The "Inevitable" Cyber-Attack: Are You Prepared?

"Inevitable"

— An SEC commissioner discussing the likelihood that a cyber-attack will bring down significant market infrastructure.

March 27, 2014

This white paper has been developed by eSentire, Inc. and The Regulatory Fundamentals Group LLC to help you understand why SEC Commissioner Luis Aguilar would conclude that a cyber-attack will inevitably bring down significant market infrastructure and to help you answer one fundamental question: Are you prepared for the inevitable?

Here's what's going on.

We all know that cyber-attacks are a fact of life, but few fully appreciate the extent to which the attacks are growing more sophisticated, increasing in volume, and targeting the financial sector and its service providers. In 2013, eSentire saw a 100% increase in targeted attacks over the prior calendar year.

Cyber-criminals regard certain financial services companies, particularly the smaller and mid-size ones, as relatively easy targets—this includes hedge funds, private equity funds and in general all registered investment advisers (RIAs). Why?

1. Access to important information. There are a lot of them and they control 5% of the U.S economy's asset base. They may have clients' funds, confidential data, their own strategies and trading models which may be of value (and used by cyber-criminals for front running and market manipulation), access to information on mergers and other highly-sensitive material.

2. They are a conduit to other desirable targets. They interact frequently with service providers, which may include larger targets (such as banks or broker-dealers) that would be more difficult for cyber-criminals to access directly, and with law firms, which can also can be valuable targets for cyber-criminals.

3. Their cyber-defenses are frequently easier to penetrate than those of larger organizations.

Because attacks focus on vulnerabilities, not company size, hackers are particularly interested in resource-constrained mid-size enterprises which typically employ weaker security measures. A 2013 study by Symantec reports that in 2012 31% of all attacks targeted businesses with fewer than 250 employees and 50% of all attacks were aimed at businesses with fewer than 2,500 employees.[1] As noted above, hackers understand that these companies can serve as the vehicle for a wider attack (such as harvesting private consumer data and penetrating larger trading partners' networks) and themselves have confidential information, intellectual property and bank accounts that could prove valuable to a cyber-criminal to use for its own purposes or to sell to others.

[1] 2013 Internet Security Threat Report, Symantec. http://www.symantec.com/security_response/publications/threatreport.jsp.

These attacks permeate multiple industries.

Recently a technology start-up publicly announced a multi-million dollar funding round from a venture capital firm. Nearly 20% of these funds were stolen by cyber-criminals who also read the trade news. Using a "spear-phishing" email containing information relevant to the firm, the attackers deceived employees and caused them to install a keystroke logger at the target firm. When the firm logged into its online banking service, the cyber-criminals captured the target's credentials and made three quick withdrawals before they were detected. This well-orchestrated and well-timed attack succeeded despite both the online credentials and a security token system distributed by the bank.

In another recent incident, a law firm suffered a six-figure loss when hackers, armed with legitimate credentials, bypassed security defenses and stole funds placed in trust accounts.[2] Such attacks are pervasive, with a well-respected cyber-security publication article reporting that during 2011, around 80 major U.S. legal firms were hacked.[3]

Hackers are not simply trying to break through systems for their own entertainment, to prove themselves in the hacker community or to gain access to bank accounts. Targeted attacks can be aimed at firms involved in significant transactions. One notable case involved China-based hackers who penetrated computer networks of several law firms in 2010 to obtain more information on a multi-billion dollar acquisition bid.[4]

Political motives are another driving force behind some cyber-attacks. For example, a group of state-sponsored hackers, dubbed the "Comment Group," infiltrated political targets, such as the president of the European Union Council, at the height of the Greek bailout controversy. The Comment Group's targets also included other economic targets: law firms, investment banks, oil companies, drug makers and technology manufacturers. The Comment Group harvested seismic maps charting oil reserves from major oil companies, stole client trade secrets from patent law firms, and obtained market analysis data from investment banks.

Even more troublesome is the possibility that a cyber-attack could be used as an act of terrorism, to bring down the fundamental infrastructures on which our evolved economies depend. This is the primary concern that is driving regulatory change today. As they work to reduce exposure, regulators are increasingly aware that the smallest link can prove the Achilles' heel that brings down the system. As noted by the head of IntercontinentalExchange Group, the interconnectivity of the system is itself a vulnerability. "The scary thing for us is not what we control…[but that] we all have common customers that are connected to us, that are connected to each other," he commented

[2] In this case, the cyber-criminals used a Trojan banker virus which mirrors a bank's website. It prevented the target's bookkeeper from accessing a bank website. A message came up that the site was down for maintenance and asked for the bookkeeper's name and phone number. Shortly thereafter the bookkeeper received a "helpful" call from the "bank" and during the call was instructed to try to log in again. This information was transferred to the hackers who now had access to all of the firm's trust accounts. http://www.lawtimesnews.com/201301072127/headline-news/law-firms-trust-account-hacked-large-six-figure-taken.

[3] Source: Help Net Security 'Law firms get hacked for deal data', January 2012.

[4] Source: Bloomberg 'China-based Hackers Target Law Firms To Get Secret Deal Data', January 2012.

recently.[5] This is the reason why firms should expect regulatory efforts in this area to accelerate in the coming months and why, as discussed below, you will need to consider how your firm might respond should the "inevitable" attack occur.

But even without facing this worst-case scenario, are you exposed? The answer is undoubtedly "yes." For hedge funds alone, eSentire has conducted hundreds of risk assessments in the past ten years and has yet to find a company where the amount of compromise did not require immediate remediation to correct high or critical vulnerabilities. A vulnerability assessment at a top 100 New York hedge fund, conducted last year, provides some insight into the levels of threat. During the course of a three-week multi-dimensional review, eSentire determined that the firm downloaded 14,000 executable files—but only a mere 4,000 were from legitimate sources. This particular hedge fund already had a policy that prohibited access to and use of social media and cloud-based storage services. But as the review highlighted, a policy is not a control. Employees may still access various sites, download materials from them and use them to transfer files. Often this is done for a benevolent purpose, such as moving large files from work to home. But without adequate encryption, there is inherent exposure.

[5] http://www.reuters.com/article/2014/03/13/us-exchanges-cybercrime-idUSBREA2C1SZ20140313.

Why is this so troublesome?

There is no end to the types of damage that can occur through a cyber-attack.

Much of the current legal and regulatory structure is focused on the concern that the personal information of individuals might be disclosed and used inappropriately—leading an individual to face financial loss and a reduction of credit rating. Many governmental bodies have proscribed steps that must be taken by a firm should such a loss occur. As discussed in RFG and eSentire's 2012 white paper,[6] the SEC and the CFTC require firms to provide clients with a privacy policy that explains how they collect, protect and use client information.

However, cyber-criminals can do far more than harvest personal information to access financial accounts. These newer initiatives focus on the scenarios noted below:

1. They can gain access to valuable firm information which can be used for the hackers own ends including, in some cases, simply to extract a payment from the target firm.[7]

2. Attacks can compromise systems so that operational uptime suffers and strategies cannot be timely executed (with a cost to profits and performance).

3. Once hit, a firm faces business disruptions (both in executing business activities and time spent in incident remediation), damage to reputation and the potential loss of funds.

4. Disruptions can spread to trading partners and the financial system as a whole. As noted above, this is the driving focus behind the most recent regulatory initiatives. Should a significant trading partner or financial clearing mechanism be affected, the ability to undertake or settle trades, mitigate risks or find liquidity could be profoundly impacted for a large number of market participants. A worst-case scenario might cause firms to fail.

While it appears that to date no internationally active bank has been shut down as a result of a cyber-attack (except indirectly as a result of the September 11th attack on the World Trade Center), some of their websites have been rendered useless for periods of time. Also, they constantly face nuisance and brand attacks.

Moreover, during 2013 at least ten major banks faced attacks by "hacktivists." This is yet another category of cyber-threat which arises from persons driven by a vision of having the moral high-ground. They may attack to destroy the reputation of the firm or its principals and use techniques ranging from defacing websites to leaking private content. JP Morgan Chase, Bank of America, CitiGroup, Wells Fargo and others have faced such attacks. Similar strikes also target the websites

[6] "The ABCs of a Technology Breach," available at http://regfg.com/Site/Page/the-abcs-of-a-technology-breach-32/.
[7] One notable group encrypts the target's web site and demands payment before providing a means to unlock the encryption.

of municipalities or online payment systems associated with utilities operators. One such example targeted the Florida Public Power website in 2013.[8]

In the Ninth Edition 2014 Global Risks report, the World Economic Forum identified "digital disintegration" as one of the leading risks faced today. It notes, "risks to the Internet continue to grow more serious for one key reason: attacking others in cyberspace (breaking into or disrupting their system) has always been easier than defending them" with almost every company's defense being readily breakable.[9]

[8] http://publicpower.com/2013/denial-of-service-attack-temporarily-overwhelms-jea-website/.
[9] http://reports.weforum.org/global-risks-2014/part-2-risks-in-focus/2-4-digital-disintegration/.

How do they get in?

Putting aside data leakage from staff, which is a frequent but often overlooked risk in the race to keep adversaries away from valuable assets, cyber-criminals often gain access to their target's network using benign looking emails carrying spyware attachments (called phishing). If the emails contain relevant content from supposedly trusted sources it is called spear-phishing.

Hedge funds are among the firms that have been attacked using dangerous emails that include timely and pertinent industry-specific subject matter. (Between February 1, 2013 and January 31, 2014 eSentire saw a 100% increase in such attacks.) These emails are much more sophisticated than the clumsy emails of the past featuring misspelled words and pictures of celebrities. In 2012, hedge fund managers were targeted by malware-bearing spam containing free advice on an account mechanism used to return income to funds. The disguise was made even more effective as it appeared to be from a legitimate source. The email contained an executable file—a Trojan—which when launched provided legitimate financial information, but also installed a key logger in the background. Later analysis showed that the key logger uploaded valuable financial data to its remote command-and-control (CIC) server. At the time of this attack, only 11 of the 42 available defense products, including well known anti-virus services, were able to detect this attachment and identify the threat.

Hackers also focus on placing content on websites as a way to reach a network. Cyber-criminals will use "drive-by-downloads" from fake websites, as well as "watering holes" set up on legitimate websites. For example, a February 2013 press report describes pages on official U.S. Government websites that contain content to promote third-parties products.[10] Such pages or those they link to could also contain malicious content. (Between February 1, 2013 and January 31, 2014 eSentire saw a 10% increase in "drive-by-downloads".)

Hackers also use malicious scans that troll security defenses looking for vulnerabilities, or even outright brute force attacks (systematically checking every possible network system password variant). (Between February 1, 2013 and January 31, 2014 eSentire saw a 20% increase in such attacks.)

Sometimes compromised physical devices are the point of entry; for example, cyber-criminals might drop a compromised USB in a parking lot in the hopes it will be picked up. On the other hand, this is often not necessary. Devices that provide remote access, such as Android phones are particularly vulnerable to web-based attacks. Only recently in mid-March, Apple announced a major hole in the SSL implementation that left iOS and Mac OS devices vulnerable to attacks using the Safari internet browser as a means of entry. Of course, the risks associated with using devices, including laptops, in public spaces are already well understood by most.[11]

---

[10] http://www.weeklystandard.com/blogs/widespread-vulnerability-found-dozens-government-open-data-websites_782700.html.

[11] See Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," (February 10, 2012). http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html.

Whatever the means of entry, once in, an inserted code is used to install key stroke loggers which harvest credentials to coveted systems and bank accounts or provide access to confidential information stored on password protected servers. Given the increased sophistication employed, users are often unaware that they are being monitored or that they may be giving access to a third-party rather than logging on to the intended system.

Recently, eSentire detected an attack that used Microsoft Word files to carry malware. The files ran a mock Windows Security Login screen, which even contained the target company's logo. When users inadvertently entered their login credentials the information was fed to another website where criminals could pick up the credentials and look for assets and financial information on their victims' networks at will.

Finally, as mentioned above, hackers may gain access to your systems through the systems of trusted advisors, such as law firms. A top FBI cyber-security expert recently reported: "We have hundreds of law firms that we see increasingly being targeted by hackers…"[12] In fact, some sources believe that most legal firms have been victims of security breaches and that these breaches operated for up to nine months before being discovered.[13]

Of particular concern, advisers are often uniquely targeted for attack, with eSentire seeing the vast majority of attacks launched against its clients as unique to the sector. Said differently, information about prospective attacks shared by governmental sources is less predictive of what a hedge fund will face than information gained from direct experience from other clients.

[12] Evan Koblentz, "LegalTech Day Three: FBI Security Expert Urges Law Firm Caution," Law Technology News (February 1, 2013)
[13] Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal at 32 (June 2013); see also, Corporate Clients Should Ask Specific Questions About Law Firm Computer Security, Experts Say, Martha Neil, ABA Law Journal, Feb 21, 2012, http://www.abajournal.com/news/article/corporate_clients_must_ponder/.

Why is so much damage done?

Most defenses simply are not effective. Most security incidents go undiscovered for months and many are discovered by external parties, not the targeted company itself.

New viruses and methods of attack are constantly being created. For a period of time, which can sometimes be quite substantial, anti-virus vendors do not identify these new mutants. If inadvertently downloaded during this period—from website visits, emails, social media and other porous technologies—-they can spread within minutes and take command and control of computers and servers throughout a global network. This control can be used to gain information about the company and eventually to shut down trading systems, gather confidential information and work other types of mischief. The *only* protection is to detect infected nodes and stop the spread of nefarious code in real time.

As noted above, many attacks lie undetected inside enterprise networks—often for months or even years. These are the most damaging breaches. The industry calls these “advanced” cyber-threats. These “sleepers” imbed themselves into a company’s network where they operate in three distinct phases.

The first is to establish a beachhead on the inside from which to conduct operations. Most security products on the market today are designed to prevent this type of breach—they look outward to prevent intrusion. However, hackers take advantage of four gaps: (i) designed to prevent the reoccurrence of recognized attacks, products may be one step behind as the threats morph, (ii) attacks outflank the defensive perimeter created by anti-virus, firewalls, and intrusion prevention systems (IPS) because these systems generally focus only on malware, not stolen credentials (malware constituted about 40% of the reported attacks in 2013 leaving the other 60% of reported attacks unattended); (iii) IT staff can be swamped with automated alerts with little guidance as to which ones to prioritize, and (iv) few firms will take responsibility for remediation once a breach does occur.

Once the threat has evaded all outward-looking security protections and established its beachhead, a second stage commences. To begin, they take control of security systems, disarm anti-virus software and cover their tracks. At this point the threats can only be detected by security experts watching 24x7x365. Later during this stage, as the intruder gathers knowledge about the enterprise, it establishes a remote command-and-control capability.

The third and final stage, once the threat has learned as much as it can, is exploitation—which often takes the form of extracting confidential information while the company is unaware. The creativity, however, of cyber-criminals never ends. Another approach recently employed has been to fully encrypt a target company’s website and demand a “ransom” payment for the encryption key. Locked out from access to its critical information, the company faces internal disruption, loss of data and loss of client confidence (although no sensitive personal data has been stolen per se).

What are you required to do about it?

To some extent this depends on the type of breach that occurs—and who your regulators are.

Sensitive personal information. Most financial regulators and legislative efforts are focused on the theft of sensitive personal information. The SEC and the CFTC have virtually identical privacy regulations, which require registered firms to adopt policies and procedures to secure client data, protect against security threats, and prevent unauthorized access to information.[14] These require a firm to provide a privacy notice to clients and investors describing how their personal information is obtained, maintained and used. In February 2014, the CFTC published best practices recommendations about compliance with these regulations.[15] Suggested practices include a written information security and privacy program tailored to the firm's activities, a designated employee to oversee the program and coordinate cyber-security risk assessments, internal testing and external testing by an independent party, a security breach action plan, and periodic reporting to senior management.

Other regulators may have their own unique requirements and expectations.

Also, in the case of information about individuals, there are numerous and conflicting laws about how personal information may be used, the kinds of protections applied to it and what must be done if there is reason to believe such data has been breached. In 2012, RFG and eSentire developed a white paper, *The ABCs of a Technology Breach*, which can be found here: www.RegFG.com/Site/Page/the-abcs-of-a-technology-breach-32/. That paper highlights some of the key regulatory requirements, discusses ways to protect against such a breach, and provides suggestions about how to respond.

Sensitive firm information. The theft of anything, including the intellectual property of a firm, may be a crime with respect to the person who steals the data—whether an outsider or an employee. But financial regulators, unlike criminal prosecutors, rarely focus their regulatory efforts on prescribing how much effort a firm must devote to protecting its own intellectual property. By and large, firms are left to take care of their own self-interest on this score—an approach that contrasts starkly with the numerous laws and regulations addressing protection and use of information about individuals (whether employees or investors).

Changes afoot. As noted above, concerns about the possibility of a cyber-attack that poses systemic risk may lead many regulators to rethink this approach. Reflecting these concerns, on March 26, 2014, the SEC hosted a roundtable. Notably, and underscoring the significance of the issue, SEC Chair Mary Jo White attended the whole session. The meeting was also attended by *all* the commissioners: Luis A. Aguilar (the initial force behind the meeting), Daniel Gallagher, Kara Stein and Michael S. Piwowar. At the commencement and throughout the session each of the

[14] Privacy of Consumer Financial Information. SEC Regulation S-P (17 CFR Part 248); CFTC Regulation (17 CFR Part 160).
[15] Available here: http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

commissioners underscored that cyber-incidents are escalating in frequency and complexity and sought to understand how the SEC could best play an active part in protecting its regulated firms, the financial markets and ultimately the country as a whole.

SEC Chair Mary Jo White stated the SEC will act with "appropriate haste" to consider what additional steps it should take. A write-up describing the roundtable can be found here.

FINRA has also announced that it is in the process of conducting examinations that will help it assess cybersecurity risks—from the types of risks firms face to understanding how firms assess risks and supervise/manage these issues.[16]

Likewise, the SEC is in the process of planning for a round of investment adviser examinations targeted on cyber-security concerns for later this fall. The SEC staff may view these exams initially as a way to gather information before any definitive industry guidance is given. For example, during this process staff may try to understand how big the cyber- security risk is for investment advisers and their clients; the types of protocols the industry uses today to identify when a cyber-attack takes place and the nature and frequency of attacks. A likely related focus will be on how a firm acts once an attack happens: who at the firm is told about it and does this include the board or governing body?

Other forces will also drive change. Those firms seeking to obtain cyber-insurance will find that insurance companies use risk-based protocols. Clearing firms are also increasingly seeking to understand the cyber-risks that arise from the firms for which they clear and some are setting minimum standards.

A firm should ask itself: what would investors want to see in place to know that their information, their assets, and their managers' ability to operate is protected? With this degree of emphasis, perhaps at some point disclosures about a firm's cyber-preparedness will make their way into offering documents.

National Associate Director of the investment adviser exam program Jane Jarcho has indicated that as regulations are developed, the staff will be working under the assumption that large firms are taking cyber-security more seriously than smaller ones. For this reason, when cyber-security guidelines come out, she expects them to apply equally to smaller firms. She offered no timetable as to when to expect these, but did indicate that they are unlikely to contain a set laundry list of precautions and actions.[17] This is a possible signal to the authors of this white paper that the SEC will follow the approach set forth in the NIST Framework, which is described below.

[16] http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219.
[17] http://www.fa-mag.com/news/sec-ia-exams-chief--small-firms-won-t-get-cyber-security-rules-exemptions-17205.html.

What *should* you do about it?

Philip Reitinger, Director of the National Cybersecurity Center, Department of Homeland Security, once provided this advice:

> "[I]f somebody wants to get into your system, they have a very, very good chance of doing it. So if you don't want your system compromised, disconnect it from the Internet. Turn it off and don't allow people to touch it, and then open up the box and take a hammer to the hard drive. At that point, you're relatively secure."[18]

For those who can't follow this advice, and with staff and outsource service models that require a more open structure, meeting current regulatory requirements may no longer be enough. This will likely become more apparent as a result of a recent game-changer: On February 12, 2014 the White House released a Framework for Improving Critical Infrastructure Cybersecurity established by the National Institute of Standards and Technology.[19]

The framework is non-prescriptive but provides a common terminology that can be used to determine how a firm addresses cyber-security issues. As awareness of the cyber-threat issue grows and the Framework provides a hard-measure of preparedness, it will no longer suffice to have processes in place to protect the personal information of your clients and investors—although that will be important. It will no longer suffice to have processes in place to protect the loss of critical firm data such as trading algorithms or to have developed and tested a business continuity plan. Of course, that is important too. From the perspective of senior management, the Framework indicates what could, and possibly should, be done and this vision far exceeds what is currently required.

The Framework describes a three-component approach to cyber-security issues. The first component highlights the need to identify, detect and protect against risks, and to respond and recover appropriately. The core also provides reference citations to help determine legal and regulatory requirements and best practices. The second component defines organizational approaches to the risks, ranging from ad hoc to fully risk-based and informed. The highest tier, which will likely become the only acceptable tier to regulators, is called the Adaptive Tier. At this level an organization has an enterprise-wide approach, uses risk-informed policies, shares information with partners and adapts its cyber-security practices through a continuous improvement process. The third component—a Profile—is based on an organization's identification of the risks that apply to its business activities and self-selection of an applicable tier of cyber-risk awareness. The Profile can describe an organization's current state of readiness and its desired state. (The Framework also notes the need to protect civil liabilities and privacy.)

[18] http://www.abajournal.com/magazine/article/cyberspace_under_siege/.
[19] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

With the Obama administration, the exchanges[20] and the financial regulators telling investment advisers that a huge cyber-security risk exists today, every management team needs to consider how to protect their firm and their clients. How can you explain that you were not prepared for the "inevitable?"

First, to understand firm exposures a risk assessment should be undertaken, as recommended in the Framework. Below we highlight some questions to consider:

1. Our firm: An attack against the firm might place the firm, its clients and its reputation at risk. Would we know if our systems have been penetrated? How? What information and assets do we have that others might want to access? What systems and information are critical and how would we maintain them in the event of an attack? How secure is information about our investors and our employees? How do we know? Who needs to be informed internally and when is senior management and our governing body informed? When should clients be informed?

2. Current state: Firms may decide that they need to baseline their current exposure by undertaking an enterprise-wide vulnerability assessment. This exercise determines if the firm's outward facing defenses have already been compromised and, if so, what types of remediation should be undertaken in the short term. At this point, firms may also want to consider on-going monitoring for future attacks.

3. Our service providers: The attack that places a business at risk may not even be directed at the firm but may instead be directed at a service provider. What if a clearing bank could not accept securities? What if the firm could not obtain liquidity? What if a risk metrics vendor went down? What if a fund board of directors could not respond to a significant issue? For this reason each firm needs to understand the critical service providers it relies on. How robust are their defenses? What precisely is the exposure to them? Are any back-up plans in place and have these been tested?

4. Other risks: The cyber-attack that places a business at risk may not directly involve it or its immediate service providers. What if one or more exchanges or key counterparties went down? What if clients go down and cannot be communicated with? Consider also third-party services on which you depend (Google Docs, Dropbox, Amazon EC2, government portals, etc.). Running different scenarios may help you identify this type of risk. Admittedly, with respect to these areas, few firms can act alone to address or mitigate the problem. However, having gone through the exercise should at least provide insights that the firm can draw upon should a scenario materialize.

[20] More than half of the world's exchanges faced cyber-attacks in 2012 leading exchange officers to express a growing sense of alarm. http://www.reuters.com/article/2014/03/13/us-exchanges-cybercrime-idUSBREA2C1SZ20140313.

The risk assessment should also include a very comprehensive list of the regulators a firm may need to interact with and their requirements. The list of regulators may need to include regulators that oversee clients and investors, as well as the firm itself.

In addition, senior management will need to consider the governance processes it seeks to build around cyber-security issues generally. This may include a requirement for management to receive periodic reports and for material events to be escalated to the governing body. As part of this process senior management will also need to consider communications internally and with external stakeholders on a variety of issues. This will range from the timing of disclosures of breaches (particularly material breaches) to more general disclosures about the nature and extent of the firm's cyber-security program, such as whether the firm is currently in or targeting the Adaptive Tier.

As noted above, laws and regulations in some jurisdictions prescribe the timing of disclosure to affected parties, regulators, consumer reporting agencies and/or enforcement personnel. Sometime contractual provisions will require disclosure. There are breaches, however, where disclosure may not be legally required, and the decision to communicate with outside parties becomes an issue of business judgment. Even if disclosure is not mandatory, it may be important to keep a particular regulator, counterparty or investor informed about a data breach, simply to maintain a good working relationship or to obtain "credit" for good citizenship in the face of an enforcement proceeding.[21] If a firm actively discloses its cyber-security program, and particularly if it states that it is in a higher protective tier, the decisions it makes about disclosures of breaches may face more scrutiny from regulators, investors and the public. This is another factor that must be considered as management navigates through this space.

[21] By way of analogy, see the SEC's enforcement division announced a new initiative encouraging municipal securities issuers and underwriters to self-report certain Exchange Act violations in exchange for favorable settlement terms. http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541090828#.UycuGYXE40N.

Conclusion.

FBI Director Robert Mueller noted in 2012, "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."[22]

In today's interconnected digital age, the issue a management team will face is not likely to as simple as a computer system or website that is down; they are much more likely to face a situation where fundamental areas of their business are inoperative. The old adage "an ounce of protection is worth a pound of cure" could not be more apt. Moreover, taking the time to clearly understand a firm's business drivers and think strategically about pitfalls—and opportunities—should competitors, counterparties or other major components of the financial system go down, could provide the ability to act nimbly and appropriately at a time when vision really matters.

About eSentire

eSentire® is the leader in Active Threat Protection solutions and services, the most comprehensive way to defend enterprises from advanced and never-before-seen cyber-threats. eSentire's flagship offering, Network Interceptor, challenges legacy security approaches, combining behavior-based analytics, immediate mitigation and actionable intelligence on a 24x7x365 basis. The company's dedicated team of security experts continuously monitors customer networks to detect and block cyber-attacks in real-time. Protecting more than $1.3 trillion in combined assets, eSentire is the trusted choice for security decision-makers in financial services, healthcare, mining, energy, engineering and construction, legal services, and technology companies. In late 2013, eSentire was named to the Deloitte Technology Fast 50 Companies to Watch and cited as a Canadian Innovation Exchange CIX Top 20 most innovative Canadian company. For more information visit www.esentire.com and follow @esentire.

About RFG

RFG specializes in helping investors, advisers, and managers understand and integrate information and processes required for holistic enterprise risk management. The result is a systematic approach to navigating today's business and legal environment. RFG works with clients to identify key opportunities and vulnerabilities from business and regulatory perspectives and provides counsel, insights and creative solutions. RFG also offers a suite of web-based regulatory intelligence tools that highlight internal governance and management needs, including the RFG Weekly Roundup™, a regulatory thought leadership alert that highlight emerging areas of scrutiny. Visit www.RegFG.com or email Information@RegFG.com to learn more.

[22] http://money.cnn.com/2012/10/24/technology/barnes--noble-hack/index.html.