Cyber Liability: Risks, Ramifications, and Mitigation

An eSentire White Paper

www.esentire.com | @esentire | sales@esentire.com

Table of Contents

1. Introduction

2. Cyber Risks

a. External threats: criminals, hackers, and nation-states

b. Attack vectors

c. Insider attacks

3. Targets of Cybercrime

4. The Impact of Cybercrime

5. The Ramifications of an Attack

a. Responding to a cyber attack or data breach

6. Protecting Yourself from Cyber attacks

a. To protect against malware and hacking

b. To protect against rogue employees

c. To address third party vendor concerns

Appendix A: Narrow Your Target Profile

Introduction

Reflecting on cyberthreats, FBI Director Robert Mueller recently noted, "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." Data breaches often go undetected for months of even years, and are rarely discovered by the victim organization. In over 90 percent of attacks against organizations with less than 1000 employees, breaches are detected by outside agencies.

Cyber Risks

External threats: criminals, hackers, and nation-states

External threats created by cyber criminals or even governments often use clever methods to exploit user expectations, piggyback on porous technologies, and seep through anti-virus software and firewalls (called *perimeter defenses*) that are ill-equipped to protect businesses from increasingly sophisticated attacks.

Case: China Mafia-style Hack Attack Droves California Tech Firm to the Brink

For three years, a group of hackers from China waged a relentless campaign of cyber harassment against Solid Oak Software Inc. The attack began less than two weeks after the owner publicly accused China of appropriating his company's parental filtering software, CYBERsitter, for a national Internet censoring project. And it ended shortly after he settled a $2.2 billion lawsuit against the Chinese government and a string of computer companies last April.

In between, the hackers assailed Solid Oak's computer systems, shutting down web and e-mail servers, spying on an employee with her webcam, and gaining access to sensitive files in a battle that caused company revenues to tumble and brought it within a hair's breadth of financial collapse.

U.S. officials say that China in particular uses its national security apparatus for such intrusions, targeting thousands of U.S. and European corporations and blurring the traditional lines of espionage. A forensic analysis of the malware identified the intruders who rifled Solid Oak's networks as a team of Shanghai-based hackers involved in a string of sensitive national security-related breaches going back years. An independent analysis later found that four of the five active filters were copied almost verbatim from CYBERsitter and that Green Dam could not operate correctly when those filters were disabled.

Cyber attacks like the one described above may simply be new manifestations of traditional criminal conspiracies or, in a significant development, they may arise from parties with different motives, goals, and resources than common criminals. Threats from nation tstaes continue to escalate as countries seek political or economic gain.

Attack vectors

The majority of successful attacks these days are those initiated from an internal perspective, being of three categories:

The Most Common Way Cyber Criminals Infiltrate Their Target's Network

- Malicious content received within an email attachment
- Malicious content received while surfing the Internet (aka 'Drive-By Download')
- Malicious content received through a lateral connection (an infected USB drive, CD/DVD, or from another infected system connected to the network)

Once in, the first thing they do is take control of security systems, disarm anti-virus software and cover their tracks. Anti-virus and firewall tools are not enough to combat such threats.

Insider attacks

So far we have focused largely on external threats but some threats exist closer to home - and arise from employees. For example, a former Citadel employee was accused of stealing trading algorithms for his own personal use. Citadel's information technology department discovered the alleged theft based on the unusually large amount of data and programs tied to the employee's profile on Citadel's computer systems. A recent Goldman case involved a near-identical fact pattern with Goldman discovering that an employee had downloaded millions of lines of trading code in anticipation of starting a new job with a competitor. Although the Citadel and Goldman cases involved theft of code, rogue employees may also seek investor data as well.

In this evolving environment, all firms need to carefully consider how to best address cybersecurity issues, including those that arise due to their reliance on service providers. In addition, firms need to design protections for investor and employee personal data, and firms that rely upon proprietary technology may require additional protections.

Targets of Cybercrime

Recent cyber attacks victimize private sector economic targets: law firms, investment banks, oil companies, drug makers, and technology manufacturers. Cyber criminals have harvested seismic maps charting oil reserves from major oil companies, stolen client trade secrets from patent law firms, and obtained market analysis data from investment banks. These attacks clearly highlight the skills and resources available to such hackers. Consider the sophisticated cyber attack tools that have been based on the Stuxnet worm that spread via Microsoft Windows before attacking specifically targeted industrial software and equipment.

These examples serve as a strong warning that cyberthreats pose a clear and present danger to Wall Street, major law firms, technology companies, and other key components of the economic engine. Cybercrime is a never-ending battle of one-upmanship between the hackers and those that stand between them and their potential victims.
In fact, President Barack Obama recently dubber cyberthreats "one of the most serious economic and national security challenges we face".

The Impact of Cybercrime

Cybercrime is big business, with estimated losses valued at $388 billion annually, rivaling the illicit narcotics industry at $411 billion. As new security cracks are identified, tools to exploit these vulnerabilities are sold on the black-market. Some even come with warranties and help desk support.

No matter how extensive the advance preparations, no firm is immune from a data breach or cyber attack. In recent years, we've witnessed the hacker group, Anonymous, disabling commercial banking and transaction websites (Visa and PayPal) as a protest against the prosecution of WikiLeaks founder, Julian Assange. The software used is free and readily available (with tutorials) through a quick Google query.

We've also seen the targeted attacks described in this document that can lead to economic loss, or near bankruptcy of the target organization. Solid Oak Software Inc. is just one example. A once successful technology company brought to the brink of financial ruin by cyber criminals.

In another client case, a sinister zero-day attack infected a machine in the network of an investment firm. The malware propagated to the next machine, but not before setting the patient zero machine into a state that overheated the CPU and cooked the server. The malware was unsuspectingly downloaded from a compromised website visited by one of the IT help desk staff. Once the attack was mitigated, the IT head of the client reflected on the impact of the attack: "Had the virus gotten into our trading system, it would have been lights out!"

The Ramifications of an Attack

No matter how extensive the advance preparations, no firm is immune from a data breach or cyber attack. In recent years, we've witnessed several high-profile attacks (Visa and PayPal) and many other targeted attacks that can lead to economic loss, or near bankruptcy of the organization.

Data loss is another issue that continues to grab headlines. Consider the recent case of 500,000 student loan records lost on a USB drive. These records contained the Social Insurance Number (SIN) amongst other financial data for the half a million applicants.

Responding to a cyber attack or data breach

A breach of a system triggers two related but distinct responses: a systems/technology assessment accompanied by a management effort to address business-side concerns. The firm will need to **(1)** quickly put a team in place to implement a (potentially wide-ranging) crisis management plan that covers multiple crucial tasks, **(2)** gather the facts necessary to make an appropriate response, **(3)** communicate appropriately with amny diverse stakeholders on a timely basis, **(4)** make any appropriate technology fixes, **(5)** verify that any fixes have fully addressed the issue, and **(6)** take remedial actions necessary to avert future problems. The size and composition of the team will depend upon the size of the firm. For larger firms, responsibility may be divided into two teams: one to handle technology isues and the other to handle business issues.

The business side (ideally represented by the firm's senior executive(s), legal, compliance, and , if needed, public relations advisors) will assess the problem's impact on firm positions, the market/industry (if these issues are applicable), and investors. The business side will also consider compliance with applicable laws and regulations. In egregious circumstances, particularly where a breach was caused by intentional employee malfeasance, legal counsel may need to advise on the manner in which an investigation should be conducted, how documents are preserved, and the amount of disclosure reqiuired.

In any case, senior management will need to determine how to provide an effective and timely communication of the firm's position to key constituencies, including regulators, investors, counter-parties, credit providers, and the general public, as appropriate given the facts and circumstances of a particular crisis.

Other constituencies that may need to be advised include law enforcement agencies. If the event is one that is covered under any applicable subscription agreement, contracts, or financial arrangement, the firm may be required to notify any party under such agreements.

In addition, some jurisdictions require the notification of parties whose data has been breached, and some states also require notifications directly to state regulators. These laws usually cover when a notification requirement is triggered, what information must be disclosed, and how quickly notification must take place.

A notification requirement is typically triggered when social security numbers, driver's license numbers, and/or financial account numbers are leaked along with names or other identifying information connected to the numbers at issue. The content of a required disclosure is usually quite specific to the state.

Protecting Yourself from Cyber attacks

Cyber attacks have evolved from the high-volume, low-value (nuisance) threats, such as chain emails and spam, to low-volume (targeted), high-value attacks all too common in firms with valuable assets such as investment research, patent applications, and mergers and acquisitions documents.

To protect against malware and hacking

1. **Perform regular vulnerability assessments**
   Perform a vulnerability assessment to determine if your firewall is properly configured, anti-virus patches are up to date, network servers and directories are secured with strong passwords, etc. More importantly, a vulnerability assessment can also detect evidence of malicious activity inside the network. Vulnerability assessments should be performed at least once, if not twice a year. Think of a vulnerability assessment like a medical check-up; it's simply good security hygiene.

2. **Establish priviledged access to data**
   Access to valuable assets should only be granted to those employees who need access to do their jobs. Don't place highly confidential content on an unprotected server and always password-protect these directories and files. For example, only finance employees should have access to the firm's accoutning needs.

3. **Develop an Acceptable Usage Policy (AUP)**
   Develop an AUP that provides guidance around downloading software, the use of personal devices, cloud-based mail and storage services, and the access and distribution of confidential information. Once the AUP is in place, ensure that your employees are trained on the procedures and risks.

4. **Get Protected. Stay Safe.**
   Engage 24/7/365 information security services that provide real-time intrusion detection and mitigation if you must protect highly valuable assets. Continuous Monitoring as a Service (CMaaS) tracks and monitors network activity including intrusions, attacks, and the accessing of sensitive data, and manages this with 24/7/365 network monitoring through a security operations center (SOC). This service is not to be confused with a 9 to 5 help desk that provides non-real-time support for firewall configuration or post-event network logging. Hackers don't keep bankers hours. They work late and they work weekends.

To protect against rogue employees

1. **Create priviledged access to confidential and critical data**
   Employees often have access to proprietary data which a firm uses to distinguish itself in the market. This data includes trading algorithms, computer codes for high frequency trading, pricing models, firm investment strategies, and client databases. Typically a firm's legal team plays an important role in securing the use of this data for the firm through registration, copyrights, and properly crafted employee agreements. More specifically, firms often use confidentiality, non-disclosure, non-competition, and non-solicitation agreements to protect intellectual property and provide clarity on these issues to employees. In the case of global operations or employees working outside of the firm's home country, it is particularly important to understand the intellectual property laws of the relevant foreign jurisdiction and the enforceability of relevant agreements. Firm managers should discuss intellectual property rights with their attorneys and have these issues out of the way before starting operations.

2. **Establish priviledged access to data**
   Access to valueable assets should only be granted to those employees who need access to do their jobs. Don't place highly confidential content on an unprotected server and always password-protect these directories and files. For example, only finance employees should have access to the firm's accounting records.

   Firms should thus build safeguards against in-house theft or improper downloading. Once boundaries are established, a firm may also choose to monitor employee behavior and computers, restrict electronic transfers, and tak electronic measures including password protection, encryption of computer systems, computer access limitations, and monitoring of email and network traffic. It is often easier to secure algorithms and confidential customer data if control over those areas is clearly delineated.

3. **Perform security background checks on employees with access to critical data**
   Employees should be carefully screened when they are hired, and they should also be made aware of what constitutes appropriate and inappropriate conduct through training, contractual agreements, and firm policies and manuals. Legal and compliance teams typically play a role in this process.

To address third-party vendor concerns

Outside threats may also result from a reliance on third-party vendors. While third-party vendors can undertake specific functions for firms, the firm will have the ultimate responsibility if anything goes wrong. To avoid liability created by third-party vendors and meet investor due diligence demands, firms should extensively vet potential vendors. When analyzing a specific service provider, a firm may benefit from considering the following:

1. **Consider the scope and criticality of third-party service**
   Carefully consider the scope of the service provider's offering. Cybersecurity risks may increase or decrease depending upon the information in the vendor's possession and the steps the vendor takes to protect it.

2. **The service provider's ability to adapt to any changes in the market or regulatory landscape**

3. **Perform a service provider background check**
   To assess adaptability, firms may choose to analyze the service provider's average tenure of staff, turnover rate, tenure of the staff assigned to the firm, financial stability, use of technology, disaster recovery and data management capabilities, policies and procedures, control environment, and client turnover.

4. **Evaluate the service provider's control structure and compliance procedures**
   In order to evaluate the provider's control structure and compliance procedures, firms may consider requesting the Type II SAS 70. The SAS 70 reports will soon be replaced by the SSAE 16, which is effective for reports for periods ending after June 15, 2011. International standards are reported under ISAE 3402, and the purpose of updating the reporting standard is so that it is similar to and complies with ISAE 3402. These standards can be used to measure third-party vendor's ability to physically secure hosted data, vet employees with background checks, conduct regular vulnerability assessments, and establish viable business continuity plans (BCP) and disaster recovery (DR) plans. These protective steps should be clearly defined, documented, and tailored to meet any requirements from specific applicable regulators. The documentation process should benefit the firm as it can then provide additional "operational" transparency to institutional investors and regulators similiar to position-level transparency within portfolios.

Appendix A: Narrow Your Target Profile

In order to better defend your organization against external attacks, we recommend that specific measures be made to limit exposure by reducing your attack profile available to an attacker. Suggested methods include:

- **Enforce a strong DMZ stance**
  Ensure that a separate network segment for Internet-accessibly systems is enforced. Even if someone is able to break into a system in the DMZ, their access to the inside will be hobbled.

- **Harden all systems within the DMZ**
  Practically every vendor has a whitepaper that details methods by which their product can be hardened against an attack. Rarely are the products shipped in a hardened state by default. This may include disabling or removing modules that are not needed or removing service-level identifiers (version numbers) that can be accessed by external entities.

- **Ensure that all patching is kept up-to-date and done so in a timely manner**
  This will require a full knowledge of all packages installed on the systems.

- **Remove default credentials**
  The administrator account names should be changed to something non-guessable.

- **Require multi-factor authentication measure for all external users connecting inbound**

- **Enact defense against file system changes**
  If a system is exploited, an attacked may use it as a malware cache to spread to other users. If files are added to your webservers, you should know about it.

- **Consider adding a Web Application Firewall (WAF) in front of critical webservers**
  A WAF can add additional rigor against targeted application attacks. In a similar vein, you should consider hiding custom web applications behind a separate authentication scheme, such as a separate SSL VPN system.

- **Restrict the inbound footprint from an external perspective**
  This includes disabling ports that don't require access from the Internet in general (including remote access to networking equipment).

- **Track all logins**
  Keep a detailed log history and security event monitoring, but pay particular attention to authentication failures, especially ones associated with high-profile users.

- **If possible, change all default access ports**
  By default, HTTPS is carried over TCP/443. However, this is not mandated. If you havea SSL-enabled VPN, by changing the port from TCP/443 to TCP/14433, external entities performing broad scanning against the default ports will not detect it.

- **Create strong outbound Access Control Lists (ACLs) on the firewall**
  In addition to enacting strong inbound ACLs on the firewalls, the creation of strong outbound ACLs on systems in the DMZ can limit the damage done if a particular system is compromised.

- **Disable auto-answer in videoconferencing systems**
  Many media-based protocols have security gaps. If it is not convenient to turn off videoconferencing when it is not needed, ensure that auto-answer is disabled.

- **Consider outsourcing web and email servers to a third-party**
  For example, hosted webservers and email servers generally have better performance and higher availability and they are two primary attack points. This approach can segregate attack vectors and prevent a breach in one to escalate to others.

- **Perform regular vulnerability assessments**
  Regular vulnerability scanning can ensure that vulnerabilities are reviewed and addressed in a timely manner. Whereas a broad internal vulnerability scan should be performed at least once a year, external scanning should be performed at least once a month.

About eSentire

eSentire® is a leader in continuous advanced threat protection solutions and managed cybersecurity services. The company's flagship offering, Active Threat Protection™, challenges legacy security approaches, combining behavior-based analytics, immediate mitigation and actionable intelligence on a 24x7x365 basis. Dedicated security experts continuously monitor customer networks to detect and block cyberattacks in real-time. Protecting more than $2.5 trillion in Assets under Management (AuM), 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**.

eSentire is named a Gartner 2015 Cool Vendor for Cloud Security Services in the 2015 Cool Vendors report by Gartner Inc.