"[iv] which directed NIST and other federal agencies to work with the private sector to develop voluntary cybersecurity standards for private companies that operate "critical infrastructure," physical or virtual systems, and assets so vital to the U.S. that their incapacity or destruction would have a debilitating impact on security, the economy, public health or safety. The Framework outlines existing best practices and standards commonly used among banks, utilities and other critical infrastructure providers and "provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs." The Framework is technology and industry neutral and is intended to complement, not replace, an organization's risk management process and cybersecurity program by providing tools to identify gaps in its practices and develop a roadmap for continuous improvement. For organizations without a program in place, the Framework is intended to provide a foundation to design and implement a cybersecurity program.

a. Three Primary Components

The Framework is comprised of three primary components: the Framework Core, the Framework Implementation Tiers and the Framework Profiles. The Framework Core sets forth cybersecurity activities that are commonly employed across critical infrastructure sectors to achieve specific outcomes and provides examples of existing standards to facilitate implementation of those activities.

i. The Framework Core

The Framework Core addresses five basic functions to be included in an organization's cybersecurity risk management program:

- Identify – understanding systems, engaging in risk assessment and asset management
- Protect – developing safeguards for delivery of critical infrastructure services (e.g., training, data security and access control)
- Detect – performing detection and monitoring activities to identify cybersecurity events
- Respond – creating action plans for responding to and mitigating cybersecurity events

- Recover – restoring damaged capabilities and making improvements after an incident

ii. The Framework Implementation Tiers

The Framework Implementation Tiers allow an organization to classify the extent to which its cybersecurity risk management practices are rigorous and sophisticated (e.g., repeatable, adaptive, risk and threat aware), informed by business needs and integrated into its overall risk management practices, on a four-point scale from "partial" to "adaptive."

iii. The Framework Profiles

The Framework Profiles provide a mechanism to create "profiles" that reflect the overall state of cybersecurity risk management, including the alignment of cybersecurity activities with business requirements, risk tolerance and resources. An organization may create a "current" profile, a snapshot of an organization's existing cybersecurity practices, as well as a "target" profile, reflecting the desired state of its practices in the future. Organizations may compare these profiles to identify gaps and provide a roadmap for migrating to the "target" state.

b. Implementation Tiers

The NIST framework also establishes four implementation tiers, which describe how extensively a company might manage its cybersecurity risks. The higher the tier, the more advanced a company's risk management procedures become. Critical infrastructure companies defending their cybersecurity practices in litigation or regulatory investigations should be prepared to show that the practices adhere to Tier 4, considered "adaptive," meaning a company is regularly evaluating the threats it faces, testing its procedures, and modifying these procedures where appropriate to address new threats.

c. SIFMA Statement on the Framework

On February 12, 2014, The Securities Industry and Financial Markets Association (SIFMA) released a statement from Kenneth E. Bentsen, Jr., President and CEO, after the NIST issued the Framework. In his statement Mr. Bentsen stated in part "... Cyber-attacks are increasingly a major threat to our financial system and the financial industry is dedicating significant resources to protect the integrity of our markets and the millions of Americans who use financial services every day. The NIST framework is a meaningful step forward in protecting the nation as it establishes a voluntary set of standards that can be applied across all industries to help reduce cyber risks to our nation's critical infrastructure. .. SIFMA will work with our members to promote a greater understanding of the NIST framework and how it can be implemented"[v]. SIFMA is a major advocate of the financial industry.

d. DeFacto Standard

Ultimately, the Framework was conceived as a "living" document that will be updated in response to ongoing feedback and changing technology and risks. While

participation is voluntary, in the absence of legislation, the Framework could be used in the context of disputes or enforcement actions as a point of comparison in assessing whether a company's practices are unreasonable, or unfair or deceptive. To that end, the framework will become the de facto standard for private sector cybersecurity in the eyes of US lawyers and regulators. That's the view of Gerald Ferguson, who specializes in intellectual property and technology issues for law firm BakerHostetler, as expressed in a recent opinion column he wrote for InformationWeek.[vi] The Framework is positioned to become the de facto standard for litigators and regulators and it can be anticipated that the financial industry will see the bar being raised with respect to cybersecurity.

4. Securities and Exchange Commission (SEC)

a. SEC Roundtable on Cybersecurity

Recent breaches at Target Corp and Neiman Marcus have sparked concern from lawmakers and revived a long-running dispute among retailers and banks over who should bear the cost of consumer losses and technology investments to improve security with respect to credit cards. As a result, the SEC had a roundtable on cybersecurity on March 26, 2014, where the challenges that cyber threats pose for market participants and public companies was discussed in depth by market and industry professionals.[vii] This was the first major focus on cyber-attacks by the SEC since 2011, when the SEC drafted informal staff-level guidance for public companies to use when considering whether to disclose cyber-attacks and their impact on a company's financial condition.[viii]

In the session related broker-dealers and investment advisers, David G. Tittsworth, Executive Director and Executive Vice President, Investment Adviser Association noted that based on his conversations with investment advisers and industry professionals, account takeover was major concern for traditional investment advisors, while state sponsored terrorism and denial of services was the greatest concern for institutional and fund money managers. The concerns of institutional money managers is based in part on the fact that nations that sponsor terrorism view the financial industry as the heart of the United States, and as such, any injury inflicted on the markets or its participants advances their agenda. Overall, while the roundtable was a success in that it clearly achieved its goal of sharing information, points of view, and best practices, it remains unclear what additional rule making will result.

b. SEC IA Exams Chief: Small Firms Won't Get Cyber Security Rules Exemptions

"Small firms won't get a pass on cyber security rules", Securities and Exchange Commission Investment Adviser/Investment Company Examination Program Chief Jane Jarcho said at the Investment Adviser Association's compliance conference on March 7, 2014. (Knutson, 2014)

As these regulations are developed by the Office of Compliance Inspections and Examinations, the working hypothesis is that large firms are taking cyber security more seriously than small advisory businesses, Jarcho said. However, when cyber security rules

are disclosed, there won't be particular, absolute precautions that have to be taken. Jarcho offered no timetable on when the rules would be released.

5. FINRA

a. 2014 FINRA Regulatory and Examination Priorities Letter

On January 2, 2014, FINRA published its ninth annual Regulatory and Examination Priorities Letter[ix] to highlight significant risks and issues that could adversely affect investors and market integrity in the coming year. FINRA noted that Cybersecurity remains a priority for FINRA in 2014 given the ongoing cybersecurity issues reported across the financial services industry. In recent years, many of the nation's largest financial institutions were targeted for disruptions through a range of different types of attacks. The frequency and sophistication of these attacks appears to be increasing. In light of this ongoing threat, FINRA continues to be concerned about the integrity of firms' infrastructure and the safety and security of sensitive customer data. Their primary focus is the integrity of firms' policies, procedures and controls to protect sensitive customer data. FINRA's evaluation of such controls may take the form of examinations and targeted investigations.

b. Targeted Examination Letters, Regarding: Cybersecurity

FINRA announced in January 2014 that it is conducting an assessment of firms' approaches to managing cyber-security threats.[x] FINRA is conducting this assessment in light of the critical role information technology (IT) plays in the securities industry, the increasing threat to firms' IT systems from a variety of sources, and the potential harm to investors, firms, and the financial system as a whole that these threats pose.

FINRA has four broad goals in performing this assessment:

- to better understand the types of threats that firms face;
- to increase our understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT systems;
- to better understand firms' approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervision; and
- as appropriate, to share observations and findings with firms.

FINRA's assessment also addresses a number of areas related to cybersecurity, including firms':

- approaches to information technology risk assessment;
- business continuity plans in case of a cyber-attack;
- organizational structures and reporting lines;
- processes for sharing and obtaining information about cybersecurity threats;
- understanding of concerns and threats faced by the industry;

- assessment of the impact of cyber-attacks on the firm over the past twelve months;
- approaches to handling distributed denial of service attacks;
- training programs;
- insurance coverage for cybersecurity-related events; and
- contractual arrangements with third-party service providers.

Daniel M. Sibears, Executive Vice President, Regulatory Operations/Shared Services, FINRA, who was a participant in the SEC Roundtable on Cybersecurity stated that this area is a key issue for FINRA, and the goal sweep on cybersecurity was to push out effective practices to membership. In light of the fact that the last two sweep exams (Business Continuity and Conflicts of Interest) that occurred as a result of FINRA Issuing a Targeted Examination Letter resulted in FINRA issuing additional guidance to membership on the respective topics, Mr. Sibears' observation appears foretelling, and it is reasonable to believe that FINRA may be issuing new guidance with respect to best practices within the year. As conflicts of interest and new guidelines on business continuity plans are now in the exam program, it is probable that the recommended best practices on cybersecurity will be integrated into the exam program as well.

6. Commodity Futures Trading Commission (CFTC)

The CFTC issued CFTC Staff Advisory No. 14-21 on February 26, 2014, which outlined recommended best practices for covered financial institutions to comply with Title V and Part 160 of the CFTC's regulations concerning security safeguards. [xi]

a. Part 160 of CFTC's Regulations

Part 160 of the CFTC's regulations requires that futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants "must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." As outlined in Part 160.30, those policies and procedures must:

- Insure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

b. Recommended Best Practices

The CFTC's recommended best practices include the development and implementation of a written information security and privacy program that is appropriate

to its size and complexity, the nature and scope of its activities, and which requires the firm to, at a minimum:

- Designate a specific employee with privacy and security management oversight responsibilities, who is part of or reports directly to senior management or the Board of Directors;
- Identify, in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information and systems processing personal information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information or systems, and establish processes and controls to assess and mitigate such risks; also, identify such risks, and establish processes and controls to assess and mitigate risks, before implementing new or material changes to internal systems;
- Train staff to implement the program, and provide regular refresher training;
- Regularly test or otherwise monitor the safeguards' controls, systems, policies and procedures, and maintain written records of the effectiveness of the controls, including the effectiveness of:
    - Access controls on personal information;
    - Appropriate encryption of electronic information in storage and transit;
    - Controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information; and
    - Employee training and supervision relating to the program.
- Obtain an independent party to test and monitor the safeguards' controls, systems, policies and procedures at least once every two year;
- Regularly evaluate and adjust the program in light of: the results of the risk assessment process; relevant changes in technology and business processes; any material changes to operations or business arrangements; and any other circumstances that the entity knows or reasonably believes may have a material impact on the program;
- Design and implement policies and procedures for responding to an incident involving unauthorized access, disclosure or use of personal information, including policies and procedures to assess the nature and scope of any such incident, and maintain a written record of the systems and information involved;
- If the covered entity determines that misuse of information has occurred or is reasonably possible, then as soon as possible notify individuals whose information was or may be misused and notify the Commission in writing

explaining the situation and possible risks (unless law enforcement requests in writing that notification be delayed); and

- Provide the Board of Directors an annual assessment of the program, including updates to the program, the effectiveness of the program, and instances during the year of unauthorized access or disclosure of personal information.

7. Massachusetts Model

The Commonwealth of Massachusetts enacted a law titled "Massachusetts Standards for the Protection of Personal Information" (201 CMR 17.00),[xii] which was designed to protect state citizens' personal information. This state law is currently the most expansive privacy law in the United States, and applies not only to firms located in Massachusetts, but also to companies that handle any personal information of Massachusetts residents.

Under the law, "personal information" to be protected includes a Massachusetts resident's name (either first and last name or first initial and last name) combined with a complete social security number, driver's license, or other state-issued number, a financial account number or a complete credit card or bank account number. This encompasses a wide variety of informational records - everything from employee, client, customer and investor records to supplier, patient and student records. What it does not include is any information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

Businesses handling of personal information of Massachusetts residents must:

- Create a written information security program (WISP) that identifies all sensitive information, security risks and controls;
- Designates an employee responsible for the WISP;
- Encrypt electronic PII sent over the internet or saved to portable media devices such as laptops or flash drives;
- Train employees on security procedures;
- Ensure vendors with access to the sensitive information are in compliance with the security requirements; and
- Assess the effectiveness of the WISP.

D. Latest Hacker Ploys & Cyber Security Scams

The sophistication of cyber criminals and terrorists has been increasing in both their technical expertise, as well as their utilization of computer software that is readily available to promote new generations of malware. This has resulted in substantial increases in the incidence of cyber-crime. In the report *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for*

Fraudsters[xiii], it was noted that the incidence of identity fraud increased in 2012 for the second consecutive year, affecting 5.26% of U.S. adults. Additionally, the report noted that:

- The number of identity fraud incidents increased by one million more consumers over the past year, and the dollar amount stolen increased to $21 billion. This equates to 1 incident of identity fraud every 3 seconds.
- Almost 1 in 4 consumers that received a data breach letter became a victim of identity fraud, which is the highest rate since 2010. This underscores the need for consumers to take all notifications seriously. The study found consumers who had their Social Security number compromised in a data breach were 5 times more likely to be a fraud victim than an average consumer.

With that said, the following sets forth a number of the most recent ploys and scams that are anticipated to turn up in the near future.

1. Phishing

a. Basic Tool in the Toolbox

As economic cyber-crime continues to surge, "Phishing" attacks continue to be one of the basic tools in the theft of personal data. Cyber-crime based on scams that use spam email to lure you into revealing your bank or brokerage account information, passwords or PINs, Social Security number or other types of confidential information continue to be the backbone of hackers continues to grow significantly.

In the interim, in a world where data mining is becoming common place as systems become more sophisticated, cyber criminals are also growing cleverer. For example it used to be that misspelled company names, poor English and jumbled Web URLs were a clear tip off to early phishing ploys. But now seemingly legitimate links can hijack users to a fraudulent site through technical code buried behind the message.

b. Browser Redirection

Cyber criminals have learned to modify a directory called a host file in Microsoft Windows that can turn your browser into vehicle for a phishing excursion - type in a Web address from your browser and you could be directed to a fraudulent site. In these messages the intruder impersonates a representative of a bank or payment system asking the victim to send personal data, or visit an “official” website. The user is invited to go through an authorization process on the forged website and data is stolen as soon as it is entered. The procedure takes a couple of seconds. After that, the victim is redirected to the legitimate web site that was mimicked by the phishers. As a result, the victim may not even be aware that has been on a malicious site and that his computer is now infected with a Trojan Horse. In the future, the malicious program could alter the bank’s original page to intercept any information entered by the victim, including credit card numbers, account number, PIN Numbers and or passwords.

c. Spear-Phishing Attacks

In spear-phishing attacks, cyber criminals target victims because of their involvement in an industry or organization they wish to compromise. Often, the e-mails contain accurate information about victims obtained via a previous intrusion or from data posted on social networking sites, blogs, or other websites. This information adds a veneer of legitimacy to the message, increasing the chances the victims will open the e-mail and respond as directed. Additionally, the communications can appears to be your boss or their boss's boss (the so-called spear-phishing variety because they are more pinpointed) … and it's not easy to ignore an email that shouts "Urgent: Immediate Action Required" and which purports to be from a higher-up.

Recent attacks have convinced victims that software or credentials they use to access specific websites needs to be updated. The e-mail contains a link for completing the update. If victims click the link, they are taken to a fraudulent website through which malware harvests details such as the victim's usernames and passwords, bank account details, credit card numbers, and other personal information. The criminals can also gain access to private networks and cause disruptions or steal intellectual property and trade secrets.

d. Hotel Internet Connections

Analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while they are establishing an Internet connection in their hotel rooms. Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to set up the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

e. Photo-Sharing Programs Compromise Computers

The FBI has recently reported that it has seen an increase in cyber criminals who use online photo-sharing programs to perpetrate scams and harm victims' computers. These criminals advertise vehicles online but will not provide pictures in the advertisement. They will send photos on request. Sometimes the photo is a single file sent as an e-mail attachment, and sometimes the victim receives a link to an online photo gallery. The photos can and often contain malicious software that infects the victim's computer, directing the user to fake websites that look nearly identical to the real sites where the original advertisement was seen. The cyber criminals run all aspects of these fake websites, including "tech support" or "live chat support" and any "recommended" escrow services. After the victim agrees to purchase the item and makes the payment, the criminals stop responding to correspondence and the victims never receive any merchandise. Regardless of whether the item is ultimately purchased, it is clear that malware can deliver Trojans to your computer even through the download of a photo or picture.

2. Account Takeover

a. Corporate Account Takeover

Corporate Account Takeover is a form of corporate identity theft where a business' online credentials are stolen by malware. This form of identity theft has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses, and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. To obtain access to financial accounts, cyber criminals target employees - often senior executives or accounting, and HR personnel and or business partners. But any employee is vulnerable to being targeted, and then through phishing or other techniques, malware is installed on their computer, which in turn steals their personal information and log-in credentials. Once the account is compromised, the cybercriminal is able to electronically steal money from business accounts. Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information - often through the spread of malware - that can also cause indirect losses and reputational damage to a business.[xiv]

b. Personal Account Takeover

As with corporate account takeover, the personal identity theft is where an individual's credit cards and or online credentials are stolen by malware. The cybercriminal either illegally charges on the cards, and or gains access to the individuals' accounts of the victim, then steal assets from the account. In many cases the theft is implemented by selling all the positions in the account and wiring the proceeds to another financial account. Historically, the account may have been a third party account. Today, the sophisticated cybercriminal is more likely to open and "spoof" accounts that appear to be owned by the victim, thus making discovery of the crime more difficult.

3. Malware for Mobile Devices

Mobile smart devices are still a relatively new phenomenon. As such, smartphone and smart-pad users have enjoyed a distinctly safe existence from malware. This is because those who create viruses, Trojan Horses, and other malicious programs have tended to focus their efforts where they are most likely to succeed. For a long time that meant only creating malware for desktop and laptop computer systems. However, with mobile devices beginning to outsell conventional computers, cyber criminals are beginning to take notice. According to a report

released by McAfee Labs, mobile malware more than doubled last year, with 17,000 new mobile-device specific malware forms having been identified.

A common way is via software downloaded outside official app stores, but there have also been instances of malware spreading via infected web or in-app ads and web and emailed links, as well as instances of apps creeping onto official stores - mostly on Android.

Among the most common type of malware is tollware, where the app surreptitiously sends texts to or silently dials into a premium rate service. Another common type of malware collects information on the user - the likes of contacts etc. - that it doesn't have permission to access - often for use in sending out spam. Additionally, malware writers have also started exploiting different aspects of mobile phones, developing apps that secretly record telephone conversations and intercept text messages used to authenticate user identity in online banking.

4. Cybercriminals Target Social Media Accounts

In a recent article published by McAfee, it was noted that social platform attacks are targeting websites with large user bases, such as Facebook, LinkedIn, Twitter, and Instagram. A majority of current attacks simply use the social platforms as access to a user's contacts, location, and even business activities. While this information does not directly profit the cyber criminals, it does make it possible to send Trojan Horses, malware and malicious messages from the victim's accounts. This information can then be used to steal the identity of friends, family and business associates of the user.[xv]

Most often, social platform attacks are able to breach users' accounts by stealing their authentication credentials upon login. This information is then used to discreetly pull personal data from users' online friends and colleagues. A recent study stated that 22% of social media users have fallen victim to a security-related incident, and recent documented attacks support the numbers. Facebook, Google, Yahoo, and other social media users, had more than two million user passwords stolen. Facebook estimates that anywhere from 50-100 million of its monthly active user accounts are fake duplicates, and as many as 14 million of those are "undesirable" on the site.

Another social media attack that is expected to take a stronghold of user information in 2014 is the "false flag" attack that tricks a user into revealing personal information or authentication credentials under the guise of the site itself. Upon changing the password, the attacker will steal the username and password information to then steal personal information about the user. Users should remain alert to any "urgent" request from the site to reset a password.

5. Ransomware

Ransomware has been around for a number of years, but in recent months it has been on the upswing, in part due to the over-the-counter market where ransomware can be purchased. The FBI has issued a number of E-Mail Warnings[xvi] regarding the ransomware program called CryptoLocker the Citadel malware platform used to deliver ransomware known as Reveton.

a. Business to Business - Customer Complaints

With respect to the CryptoLocker ransomware, businesses are receiving e-mails with alleged customer complaints containing an attachment that when opened, appears as

a window and is in fact a malware downloader. This downloader then downloads and installs the actual CryptoLocker malware. The verbiage in the window states that important files have been encrypted using a unique public key generated for the computer. To decrypt the files, you need to obtain the private key. A copy of the private key is located on a remote server that will destroy the key after the specified time shown in the window. The attackers demand a ransom of $300 to be paid in order to decrypt the files.

Unfortunately, once the encryption of the files is complete, decryption is not feasible. To obtain the file specific Advanced Encryption Standard (AES) key to decrypt a file, you need the private RSA key (an algorithm for public key cryptography) corresponding to the RSA public key generated for the victim's system by the command and control server. However, this key never leaves the command and control server, putting it out of reach of everyone except the attacker. The recommended solution is to scrub your hard drive and restore encrypted files from a backup.

In the 2014 Report on Cyber Security issued by the University of Kent in the UK has revealed that "around 40% of people who fall victim to an advanced form of malware, known as CryptoLocker, have agreed to pay a ransom of around £300 to recover their files. xvii Their research also reveals that the prevalence of this type of ransomware (or malware) which makes personal files inaccessible by encrypting them - equates to approximately one case in 30, much higher than previous estimates suggested."

b. Department of Homeland Security

Cyber criminals are currently utilizing alleged communications from the Department of Homeland Security (DHS) to extort money from unsuspecting victims in another ransomware campaign. The e-mails direct the victims to a download website, at which time it is installed on their computers.

The ransomware is used to intimidate victims into paying a fine to "unlock" their computers. The ransomware has been called "FBI Ransomware" because it frequently uses the FBI's name, but similar ransomware campaigns have used the names of other law enforcement agencies such as DHS. As in other variations, the ransomware using the name of DHS produces a warning that accuses victims of violating various U.S. laws and locks their computers. To unlock their computers and avoid legal issues, victims are told they must pay a $300 fine via a prepaid money card. This is not a legitimate communication from law enforcement, but rather is an attempt to extort money from the victim.

6. Point of Sales Attacks

In December 2013, we heard of a series of point-of-sale (POS) attacks on multiple retail chains across the United States, including Target (which has been ranked among the largest data-loss incidents of all time with up to 110 million transaction records being stolen), Neiman Marcus, White Lodging, Harbor Freight Tools, Easton-Bell Sports, Michaels Stores, and Wichcraft. In the McAfee Labs Threats Report Fourth Quarter 2013, it was noted that while the breaches were unprecedented in numbers of records stolen, what is even more notable is how well the malware industry served its customers.[xviii] Apparently, the attackers purchased off-the-shelf point-of-sale

malware, then made straightforward modifications so they could target their attacks, and it's likely that they both tested their targets' defenses and evaded those defenses using purchased software. They even had a ready and efficient black market for selling the stolen credit card information, including an anonymous, virtual-currency-based point-of-sale payment system. As McAfee observed in its report, "raw materials, manufacturing, marketplace, transactional support - it's all there for thieves to use."

7. Cloud-Based Corporate Applications

Data is the currency of the virtual world and with more and more data being stored in the cloud, further deployment of cloud-based corporate applications will create new attack opportunities for cybercriminals. The issue for corporate security experts is that when a corporate application moves to the cloud, the organization loses visibility and control over the security profile. This puts tremendous pressure on ensuring that the cloud provider's user agreement clearly states that proper security measures are in place and are constantly upgraded to combat evolving security threats and performing quality due diligence to the service provider.[xix]

E. Protecting Client Information

1. Regulation S-ID Identity Theft Red Flags

All broker-dealers and investment advisors are required to develop an Identity Theft Prevention Program ("Program") for all "covered accounts" in response to implementation of the Regulation S-ID Identity Theft Red Flags Rules. The Program and the underlying procedures implemented should be designed, developed and implemented to identify, detect, mitigate and respond to patterns, practices or specific activities that could indicate identity theft in connection with the opening of covered accounts or any existing covered account.

a. "Covered accounts" Pursuant to Regulation S-ID include:

i. Family and Household Accounts

Accounts maintained primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions such as brokerage accounts that permit wire transfers or other payments to third parties.

ii. Any Account With Foreseeable Risk of Identity Theft

Any other account, including a business account or institutional account that poses a reasonably foreseeable risk to clients or to the safety/soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

b. Red Flags That Could Suggest Identity Theft Has Occurred.

All activity involving covered accounts should be monitored, including the account opening process, conduct of business with the client, and closure of the account, to help prevent identity theft. A key element of such monitoring is a requirement that all

employees be vigilant for "red flags" identified below that might suggest a concern regarding possible identity theft:

i. Notifications and Alerts When a Consumer Reporting Agency is Utilized

Red flags may arise in connection with notifications or alerts from consumer reporting agencies which may include:

- A fraud or active duty alert is included with a consumer report;
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
- A consumer reporting agency provides a notice of address discrepancy;
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    - A recent and significant increase in the volume of inquiries,
    - An unusual number of recently established credit relationships,
    - A material change in the use of credit, especially with respect to recently established credit relationships,
    - An account that was closed for cause or identified for abuse of account privileges by the company;

Should the company receive a notice of address discrepancy, notification or alert from a consumer reporting agency the company must form a reasonable belief that it is the correct consumer report. Notices of discrepancy will be forwarded to the Chief Compliance Officer or his/her designee for investigation. The Chief Compliance Officer or his/her designee will contact the customer regarding the report or use alternative documentation to verify the information provided. Alternative information sources might be:

- Information obtained and used to verify the identity in accordance with the company's Customer Identification Plan;
- Requesting the customer to provide additional address verification; evidence such as a recent utility bill, bank account statement, etc.;
- Information maintained in the company's records, such as address change notifications, applications, new account documentation; or
- Information obtained from other third party vendors.

ii. Red Flags Arising From Suspicious Client Documentation

Red flags may arise in connection with the account opening process, or during other situations in which a client may be required to present documents such as those that contain photographs, physical descriptions, signatures, etc. Such red flags could include:

- Documents provided for identification appear to have been altered or forged;
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check; or
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

iii. Red Flags Arising From Client's Personal Identifying Information

Red flags may arise in connection with the account opening process, or during other situations in which a client may be required to present personal identifying information, such as social security numbers, phone numbers, address information, etc. Such red flags could potentially include:

- Personal identifying information provided is inconsistent when compared against external information sources used by the company. For example:
  - The address does not match any address in the consumer report
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File;
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth;

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the company. For example:
    - The address on an application is the same as the address provided on a fraudulent application,
    - The phone number on an application is the same as the number provided on a fraudulent application;
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the company. For example:
    - The address on an application is fictitious, a mail drop, or a prison,
    - The phone number is invalid, or is associated with a pager or answering service;
- The SSN provided is the same as that submitted by other persons opening an account or other customers;
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
- Personal identifying information provided is not consistent with personal identifying information that is on file with the company;
- If the company uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

iv. Red Flags Arising From Suspicious Activity Related to the Covered Account

Red flags may arise in connection with activity that takes place in a client's account. Such red flags could potentially include:

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - Nonpayment when there is no history of late or missed payments
    - A material increase in the use of available credit
    - A material change in purchasing or spending patterns
    - A material change in electronic fund transfer patterns in connection with a deposit account
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

v. Red Flags Arising From Direct Notice to a Firm

Red flags may arise in connection with direct notice given to the Firm regarding possible compromising of the account. Such notice may come from any credible source, including the client, law enforcement agencies, regulatory bodies, etc. Such red flags could potentially include:

- The company is notified that the customer is not receiving paper account statements.
- The company is notified of unauthorized charges or transactions in connection with a customer's covered account.
- The company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft

vi. Red Flags Arising From Any Other Source

Red flags may arise from any of a wide variety of other sources, often in ways that might be uniquely based on the nature of the business engaged in with a client, or based on how a firm communicates with a client. The employees of firms should be aware and vigilant to any red flags that might be similar to those listed above that might reveal the possibility that an identity theft may have occurred.

c. Ongoing Review and Update of Policy

The company will periodically review and determine whether it is necessary to update the Identity Theft Prevention Program policy and procedures when there are

changes periodically, to reflect changes in risks to customers or to the safety and soundness of the company from identity theft, based on factors such as:

- Experiences of the company with identity theft;
- Changes in the method of identity theft;
- Changes in the methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that the company offers; or
- Changes in the business arrangements of the company such as merger, acquisition, alliance, joint venture and service provider arrangements.

F. Best Practices for Data Protection

Most firms in the financial industry have already begun implementing procedures and processes as a result of the implementation of Regulation SP and Regulation SP-ID. However, as technology evolves and hackers become more sophisticated, it is critical to review the processes utilized for the protection of personal information. The CFTC guidelines and the state of Massachusetts privacy statutes have a lot in common, and they provide guidance for firms wanting to take a pro-active approach to cybersecurity. The following represents a summary list of the best practices that should be considered in light of the onslaught of cybercrime,

1. Understand Information Handling Processes

a. Review and Inventory Current Process

Review and inventory your current processes for collecting, retaining and using personal information. Understand the amount of personal information collected, the form it is retained in(hard copy versus electronic), the length of time it is retained, who in the organization has access to it, and how is it disposed of after it is no longer needed.

b. Limit the Amount of Personal Info Collected

Examine the personal information collected. It is a good business practice to limit the collection of personal information to only that information which you absolutely need.

c. Retain Information Only as Long as Necessary

Implement a record retention policy and maintain personal information records only as long as needed and or required pursuant to the record retention rules.

2. Designate a Data Security Coordinator

Firms should designate one or more persons as an information security coordinator and they should be charged with maintaining the information security plan. The coordinator(s) would answer to senior management and the responsibilities of the coordinator(s) should include:

- Initial implementation of the plan

- Initial training of employees including temporary and contract employees (annually thereafter)
- Regular testing of the plan's safeguards
- Annual review of the scope of the plan or whenever there is a material change in business practices that may affect the security or integrity of records containing personal information
- Evaluation of the ability of third party service providers to comply with your privacy and record destruction policies.

3. Access to Personal Information Access

a. Keep It Under Lock & Key

All hard copy records containing personal information should be stored in locked facilities when not being used. This includes removing personal information from your desk in the evening, and maintaining screen savers on your computer for when you leave your computer.

b. Restrict Access to Personal Information

Access to records containing personal information, whether in hardcopy or electronic format, should be limited to only those persons who require it in order to perform their job function.

c. Establish Policies for Off-Site Use of Personal Information

Develop security policies for employees relating to the storage, access and transportation of records containing personal information outside of your business premises.

d. Guard Against External Threats

Up-to-date security tools, firewall protection, malware protection, antivirus definitions and operating system security patches should be in place for all systems processing personal information.

e. Visitor Procedures — Tighten Up Access to Your Facilities.

Depending on the size and layout of your facilities, it may be prudent to restrict visitor access to one entry point for each building in which personal information is stored. Additionally, it's always a good policy to require visitors to be escorted in all areas of the facility where personal information is stored. Finally, personal information should not be left in plain view while unattended.

4. Computer Security Requirements – "Reasonable Means"

You should use "reasonable means" through technology to protect personal data. The following represent a few of the technically feasible alternatives available to most firms in the financial industry:

a. Secure User Authentication Protocol

These protocols include control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords; control of password security; restricting access to active users; and blocking access after multiple attempts.

b. Secure Access Control Measures

These measures must include restricting access to records and files containing personal information to those who "need to know" to perform their jobs as well as assigning unique IDs and passwords (not shared nor vendor supplied default passwords).

c. Monitoring for Unauthorized Use or Unauthorized Access

Reasonable monitoring of systems for unauthorized use of or access to personal information should be implemented. There are a variety of methods and tools available in order to effectively monitor and protect against unauthorized activity, intrusion detection tools, application logs, server firewalls, network security logs and file system auditing, to name a few.

d. Firewall Protection and OS Patches

For files containing personal information on a system that is connected to the Internet, you must implement and maintain "reasonably up-to-date" firewall protection and operating system security patches.

e. Viruses and Malware

You must implement and maintain up-to-date versions of system security agent software that includes malware protection and "reasonably up-to-date" patches and virus definitions. Additionally, you must be set up to receive the most current security updates on a regular basis.

5. Encryption

Benjamin T. Wilson JD, CISSP, a writer for EzineArticles.com stated that "Encrypted data does not usually give rise to claims of data breach. Most often, data is stolen when it is unencrypted and transmitted in clear text - not when it is protected by encryption." With that in mind, laptops, portable devices, backup tapes, email and public network and wireless transmissions containing personal information should require encryption.

a. Encrypt Transmitted Records Containing Personal Information

If it is technically feasible to do so, outgoing emails containing personal information, as well as any personal information traveling across public networks or transmitted wirelessly, should be encrypted. If it is not technically feasible to encrypt, implement best practices by not sending unencrypted personal information in an email (for example, redacting social security numbers and or account numbers from unencrypted e-mail communications).

b. Encrypt Portable Devices Containing Personal Information

Not all portable devices need to be encrypted. Only those portable devices that contain personal information should be encrypted if it is technically feasible. For example, at this point in the development of encryption technology, there is little, if any, accepted encryption technology for most portable devices (cell phones, Blackberries, IPhones, Netbooks, etc.). Since it may not be possible to encrypt portable devices, personal information should not be maintained on such devices.

c. Web Site

To the extent your company or third party web portals have user access in which personal information is entered, those sites should be verified as being secure.

6. Third Party Service Providers

a. Third Party Service Providers' Due Diligence

Most firms buy much of their information technology and services from third party suppliers. Therefore, these suppliers' vulnerabilities become the vulnerabilities of the firms for whom they provide products and services. You need to confirm that any third party service provider with access to personal information is capable of maintaining appropriate safeguards to protect personal information. This includes any vendors who handle personal information on your behalf (e.g., background check services, payroll services, life and health insurance providers, 401K administrator services, credit card processing firms, etc.). Ultimately, a third party service provider with access to personal information has to have as good or better data retention than the company.

b. Third Party Service Providers Should Be Contractually Obligated to Implement and Maintain Appropriate Security Measure

You should require all third party service providers with access to personal information to enter into written contracts requiring them to implement and maintain appropriate measures for protecting and destroying personal information that is maintained on your behalf.

7. BYOD

As the bring-your-own-device (BYOD) trend continues to gain momentum in the workplace, businesses of all sizes continue to see information security risks increased, and being exploited. These risks stem from both internal and external threats including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable business applications. As a result, firms utilizing the BYOD platform should have a BYOD program in place to address the accidental disclosures due to loss of boundary between work and personal data and more business information being held in unprotected manner on consumer devices.

To minimize these risks, employers may want to consider implementing BYOD policies. Those policies should take into account a number of the issues, including the following:

- Firms should determine what smart phones and tablets employees are using, and make a determination of which devices are supported;
- Firms should require strong passwords, not just a simple 4-digit pin;
- Firms should communicate that the company owns the information stored on its servers that the employees access through their devices and can wipe (delete) the information stored on the device in the event it is lost or stolen because that information contains confidential business information owned by the organization; and
- When an employee separates from an organization with his/her personal device, the firm could be vulnerable and risk losing its confidential business information. A thorough BYOD policy will likely address this by making it mandatory that the employer will wipe (delete) any company-stored information on the personal device at the time of the employee's departure. Because many employees have personal information such as photographs or music or other purchased applications, employers should consider developing a protocol to protect the employee's personal information while still removing the company data.

8. Employee Issues

a. Train Employees on an Ongoing Basis

Cloud, social and mobile technologies, including "Bring Your Own Device" (BYOD), are simply too cost efficient and effective for companies to ignore them. However, these technology trends will require they embrace the fact that the corporate network now has extended beyond the immediate control of IT. This has resulted in companies having to better control how corporate and personal data travels, and ensuring the education of their employees on the responsibilities they have in securing such data.

In light of the regulatory obligations and best practice considerations, employees (including full time, part-time, temporary and contract employees) should be trained on an ongoing basis on the proper use of computer security systems, the importance of personal information security and on identity theft prevention. Employees are on the front line of handling and processing personal information and it is critical that they receive on-going training as this area of cyber-crime evolves.

This training can be incorporated easily into the firm-element continuing education plan and or the annual compliance meeting. In general, a good starting point for resources that can be utilized for training and education would be the (i) Microsoft web-site on Phishing http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx; (ii) the MS-ISAC web-site, which is located at http://msisac.cisecurity.org. MS-ISAC provides for information sharing between governmental entities and various corporate partners. It transitioned into a not-for-profit status under the auspices of the Center for Internet Security in 2010 and is designated by the U.S. Department of Homeland Security as the ISAC for state, local, tribal and territorial governmental entities; and or (iii) The IC3 web-site, which is located at http://www.ic3.gov/about/default.aspx. IC3 was established as a partnership

between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate.

b. Prevent Terminated Employees from Accessing Personal Information

You should have measures in place to prevent terminated employees from accessing records containing personal information. It is good practice to immediately terminate their physical and electronic access to such records, including deactivating their passwords and user names.

9. Ongoing Monitoring

Companies should conduct regular reviews of their information security policies for relevancy and operational effectiveness as well as regular reviews of organizational adherence to the established operational protocols. As a best practice, these reviews should be conducted on an annual basis at a minimum, or whenever there is a material change in business practices that may affect the security or integrity of records containing personal information.

10. Customer Education

As important as employee training is, it is also important to provide your customers with educational materials regarding cyber security. By increasing their awareness of the issues your customers will be better able to protect themselves, which also protects the firm. The FINRA Investor web-site is a good starting point for resources that can be utilized for customer education, and it is available here. A few of the articles that could be helpful would include:

- Well-Traveled Fraud—Advance-Fee Scams Target Non-U.S. Investors Using Fake Regulator Websites and False Broker Identities; [xx]
- "Phishing" and Other Online Identity Theft Scams: Don't Take the Bait;[xxi]
- Inbox Alert—Don't Trade on Pump-And-Dump Stock Emails;[xxii] and
- Email Hack Attack? Be Sure to Notify Brokerage Firms and Other Financial Institutions.[xxiii].

11. Insurnace

In light of the risks associated with breaches in cybersecurity, companies should review their insurance policies to determine if additional coverage and or riders are appropriate to address data breaches and or identity theft.

G. 2014 Cyber Regulatory Gotcha's

While it is important to discuss the best practices as they drive the future and help us set goals, in wrapping up a discussion of data protection for the average financial firm it is important to look at the regulatory gotcha's. The following items represent practices that, based on readily

available and commercially reasonable technology, will in all likelihood result in regulatory action against the firm in the event of a breach of their cyber security:

1. Account Takeover

Failure to confirm the customers' identity with respect to wire instructions. A significant number of FINRA enforcement actions and or investigations relate to unauthorized wires that were commenced by e-mail or fax instructions, and the identity was not confirmed.

2. Encryption

The failure to use an encryption platform for the mailing or e-mailing of customer or employee information such as account numbers and or social security numbers that have not been redacted.

3. Password Protection

The failure to use password protection on devices that contain customer information such as laptops, computers, tablets and cellular phones.

4. Failure to Protect Data

The failure to protect customers' personal data while your desk is left unattended. This relates to both hard copies of data left unattended on the desk, and data available on computer screens while no one is at the computer.

5. Virus Detection Software

The failure to utilize current virus detection software, and the breach is tied malware that would have been detected normal course.

H. Business Continuity Plan

1. Targeted Examination Letter – and Sweep Exam

In November 2012, FINRA issued a Targeted Examination Letter[xxiv], in coordination with the Securities and Exchange Commission ("SEC"), and the Commodity Futures Trading Commission ("CFTC"). At that time FINRA advised membership that it would be conducting a review of the impact of Hurricane Sandy on firms' operations and their ability to conduct business at a time when business continuity plans were enacted. As a result of that joint review, FINRA, the SEC and CFTC issued a Business Continuity Planning Advisory (FINRA Notice to Members 13-25[xxv]).

The advisory represents the first major guidance issued by FINRA, the SEC and or the CFTC since BCPs were mandated by the SEC for investment advisers and broker-dealers (FINRA Rule 4370, formerly NASD Rule 3500 series for broker-dealers). It is anticipated that the guidance will have a significant impact on the BCPs for broker-dealers and financial advisers as the compliance bar gets raised. The advisory compiles a summary of what the regulators learned in their BCP examinations; and encourages firms to review their BCPs to implement best practices to improve response time to, and reduction of recovery time after, significant large-scale events.

2. Best Practice Considerations

While it was noted that the impact of a business disruption is going to be based upon the severity of the disruption, it also noted that BCPs need to take into account the firm's location, size, type of business and need for contact with customers and regulators. Best practice considerations include the following:

- the lack of communications, transportation, office space, fuel and water;
- the possible need to use an alternative location in a separate geographic region;
- critical vendor relationships and the vendor's ability to perform crucial services in light of the disruption;
- the use of multiple communications vendors;
- communication plans with customers, clearing firms, regulators and other third parties;
- regulatory and compliance reporting; and
- an annual review and testing of the BCPs.

3. Other Lessons Learned and Sweep Exam Conclusions

In preparation of a significant business disruption, both broker-dealers and investment advisers should consider reviewing their current BCPs, as applicable, to determine if they are compliant with the best practices set forth in the advisory. Click the following for a pro-forma worksheet titled "*2014 Business Continuity Plan Update Worksheet*", which was prepared to assist financial firms in making an assessment as to whether their BCP may need to be modified to address the best practices noted in the advisory. In addition, a number of those best practices that should be addressed in the BCPs include the following items:

- To the extent that a firm is located in an area where widespread disruptions are likely to occur, the BCPs should address lack of communications, transportation and electricity.
- Whether employees will be able to travel to the office, or an alternate work location or if they have the ability to work from home.
- The utilization of alternate locations that are geographically separated from the primary office, and what key personnel will be relocated to the site. Consideration should be given to housing and transportation for personnel and the amount of space needed, computers, additional phone lines, generators and internet.
- The BCPs should address categorizing vendors and third party service providers (low-risk, high-risk, etc.) and evaluate the risk in BCP plans.
- Address whether a firm's critical vendors have business continuity plans to ascertain that the vendor utilizes alternate locations, back-up systems (and the capacity of the back-up system), the amount of time the vendor expects to be out

of service during a significant business disruption and the amount of time it will take them to commence service.

- Redundant services for telephone and internet, and if staff members are permitted to work remotely, the availability of telephone and, internet services for those locations.
- Have BCPs been made available to customers, and employees, as well as counterparties and third party vendors, including up to date information on the web site.
- Contact information for the various regulatory authorities as well as for the designated principal to contact the appropriate regulators if the firm has to implement its BCP.
- Annual testing of BCPs to ensure that the plan is practical, and that it actually functions as designed and is in compliance with regulatory requirements, communication changes, vendor changes and personnel changes.

I. CONCLUSION

Cybersecurity, identity theft red flags and business continuity are all critical issues that the financial industry currently faces, and as such 2014 may well be another difficult year implementation of new guidelines and potential rulemaking from both the SEC and FINRA. As the standard of care is being raised for the handling of private information and resumption of business activities following a business disruption it is becoming more important to actively face the related challenges directly. Ultimately, a firm that is subject to a breach of its cybersecurity, customer identity protection and or faces a business disruption, will be judged in hindsight, and as such, it is critical to have implemented a reasonable, risk based procedures and processes to address these matters.

J. HANDOUTS / RESOURCES

Please click the hyperlinks for:

- FINRA Firm Checklist for Compromised Accounts
- Safeguarding Your Financial Information: An Identity Theft Prevention Checklist
- 2014 Business Continuity Plan Update Worksheet

For a copy of the respective document in word and or excel format, please contact Daniel LeGaye, at dan.legaye@legayelaw.com.

K. END NOTES

[i] Full text of the public statement of SEC Commissioner Luis A. Aguilar given at the SEC Roundtable on Cybersecurity on March 26, 2014 is available here.

[ii] Cybersecurity a Top Priority, available here.

[iii] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, *Version* 1.0 (Feb. 12, 2014), available here.

[iv] Exec. Order, Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), available here ("Executive Order").

[v] SIFMA Statement on NIST Cybersecurity Framework, available here.

[vi] Information Weekly; NIST Cybersecurity Framework: Don't underestimate, available here.

[vii] Webinar of the SEC Cybersecurity Roundtable is available here.

[viii] Division of Corporation Finance, SEC, CF Disclosure Guidance: Topic No. 2, available here.

[ix] 2014 FINRA Regulatory and Examination Priorities Letter is available here.

[x] FINRA - Targeted Examination Letters, Cybersecurity is available here.

[xi] CFTC Staff Advisory No. 14-21, available here.

[xii] Massachusetts Standards for the Protection of Personal Information (201-CMR-17.00), available here.

[xiii] 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available here.

[xiv] Fraud Advisory for Businesses: Corporate Account Take Over, prepared through a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), available here.

[xv] How Cybercriminals Target Social Media Accounts, available here.

[xvi] FBI E-mails Warnings, available here.

[xvii] 2014 Report on Cyber Security, issued by University of Kent, available here

[xviii] McAfee Labs Threats Report Fourth Quarter 2013, available here.

[xix] Top Cyber Threats for 2014, available here.

[xx] Well-Traveled Fraud—Advance-Fee Scams Target Non-U.S. Investors Using Fake Regulator Websites and False Broker Identities; available here.

[xxi] "Phishing" and Other Online Identity Theft Scams: Don't Take the Bait; available here.

[xxii] Inbox Alert—Don't Trade on Pump-And-Dump Stock Emails, available here.

[xxiii] Email Hack Attack? Be Sure to Notify Brokerage Firms and Other Financial Institutions is available here.

[xxiv] Targeted Examination Letters – Business Continuity Plans, resource attached here.

[xxv] FINRA Notice to Members 13-25, resource attached here.