Data Privacy and Protection

mimic TECHNOLOGIES

Proven RIA Technology Solutions

CONTAINED WITHIN

Regulators demand that firms have in place procedures and programs designed to protect clients' nonpublic personal information.

Data Privacy and Protection

It is a subject that is taken very seriously by regulators and your clients alike, and for good reason. Regulators demand that firms have in place procedures and programs designed to protect clients' nonpublic personal information (NPI). Your clients expect nothing less than 100% safety of their private information housed at your firm. There are many laws and regulations on the books regarding data privacy, and the penalties for data breaches can impact your firm monetarily and significantly impact your reputation in the eyes of the investing public. Any way you look at it, a data breach can potentially put your firm out of business. Thankfully, there are tools available that can assist in compliance and help ensure the safety of your client's data.

Executive Summary

Firms need to be aware that customer information and records can be compromised in a number of different ways, especially in this day and age of web-based access to trading platforms and records. Firms must understand and address the potential risks of network and system intrusions. Since these types of security breaches can raise both investor protection and market integrity concerns, it is of the utmost importance that firms protect customer information and assets.

The regulatory environment that firms have to work within has become increasingly more challenging over the past several years and there are no indications that the pressure will subside any time soon. Quite the contrary, it is only going to get more difficult. In this white paper we will concern ourselves with some of the regulations that specifically address data privacy. Of course; the material contained below is not intended as a single source of information nor is it a one-stop solution for implementing compliance or data security strategies. Rather, the paper serves to provide an overview of regulations and to illustrate how Mimic Technologies can help your firm meet regulatory compliance by providing you with the services, expertise, and information that you need to be able to manage these risks.

Regulatory Landscape – What Rules are in Place Regarding Data Privacy?

Data Privacy rules are not new. The Gramm-Leach-Bliley Act (GLBA) was initiated more than 13 years ago. That being said, regulators frequently find compliance deficiencies stemming from customer complaints or during routine examinations. There still appears to be confusion over what is needed in order to comply with data privacy rules and how to properly protect client nonpublic personal information.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, was passed Nov. 12, 1999 and requires financial institutions to provide each client with a privacy notice at the time a relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used and how that information is protected.

Secondly, and perhaps more importantly for our discussions, the Safeguards Rule requires financial institutions to develop a written information security policy that describes how the company is prepared to protect clients' nonpublic personal information. Like other laws, this rule is intended to do what most businesses should already be doing: protecting their clients.

Let's look at two sections of GLBA in more detail - the Safeguards Rule and Pretexting.

The Safeguards Rule requires financial institutions to develop a written information security policy that describes how the company is prepared for, and how they plan to continue to protect clients' nonpublic personal information. The Safeguards Rule applies to information of any consumers, past or present, of the financial institution's products or services. This plan requires institutions to:

- List at least one employee to manage the safeguards.
- Construct a thorough risk analysis of each department handling the nonpublic information.
- Develop, monitor, and test a program to secure the information, and
- Change the safeguards as needed with the changes in how information is collected, stored, and used.

➢ More information pertaining to the GLBA can be found at: *http://www.sec.gov/rules/final/34-42974.htm*

The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to perform a risk analysis on their current processes.

Pretexting (or "Social Engineering") occurs when someone tries to gain access to nonpublic personal information without proper authority to do so. This could be through requesting private information while impersonating the account holder, via phone, mail, email, or even by 'phishing' (i.e., using electronic communication to masquerade as a trustworthy entity while attempting to obtain protected information or deliver malicious software). The Pretexting Protection section of GLBA encourages organizations to implement safeguards against pretexting. These include having a well-written security policy designed to develop, monitor, and test a program to secure the information. It would likely include a section on training employees to recognize and deflect inquiries made under pretext.

Time and time again we see firms that, due to inadequate safeguards and training, allow a customer's nonpublic personal information to be compromised by an imposter pretending to be the customer via email or other electronic communications. Not only does this cost the firm money, it can expose them to intense regulatory scrutiny and do irreparable damage to the firm's reputation, thus leading to a loss of clients. See Sidebar for a real world case study.

Regulation S-P

Another regulation about which advisors need to be aware is Regulation S-P. The Privacy of Consumer Financial Information, otherwise known as Regulation S-P (Reg. S-P, for short), has been adopted by the SEC in accordance with Section 504 of the GLBA. Under the SEC's Regulation S-P, firms are required to have policies and procedures addressing the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information and against unauthorized access to or use of customer records or information. Regulation S-P mandates that firms:

- Maintain written records designating an employee (or employees) to be responsible for the oversight and coordination of the program
- Require the coordinator to be responsible for identifying foreseeable security risks, and to design policies and measures to prevent those risks
- Perform regular testing and monitoring of the effectiveness of the safeguards

REAL WORLD CASE STUDY

FINRA sanction 6/17/13

A registered representative in West Bloomfield, Michigan submitted a Letter of Acceptance, Waiver and Consent in which she was fined $5,000 and suspended from association with any FINRA member in any capacity for 30 days.

Without admitting or denying the findings, the representative consented to the described sanctions and to the entry of findings that she affected wire transfers totaling $13,400 from a firm customer's account to an unrelated third-party account after receiving fraudulent emails from someone purporting to be the customer. She received emails from a hacker purporting to be the customer who requested the customer's account balance and then sent fully executed letters of authorization (LOAs) that fraudulently authorized wire transfers to an account at a third party bank. The findings stated that the representative did not authenticate the customer's signature contrary to firm policies and procedures, which required registered representatives and associated persons to speak to the customer prior to affecting a transfer of funds to an outside account. She processed the transfers and falsely indicated on the firm's internal system that she spoke with the customer and verified the customer's identity. The findings also stated that after the customer discovered the improper wire transfers on her account, she contacted the representative. While the representative and the customer were discussing the fraudulent wire transfers, the representative received another request from the hacker, requesting a third transfer of $7,350. The hacker attached an executed fraudulent LOA to the request. The representative did not respond to the request and contacted her firm's office management team and advised them of the previous transfers. The firm credited the customer's account for the full amount of the transfers. The findings also included that the representative caused her firm to maintain false books and records related to the wire transfers.

- Train staff on the key elements of the security program and how to implement the program
- Oversee service providers to the firm and assess their safeguards regarding privacy of customer information and monitoring

➢ The full text of Reg. S-P can be found at: *http://www.sec.gov/rules/final/34-42974.htm*

Furthermore, Reg. S-P requires that firms properly dispose of customer nonpublic personal information by taking reasonable steps to protect against the unauthorized access or use of the information in connection with its disposal.

Failure to comply with GLBA, Reg. S-P, and other data privacy rules may result in serious penalties not limited to:

- Civil penalties of $100,00 or more
- Jail time of up to 5 years
- Regulatory enforcement actions including censure, cease and desist orders, and written agreements with regulators

Failure to comply with GLBA, Reg. S-P, and other data privacy rules may result in serious penalties not limited to:

***Civil penalties** of $100,00 or more*

***Jail time** of up to 5 years*

*Regulatory enforcement actions including **censure**, cease and desist orders, and written agreements with regulators*

Other Noteworthy Regulations

GLBA and Regulation S-P are not the only regulations about which firms need to be aware. Below we have listed some other regulations that deal with, either directly or indirectly, data privacy. Please keep in mind that depending on the size and structure of your firm, these regulations may not impact you currently. However, since the laws and regulations in place now may be amended in the future or used as the basis of a new regulation, it is best to at least be aware of what they are.

Dodd–Frank Wall Street Reform and Consumer Protection Act

Signed into law in July 2010, Dodd–Frank ushered in the most significant changes to financial regulation in the United States since the Great Depression. Aimed at restoring responsibility and accountability to the U.S. financial system, Dodd-Frank affects all federal financial regulatory agencies and almost every facet of the nation's financial services industry. It requires improved consumer protection; an end to government bailouts for large financial firms; creation of a council to identify systemic risks; elimination of loopholes for risky practices; new rules for rating credit; and the ability for regulators to expand their pursuit of financial fraud.

Clients expect nothing less than 100% safety of their private information housed at your firm.

Sarbanes-Oxley Act (SOX)

Section 404 of SOX mandates that publicly traded companies implement and maintain internal controls for the protection of corporate financial information, and for the timely detection of unauthorized access, insider abuse and unauthorized sharing of the information. Organizations found in noncompliance will be subject to substantial fines and significant jail time. The rules mandate this for publicly traded companies, though it is a good idea for companies of all sizes. While SOX does not seem to directly deal with data privacy or information security, without sound information systems that store all the vital data of any and all financial firms, a firm would not be able to comply with this act.

Payment Card Industry Data Security Standard (PCI DSS)

Introduced by the Payment Card Industry Security Standards Council in December 2004, this set of security best practices specifies technical and operational requirements to help organizations that process card payments prevent credit card fraud, hacking, and security vulnerabilities and threats.

PCI DSS mandates 12 steps that organizations must take to safeguard credit card data, such as installing firewalls, changing default passwords on network devices, encrypting transmission of data across open networks, and restricting access to data on a need-to-know basis. All companies, including Investment Advisor firms, that process, transmit, or store credit card data must comply with PCI DSS. The current version, 2.0, took effect January 2011.

Identity Theft and Assumption Deterrence Act of 1998

This act was passed by the Federal Trade Commission (FTC) in 1998 to combat the increase in identity theft. Title 18, Chapter 47, Section 1028 of the United States code outlines federal laws governing the theft and use of nonpublic personal information. The law, otherwise known as the Identity Theft and Assumption Deterrence Act, was the first law to criminalize identity theft at the federal level, as well as outline potential penalties for violations of the act which can include significant jail time. It also authorized the FTC to register complaints of identity theft and all federal law enforcement agencies to investigate and prosecute them.

Risk and the Need for Solutions

It is impossible in this day and age to conduct business without an online presence or the use of electronic communication. Inevitably, with the use of such communications and technology comes the risk of network and systems breaches and data compromise. The first three quarters of 2013 have shown that 57% of recorded data loss incidents were due to security breaches involving hacking (41%), fraud/social engineering (12%), or email (4%). Because of this it is of paramount importance that firms have in place sound programs to ensure the safety of customer data and non-public personal information. There is no one-size-fits-all solution that will work for all firms. However, having a proactive regiment of monitoring and testing in place, along with the proper training of firm employees, will show your firm's staff, clients, and regulators that privacy and data security is taken seriously as you achieve compliance with the regulations.

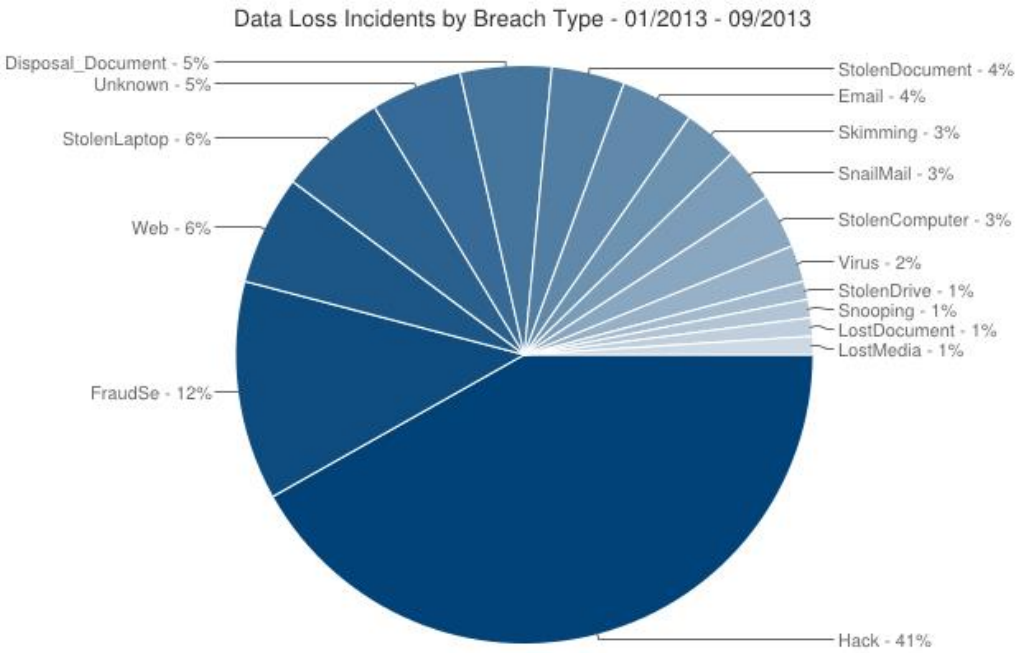

Chart courtesy of DataLossDB (http://datalossdb.org/) and the Open Security Foundation

Failure to comply with data security requirements not only opens up the firm to the risk of significant fines and penalties from regulators, but it can also lead to irreparable damage to the firm's reputation. The bottom line - Clients do not maintain relationships with firms they do not trust. There is no quicker way to lose the trust of clients than to allow for their personal data to be compromised.

Understanding the myriad of data security regulations that apply to your business is important and no small task. Assessing the technology available to you to assist in compliance to these regulations may at first glance seem like a rather daunting task. Rest assured — it may not be as difficult as you think.

***Bottom line**:*
There is no quicker way to lose the trust of clients than to allow for their personal data to be compromised.

Basic Security Concepts

Working towards regulatory compliance with regards to data privacy and protection will require systems to be put in place that define, implement, maintain, and test the secureness of your network and computer systems. Securing your network and systems requires a multi-layered approach beginning with several default security measures that — while not solely enough to secure your network and clients' nonpublic personal information — are considered to be the basic requirements.

Passwords

We all know what passwords are and how they are used. But few realize that most employees use passwords that are discoverable in mere minutes. Or that most individuals reuse the same password whether logging into social media websites, online retail websites, their online bank, or your network. This means that some of those "Large Data" breaches you hear about in the news may contain some of your employee's passwords: passwords that might also allow access to your firm's systems and your client's nonpublic personal information. Securing passwords takes a proactive posture with defined policies that need to be managed by senior staff and reinforced digitally by your systems.

Passwords don't need to be overly complex to be strong. Relying solely on complexity tends to lead towards shorter passwords. The argument being that "*My password is so complex that I can barely remember it, how will anyone ever guess it? So it does not have to be that long!*" The unfortunate fact is that today's computers boast so much computing power that sometimes complexity by itself is not enough. A test exercise that attempted to crack 10 passwords ranging in complexity proved that, on standard computing hardware, all 10 passwords were easily cracked within 20 minutes. The passwords used in this exercise were encrypted using a Microsoft® network authentication scheme that is widely in use on most Microsoft Active Directory Domains and Windows computers. The exercise showed that a very complex and hard to memorize password of `qhQ2Y0s71aZ=dy` fell to this attack as quickly as a simple password of `betty1953`.

So if complexity is not enough than what is? General best practices for protecting passwords from cracking attacks can be summed up in two points, the first being a bit of complexity and the other being length. Of these two points, length is the more important contributor to the strength of the password. It is recommended that passwords be at least 15 characters long, but you should strive for even longer. The example below will provide more information on how this can be accomplished with ease. Moreover, when a person is designing a password for their use, they should avoid using known data points about themselves or those close to them. Values like important dates, family member names, favorite sporting teams, etc. should all be avoided. Leaning towards a favorite personal phrase with added complexity works very well and is more easily memorized.

Example:

Personal Phrase:

```
my security rocks
```

Add some complexity and randomness to create a password/passphrase:

```
my2 $ecurity4 RoKs6!
```

You now have a long complex password that is 20 characters long, is composed of upper and lower case alphanumeric characters, contains special characters and is relatively easy to memorize.

Firewalls

The software or hardware based security devices that control what network traffic can enter and leave your network and computers are known as firewalls. The predominant functions of these devices are defined within catalogs of cryptic rules that spell out how applications and computers are allowed to access each other within the network and from the Internet.

Given that firewalls only allow traffic that is permitted by one of these cryptic rules, many firewall vendors lean towards having a less restrictive set of default rules to avoid creating client issues when initially installing the product within their network. This means that simply plugging a firewall into your network doesn't necessarily provide you the full protection that it is meant to provide. An important part of the installation process must require steps that analyze what types of network communications are required by your network. This is followed by manual customization of your firewalls set of rules to reflect these requirements.

Antivirus

Abbreviated AV, antivirus software products aim to prevent virus and malware infections by identifying and removing files that match certain criteria. Majority of AV solution providers lean heavily on pattern matching against what are known as signatures. When an antivirus vendor identifies a malicious program, it is analyzed and distilled down into a signature or fingerprint that uniquely identifies the malicious file. The AV software can then actively compare files that are downloaded, opened, or run to these signatures looking for a match.

These signatures are maintained and updated daily, sometimes even more frequently. In order for the AV software that is installed on your systems to be effective against known malicious programs, these signatures must be updated often and regularly. Moreover, signature based AV solutions provide little to no protection against viruses and malware that is not yet known to the vendor or where signatures are yet to have been written.

Security beyond the basics

The basic security points mentioned each merit a white paper of their own and even then each of these topics would just barely be introduced. These topics need to be considered the bare minimums when considering the security of a network. They alone would provide some protection from most of the malicious "noise" and automated malware that exists on the Internet; however, these are only the beginning if the goal is data protection and regulatory compliance.

Each organization is unique in how it manages data, business practices, and employees. These unique considerations need to be taken into account when thinking about securing your network and your clients' nonpublic personal information. There are many complex aspects that need to be considered when designing a security policy that moves you towards regulatory compliance. Likewise, there are many tools and practices that help with addressing these needs, such as:

- Setting Security Policy
- Vulnerability Management
- Access Controls
- Multi-factor Authentication
- Intrusion Detection

- Intrusion Prevention
- Data Loss Prevention
- Employee Training (Social Engineering, Phishing, etc).
- Penetration Testing
- And so much more …

Being able to effectively navigate the complexities that are present even in the basics of security can be very difficult. Large corporations hire teams of dedicated staff to meet these needs. These are costs that small to medium sized firms usually can't shoulder.

Finding Solutions

The inherent difficulty associated with managing informational security risk lies in the need for highly specialized expertise. Hiring this level of expertise is usually considered to be cost prohibitive for small to medium sized firms, so short-term consulting arrangements have become the norm. While these short-term consulting arrangements accomplish tasks that allow for a firm to work towards regulatory compliance and provide a level of understanding regarding the firm's current exposure to these types of risk, these beneficial results are short lived. The continually evolving threat landscape of today's web-connected marketplace mandates that ongoing monitoring and the ability to identify and react to change are key components to maintaining a security posture that will effectively protect your client's nonpublic personal information.

The reality of the matter is that once procedures have been put in place to establish regulatory compliance and to determine your firm's overall risk baseline, ongoing monitoring and proactive reaction to threat changes is mandatory to maintaining compliance and keeping your exposure to these risks in check. This is where Mimic Technologies' Total AdvisorSecure™ program can be leveraged as your virtual security department. Total AdvisorSecure™ is a premium managed services offering designed to help your Registered Investment Advisory firm answer its needs for security risk awareness and systems security in order to work towards regulatory compliance. From establishing a standing security policy and quantifying your firm's exposure to infosecurity risk to pressure testing your current systems and procedures through penetration testing, Mimic Technologies can help you work towards truly securing your clients' nonpublic personal information.

Contact us:

888-99-MIMIC (64642)

Fax: 847-919-3862

info@mimictechnologies.com