



White Paper

ID Theft: Corporate Consequences and Responsibilities

**By Marne Gordan
Director of Regulatory Affairs
February 2005**

TABLE OF CONTENTS

Introduction	3
Who Done It?	4
Bracing for Impact	6
Go Phish!	10
Conclusion	13
The Cybertrust Approach	13
<i>Cybertrust's Risk Commander</i>	14
<i>Data Gathering</i>	14
<i>Analysis</i>	14
<i>Intelligence</i>	14
Cybertrust's Risk Management Program	16
<i>TruIntelligence</i>	16
<i>Actionable Intelligence</i>	16
<i>Security Management Methodology</i>	17
Resources	17



Introduction

Identity theft cost U.S. business over \$50 billion in 2003. Although primarily perceived as a consumer issue, ID theft can have a tremendous effect on an organization in terms of corrective action, loss of revenue, and loss of reputation. Egghead Software is the ultimate example; once the largest retail software vendor in the market, it changed its business model to online-only delivery in 1998 in order to capitalize on the dot-com "boom." In December 2000, a simple hack of its Web site led to the exposure of millions of customer data files including credit card numbers; Egghead never recovered from the incident, and was effectively out of business by early 2001.

Unfortunately, this is not an isolated circumstance. Attacks against businesses and organizations for the purpose of credit card and identity theft are increasing exponentially. In fact, ID theft is the fastest growing crime in the United States. The Federal Trade Commission (FTC) received approximately 215,000 consumer complaints regarding ID theft in 2003, by far the largest (42%) category of consumer complaint recorded. This represents 249% growth from 2001.

ID theft can be devastating to the consumer; credit card theft is bad enough, but even in the worst cases, the consumer is usually liable for no more than \$50.00 when the card/card number is stolen and used for fraudulent purchases. Many cards even carry zero-liability in the event of theft. ID theft, however, can have much deeper consequences, and can go on for weeks or months without the consumer's knowledge. Debt associated with ID theft can run into the hundreds of thousand of dollars, often destroying the victim's credit rating, and requiring hours of paperwork and legal assistance to restore the victim's "good name".

It is often broken down into three broad categories. "True name" fraud occurs when the criminal uses personal information to open a new account or establish benefits; the name and Social Security Number (SSN) are legitimate, but goods, services, benefits, correspondence, etc. are directed toward an alternate address. In an "account takeover", the criminal gains access to an existing, legitimate account. Funds are transferred or benefits directed immediately to an alternate. Finally, "criminal" ID theft involves the thief assuming an alternate identity to avoid prosecution; this is the least common of the three.

Consumers are becoming more conscious of fraudulent activity, particularly in the online community, and the need to protect their personal information. Attention is always drawn to this subject during the holiday shopping/end-of-year charitable giving season; literally hundreds of articles, news stories, and other types of warnings appear, reminding consumers to be vigilant in guarding their personal information, and describing the various precautions necessary to protect themselves from fraud. The FTC operates a Web site devoted to dealing with ID theft and abuse (<http://www.consumer.gov/idtheft>). 1

¹ Source: FTC National and State Trends in Fraud and Identity Theft Report
<http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf>¹



These warnings, however, are often aimed at the wrong target. Although consumers are ultimately responsible for protecting themselves and their information, they lose direct control over that information at precisely the point that it becomes an attractive target for thieves. During a given legitimate online transaction, the consumer hands direct control over their data over to a merchant, a subscription service, or a government agency for the furtherance of that transaction. When it has been completed, the consumer's personal information becomes a data file, residing in the online organization's network. The consumer is now completely dependent on the organization to effectively maintain the security and confidentiality of that data.

At the individual level, the consumer is no longer the primary focus for attack. Just as in the physical world, where it is far more profitable for a thief to rob a bank or a store rather than stealing wallets one-by-one, it is far more profitable and less precarious for cyber thieves to access databases that store thousands of consumer records than it is for them to employ the more traditional methods of "dumpster diving," stealing mail or pretext phone calling. Often times, thieves can accomplish their exploits from the comfort and discretion of their own homes.

Tips for Protecting Sensitive Data

Identify all non-public personal information in the environment. Make certain that this includes customer information, partner information, and employee information. Non-public personal information is defined as data not readily available in the phone book, such as name AND Social Security number, bank account number, customer account number, credit/debit card information, other payment information, insurance identification number, etc.

Who Done It?

In December 2003, Daniel Baas of Milford, Ohio, pled guilty to charges of hacking into the computer system and stealing information from Acxiom Corporation*, a firm that analyzes consumer databases for a variety of companies, including several Fortune 500 firms. He has also been charged with stealing information from several large companies including Cincinnati Bell, AT&T Mobile, Sprint PCS, Nextel, and his former employer, Market Intelligence Group.

He was discovered after he bragged to Internet chat mates that he had accessed Acxiom and removed databases. He then solicited for help online to organize the sale of this stolen data. Detectives caught Baas after finding chat transcripts on the computer of another suspected hacker. In those logs, Baas told the hacker that he had access to the Cincinnati Bell database.

That information led detectives to file search warrants for Baas' residence, where they found CDs containing information about Acxiom's clients and customers. Forensic investigation concluded that the hack on Acxiom had taken place from Baas' home computer from Dec. 10, 2002, to Jan. 2, 2003. Acxiom was unaware of the breach until contacted by authorities.²

The Baas example is the typical perception of an ID theft attack – a "skilled" hacker attacking from outside the organization. Statistically speaking, however, most successful ID theft exploits are carried out by trusted insiders with ready access to aggregate sources of consumer information*

*Source: The United States Secret Service joint study with CERT "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector" August 2004

² Source: Associated Press



Case in point: the arrest of Phillip Cummings, a former employee of Teledata Communications in Long Island, NY, in November 2002, for stealing the personal information of approximately 30,000 individuals over a period of three years. Teledata provides hardware, services, and technical support to the three major credit bureaus (Equifax, Experian, and TransUnion). All lenders in the U.S. use at least one of these credit bureaus to produce credit reports on their customers. As a helpdesk employee, Mr. Cummings was easily able to obtain access to Teledata's client companies' customer databases. He and an accomplice used legitimate passwords and user accounts to run credit reports on thousands of individuals, and then sold the personal information to identity thieves, who used it to obtain loans, open new lines of credit and hijack bank accounts. Millions of dollars were stolen from the unsuspecting consumers over the course of a few months; it was not until several client organizations reported continued billing discrepancies that an investigation led to the discovery of the fraud.

Again, this kind of exploit against an organization by a trusted insider is hardly an isolated incident. In early 2003, Marie Louissaint, an administrative assistant in loan registrations for Weichert Financial Services in Newark, NJ* allegedly stole over 3,700 consumer credit profiles and used the information to rent multiple apartments, create fake driver's licenses, establish lines of credit, and fraudulently purchase thousands of dollars' worth of computing equipment and electronics.³

An unnamed "disgruntled" employee of ThruPoint*, a global networking consultancy, gained unauthorized access to a server containing proprietary corporate records (including the personal information of a number of employees), and distributed those documents to a group of former employees, who then published it on their own Web site.⁴

Hundreds of similar incidents have been reported since 2000, but these attacks are not always high-tech nor are they confined to the financial services industry. One method of illegal data collection popular at restaurants, bars, and nightclubs is the use of "skimmers". A skimmer is a device about the size of a credit card. In a typical exploit, the criminal will buy off a waiter in a restaurant. When the customer surrenders a credit card to settle the bill, the waiter runs it through the skimmer, which stores the information from the magnetic strip. Waiters can often gather as many as 50 - 100 credit cards a night, and a \$50-per-card incentive is often too tempting to ignore.

Tips for Protecting Sensitive Data

Classify such customer and employee data as sensitive. Apply sensitive data handling protocols to this information.

Access to Social Security numbers is often the simplest and most lucrative means of attack, and an employee in any type of organization that has access to consumer Social Security information can use it or sell it to criminals. Once the Social Security number is obtained, the possibilities are almost limitless. The first step is often setting up dummy bank and savings accounts. The very presence of the account will often prompt the bank to give the criminal a credit card, and then the spending spree begins.

This is a nightmare scenario for consumers. Depending upon the extent of the fraud, it can take years for an individual whose identity has been compromised to resolve disputes, correct errors and complete paperwork necessary to restore proper identity and a decent credit rating.

³ Source: Associated Press, May 1, 2003.

⁴ Source: Silicon.com June 23,2003.



Business suffers as well; the financial impact of stolen credit cards alone can be staggering. Consumers are protected by a \$50 liability cap on stolen credit cards; many card issuers offer consumers zero liability in case of theft. That leaves business to pick up the tab for millions of dollars in fraud each year.

Bracing for Impact

The impact on business and consumers alike has drawn the attention of Federal and state government. The FTC provides some minimal ID theft guidance for business on its Web site, but it is limited to advice for dealing with breaches after the fact. There are several ID theft/consumer data protection bills currently in Congressional committee or before the U.S. House of Representatives, including HR.2622, revisions to the Fair Credit Reporting Act.

The State of California, however, was the first to come forward with legislation designed to proactively protect the consumer from ID theft; it was in response to a serious security breach in April 2002. Hackers had broken into the payroll database for the State of California and collected names, Social Security numbers, and payroll information for over 260,000 state employees. The breach went undetected for over a month, and the employees were not notified for an additional 2 – 3 weeks. During that time, attempts had been made to fraudulently access the bank accounts and credit cards of several of the employees.⁵

In July 2003, CA SB 1386: the Database Breach Notification Security Act went into effect. It applies to all organizations doing business in California, or storing records of consumers, customers, or employees that are California citizens. Such an organization must now notify those individuals if it experiences a breach in security to the extent that the database was compromised, and records were, or may have been, exposed. There are two exceptions; one for organizations that do not use computers, and the other for organizations that encrypt the database files in storage – as long as they can prove that the encrypted data was not compromised. Organizations must notify these individuals of the danger to their information within a reasonable (though non-specified) timeframe.

Surprisingly, there was a strong reaction from the business community, particularly the financial services industry, against this legislation. It was originally perceived as unduly burdensome because of the hard costs associated with notification, and the soft costs associated with potential loss of reputation and market share.

This legislation, while not perfect, is good for both consumers and business, simply because 'forewarned is forearmed'. When consumers are notified immediately following a breach, they can begin to check credit statements and reports, check for unusual bank account activity, and notify

Tips for Protecting Sensitive Data

Classify such customer and employee data as sensitive. Apply sensitive data handling protocols to this information.

Grant employee access to such data based on job function, and for specific purposes only. Apply the principle of least privilege when granting access. Review access and privilege on a regular basis, to account for employee turnover and changes in job status and function. Perform background checks on employees that will have access to sensitive data prior to employment or promotion.

⁵ Source: New York Law Journal <http://www.akingump.com/docs/publication/533.pdf>



relevant third parties of the potential exposure. This will limit the time and the amount of funds available to the criminal to perpetrate fraud, thereby reducing the potential liability for merchants and financial institutions alike, and dramatically reducing the impact to the consumer. Since the bill went into effect, there have been no public large-scale breaches that would trigger the notification process reported.

Tips for Protecting Sensitive Data

Restrict physical and logical access to this data. Make certain that it is stored on isolated internal network segments. Encrypt data in storage as required by law.

Success at state level prompted the introduction of similar Federal legislation by Dianne Feinstein (D-CA). In her bill, S1350: the Notification of Risk to Personal Data Act, she proposes that any organization engaged in interstate commerce which stores personal consumer information in electronic format must notify that individual in case of a security breach in which that information was accessed by an unauthorized third-party.

While the California legislation was a good first attempt by a state to notify and protect consumers, it was by no means comprehensive, and cannot be reasonably co-opted at the national level. There are many holes in the proposed national legislation as it stands:

- 1) The bill is limited to data in electronic format. There is nothing governing database printouts, removable media, files stolen from off-site storage, etc.
- 2) The bill does not specify an appropriate timeframe for notification to take place. Notification made "as expeditiously as possible" is too broad and subjective in scope.
- 3) The bill is punitive. It focuses primarily on actions against organizations that fail to comply.
- 4) The bill does not contain basic information security provisions. It does not require affected organizations to monitor their networks or Internet perimeter for unusual activity or to detect security breaches. It does not instruct organizations on securing personal information, nor does it set forth 'minimum necessary' requirements for so doing.

In addition to Senator Feinstein's bill, Senator Jon Corzine (D-NJ), has proposed amendments to the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. In S1633: Identity Theft Notification and Credit Restoration Act of 2003, he proposes that financial institutions be required to notify affected consumers, credit reporting agencies, and appropriate law enforcement in the event of a breach of security and access to personal information by unauthorized third parties. This bill would also apply to service providers and other third parties that maintain personal information on behalf of the financial institution. The bill contains other provisions regarding the notation of fraud alerts in consumer credit reports.

Unlike the Feinstein bill, S1633 does not center on criminal penalties associated with non-compliance, although it does allow for a private right of action for consumers adversely affected by the exposure of their personal information. More importantly, the bill does not limit breaches to databases or information in electronic format, but applies to breaches of personal information in general, which would include data in all forms of media. Unfortunately, this bill applies only to financial institutions and their business partners.

Of all the Federal legislation currently pending, however, the Corzine bill is strongest because it directly references existing Federal mandates for information security.



In fact, the Federally-regulated industries have made some good progress in holding organizations responsible for the protection of personal consumer information. The financial services industry, in particular, has had seen success in certain segments with the Financial Services Modernization Act of 1999 (also known as Gramm-Leach-Bliley or GLB). This Act, which went into effect in July 2001, requires financial services organizations to maintain the privacy and confidentiality of their customers' personal data. Financial institutions, directly regulated by banking agencies and credit union authorities, are further charged to protect such data from theft, misuse and unauthorized alteration. These organizations are required to apply specific security control measures to customer data, including controlling employee access to customer data by job function, performing background checks on employees that require access to customer data, encrypting customer data in transit and in storage, implementing change control policies and procedures to ensure that data is not corrupted, implementing incident response procedures in the event of an attack, and monitoring customer systems for unusual activity. These requirements provide the basis of a solid security foundation for the corporate computing environment.

The health care industry has similar provision for protecting consumers' personal and medical information. Under the Health Information Portability and Accountability Act (HIPAA), the Security Standard requirements are even more specific and stringent than what is required under GLB. They include physical and logical data access control, background checks on employees, encrypting customer data in transit and in storage, change control management, incident response and disaster recovery plans, monitoring system use, data handling policies and procedures, and application criticality analysis.

HIPAA and GLB represent a new trend in Federal regulation; they focus on information security risk management. This includes traditional technical security measures, but also makes provision for physical and administrative security protections as well. Ownership of and responsibility for information security is moving from the IT department to senior management, with the goal of mitigating risk across the enterprise. These security regulations share two other key elements that make them unusual:

- 1) Traditionally, Federal regulation and guidance has focused on protecting corporate data assets and the corporate computing environment. These new regulations, however, are specifically focused on consumer confidentiality and protecting their personal information. The organization is held directly responsible for appropriately protecting the data for the benefit of the consumer.
- 2) These regulations also hold directly-affected organizations responsible for their business partners and other organizations with whom they share customer data. HIPAA and GLB have provisions whereby service providers, data processors, data warehouses, billing organizations, etc., are held accountable through contract or service level agreements to maintain the confidentiality of and providing security protection for customer data that they process and/or store. By default, these regulations are spreading into other industries, following and protecting the flow of data through all points of transaction and storage.

In short, these regulations extend the duty of care that these industries and their allied partners owe to their consumers to include the protection of personal information.



Organizations in the health care and financial services industries are successfully protecting their consumer data, and will be well-positioned to comply with future state and Federal ID Theft legislation. But for those organizations outside these two industries, which are already subject to CA SB1386, or those that wish to take a proactive stance on ID Theft, where can they turn for guidance in implementing similar safeguards for security and confidentiality?

Fortunately, there is no shortage of best-practice documentation and voluntary security standards that any organization can employ to protect consumer information and improve the overall security posture. At minimum, organizations can take a few simple steps immediately to improve data security:

- Classify customer data as sensitive
- Create or revise sensitive data-handling policies and procedures to include items such as:
 - Limiting access to customer data based upon job function
 - Locking file drawers and cabinets that store customer data printouts
 - Securely destroying customer data on all forms of media—formatting discs, diskettes and tapes; shredding printouts and paper files, etc.
- Keep customer data available on the public-facing Web server only as long as needed (presumably the length of the transaction)
- Routinely patch the Operating System on the Web server
- Pass customer data from the Web server to a database server
- Locate the database server on an isolated internal network segment
- Limit physical and logical (electronic) access to the database server by:
 - Restricting logical access to customer data through authentication measures
 - Routinely reviewing user accounts and privileges, in order to accommodate staff turnover and changes in job function
- Perform background checks on employees that have access to customer data
- Enable logging on critical systems
- Routinely review logs for unusual activity
- Employ intrusion detection systems (IDS)

Finally, the organization must implement an incident-response plan to deal with unauthorized intrusion into the corporate computing environment and/or breaches data security. The incident-response plan must include definition of an “incident,” identification of key personnel, notification and escalation procedures, and procedures for notifying law enforcement of the breach. If the organization is subject to CS SB1386, the response plan must also include provisions for notification. In order to be effective, the plan must be periodically reviewed, so that information remains current, and tested at least once annually.



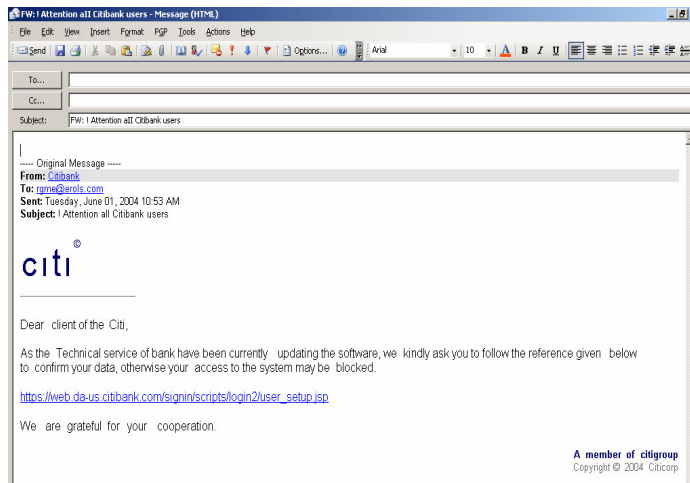
Go Phish!

Such protections are appropriate and effective when an exploit or attack takes place inside the corporate computing environment. The most lucrative and fastest-growing source of identity theft, however, takes place outside of the network and without the organization's knowledge. Phishing is by far the easiest and most profitable form of ID theft, and criminal activity in this area has risen dramatically in the last two years. According to the Anti-Phishing Working Group, these exploits have seen a monthly growth rate of 52% in 2004 alone.

Phishing attacks use spoofed e-mails and fraudulent Web sites that are designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By "hijacking" the trusted brands and respected reputations of well-known banks, online retailers, credit card companies, government agencies, and other organizations, phishers employ simple social engineering tactics to gain consumer confidence and collect personal information. Phishing attacks range from the clumsy and obvious to the clever and sophisticated; well executed phishes are able to convince up to 5% of recipients to respond to them⁶. To put that in perspective, legitimate organizations using email as a marketing tool consider a 0.2 –0.4% response rate is average, and a 1 – 3% response rate very successful.⁷

Tips for Protecting Sensitive Data

Take threats seriously. If contacted by a group or individual that claims to have accessed sensitive data (usually for purposes of blackmail), contact law enforcement immediately. In many previous cases, these threats have been legitimate.



Would Citibank really send this?

⁶ Source: Anti-phishing Working Group June 2004 Report

⁷ Source: Anti-Phishing Working Group June 2004 Report



Dear [REDACTED],
Federal Deposit Insurance Corporation

As use of the Internet continues to expand, more banks and thrifts are using the Web to offer products and services or otherwise enhance communications with consumers.

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct banking business, any day, any time. However, safe banking online involves making good choices - decisions that will help you avoid costly surprises or even scams.

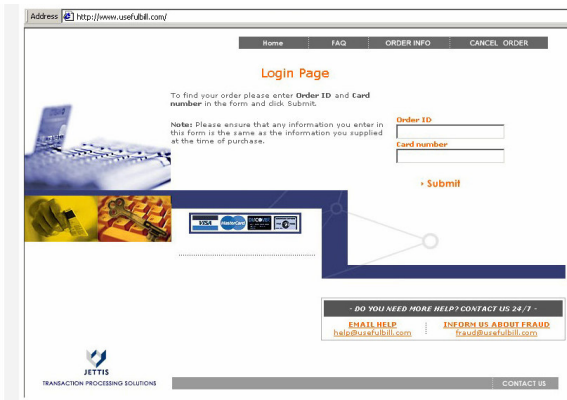
Due to concerns, for the safety and integrity of the FDIC community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in Bank account deletion. This notification expires on September 15th 2004.

Once you have updated your account records your Bank Account will not be interrupted and will continue as normal.

Please follow the link below and renew your account information.
http://www.fdic.gov/register/cgi-bin/fdc_intsafe/register.jsp

Would the Federal Government really send this?



Some phishes are not that easy to spot.

Unfortunately, there is little that a target organization can do to protect itself and its customers from being the target of a phishing exploit. Phishers collect lists of email addresses from a variety of sources, set up fake Web sites for data capture, and run the attacks for only a few days – by the time a target organization finds out that its name or brand has been used for a phish, the attackers may have already abandoned their Web site and covered their tracks. Most organizations that have been used as phish bait, however, do offer assistance to those customers that have unwittingly disclosed personal information. The FTC offers guidance for target organizations in dealing with their compromised consumers; in general, the target organization should:

- 1) Contact the FTC immediately to report that it is being used as phish bait



- 2) If the organization has solicited the collection of personal information from customers via email in the past, cease doing so immediately
- 3) Post a notice on its Web site that it has been used as phish bait (such notices should contain details of the phishing attack)
- 4) Send emails to customers, warning them of the phishing attack
- 5) Set up a spoof@organization.com email contact address for customers and consumers to submit the phish emails or details regarding the attack (collection of evidence may be helpful in pursuing the attacker).

Several work groups and consortia in the financial services industry are working to define technical and operating requirements for counter-phishing measures, but realistically, at this point, there is little else that the target organization can do. It is as much a victim of the phishing attack as is the consumer, as its brand and reputation suffer in the aftermath. Because the attacks take place outside of the corporate computing environment, the organization is not liable for consumer protection under the Fair Credit Reporting Act. The organization may never come into contact with the attacker, and fraudulent transactions made with stolen credit cards or originated from stolen Social Security numbers do not pass through the network. The target organization, therefore, has no transaction records or documentation to provide to the consumer as required in other instances of fraud under FCRA.

Finally, there is another victim in the phishing attack that few recognize. Phishers must conceal their identities and their location, leaving as little forensic evidence as possible to avoid being traced and discovered. Most phishers will therefore hijack poorly protected Web servers to “host” their phishing sites. These sites are often very simple – nicely executed graphics supporting one or two web pages driven by a data collection agent. A small Web site placed on a large capacity server can go undetected if the server’s legitimate owner is not particularly vigilant. Such phishing sites run non-port 80 traffic, typically using ports 4903 and 4901, which have actually become known as the “phishing” ports. Phishers hack into a poorly-secured server, set up the fake site, send out their emails, and run the collection for short periods of time – usually 2 – 4 days. If the attack is traced, it leads to a DNS and IP space owned by an innocent third party.

As responsible cyber citizens, there are some simple protections that organizations can apply to their Web servers to be a less attractive as “host” to phishers. In general, organizations should:

- Use reputable Internet Service Providers (ISPs) (cut-rate providers often offer less-than-the best service and security)
- Use dedicated servers for their Web sites, rather than operating in a shared hosting environment (security is more difficult to control in a shared environment)
- Employ a firewall – correctly
 - Adopt the principle of default-deny for both ingress and egress
 - Close all ports not in use
 - Turn off all services not in use
 - Routinely examine Web logs
 - Closely examine unusual traffic and/or usage



Though simple and, for the most part, low cost, these protections would make it that much more difficult for a phisher to successfully compromise the server and run an attack. If nothing else, the organization can at least close the phishing ports for minimal protection.

Ultimately, the containment of phishing exploits depends upon the behavior and vigilance of the consumer. As phishing attacks become more clever and sophisticated, it becomes increasingly difficult to discern the attacks from legitimate communication. Target organizations can only be appropriately reactive in the wake of a phishing attack, but all organizations can protect their Web servers to avoid becoming an unwitting host.

Conclusion

Given the state of the interconnected eBusiness environment, it is reasonable for any organization to anticipate threats to its environment and data. There is no longer any stigma associated with the breach itself; what is important is how the organization handles that breach. Often times, a set of simple, synergistic control measures can quickly and significantly reduce the risk of a successful exploit of critical assets and data. A good incident response plan can help minimize the damage to the organization. Had Egghead.com employed a few of these simple protections, they might have saved their consumers from harm and themselves from disaster.

Not all organizations fully appreciate their responsibility in maintaining the confidentiality of personal data; not all organizations process, store and destroy consumer information securely. Because of the inherent risks, business can and must take proactive measures to protect data from compromise. At minimum, organizations owe the consumer a certain duty of care, because of the impact to an individual whose information has been compromised and/or identity stolen.

It is the consumer that now bears the brunt of discovering fraudulent activity, reporting it to credit agencies and law enforcement, and cleaning and restoring their credit record. As consumers become more vigilant, and government more involved, the burden will ultimately shift toward the organization to extend appropriate safeguards and custodial care to sensitive personal information, and protect the consumer, and themselves, from harm.

The Cybertrust Approach

Cybertrust is the leading provider of intelligent risk management products and services. As an organization, Cybertrust dramatically improves security and reduces risk by assisting client organizations make better security decisions and maximizing the effectiveness of existing security personnel, processes and technology. Currently, Cybertrust has two offerings that can assist client organizations with information security management.



Cybertrust's Risk Commander

Cybertrust's Risk Commander is a compliance management and risk analysis application that enables client organizations to effectively direct and track progress toward compliance with information security regulations, standards and practices, and to demonstrate overall risk reduction across the enterprise.

Risk Commander provides a single interface to monitor information security compliance. It allows the client organization to:

- Manage the compliance program accurately and consistently
- Produce quantitative risk analysis results
- Increase the efficiency of the information security staff; and
- Demonstrate comprehensive compliance effectiveness

Risk Commander offers flexible configuration options so that the client organization can properly manage compliance activities. It has automated the compliance process into three distinct phases:

Data Gathering

Using the Adaptive Survey Module, the organization collects data for specific regulations and standards, as well as its own corporate security policies. Risk Commander can also automatically import and integrate data from multiple commercial and proprietary asset management, vulnerability scanning, and compliance testing tools. Risk Commander consolidates this data in a controlled, repeatable and efficient manner to ensure consistent data quality.

Analysis

Risk Commander's proprietary automated analysis engine applies rules developed by subject matter experts and compares collected data to standards and regulations to quickly identify compliance issues. Automated analysis helps reduce overall compliance assessment efforts by identifying risks, and producing consistent, measurable results. This allows scarce resources to be directed to the most urgent remediation activities.

Intelligence

Risk Commander's Dashboard and Scorecards deliver quantitative graphical and trend charts that offer at-a-glance insight into organizational performance. User-defined filters help pinpoint compliance issues and vulnerabilities of particular interest. Narrative reports support the overview charts and graphs for in-depth review. Risk Commander's workflow can automatically generate a remediation task for every vulnerability and compliance issue it detects, enabling comprehensive remediation management and oversight.

Risk Commander facilitates access to critical information, by providing

- Immediate Access to Key Reports



- The Dashboard offers immediate access to key tactical and strategic reports for compliance, vulnerability and remediation. Users can customize their Dashboard so it delivers the right information in the right format.
- Flexible Asset Management
The Resource Manager lets you configure the application to fit the organization, allowing the management of technical assets like servers and applications as well as non-technical assets like individuals and physical locations.
- Efficient Data Collection
Risk Commander helps you gather and consolidate information across your entire enterprise. You collect data once and it is automatically applied to multiple standards, saving time and eliminating redundant data capture. You can even assign policies to different business units and divisions as your business needs dictate.
- Integrated Compliance Expertise
By integrating compliance standards, requirements, and controls directly into the application, Risk Commander interprets and clarifies compliance issues, reducing the need for consulting engagements. Based on the client organization's compliance priorities, rating thresholds can be established that fit specific needs.
- Quantitative, Measurable Results
Risk Commander eliminates reliance on qualitative assessments by providing Compliance Scorecards with quantitative results that can directly improve oversight and control. With the intelligent use of automation, analysis can be performed as needed, producing quarterly, monthly, and ad hoc results, with a view of performance trends over time.
- Robust Reporting
Risk Commander's robust reporting capabilities allow easy production of customized reports from the business, technical, or regulatory perspective. Immediate access to such information reduces demands on information security staff.
- High-Level Overviews and Supporting Details
Risk Commander effectively communicates "the big picture" for corporate-level executives through its Compliance Overview, which identifies issues and pinpoints violations. It also provides easy access to supporting details for front-line personnel, including a summary of key compliance elements and remediation details for each issue.
- Enterprise Vulnerability Management
With Risk Commander, multiple sources of vulnerability data can be integrated to provide a comprehensive view of performance. The client organization can also use metrics to compare business units and determine which have the highest level of risk.
- Automated Issue Tracking



The Remediation Scorecard quickly highlights tasks by priority and status so that pending issues are identified and factored into the organization's level of risk tolerance. Risk Commander's automated analysis engine adheres to a closed-loop checking process that compares all remediation tasks against the latest vulnerability and compliance results to confirm that tasks are completed and identify any outstanding issues.

Risk Commander delivers the tools, knowledge, and automation necessary to the client organization to effectively manage enterprise-wide compliance efforts, by

- Bringing information security metrics in line with other disciplines in the organization
- Delivering comprehensive, current, and relevant information to all stakeholders
- Establishing consistent collection, analysis, scoring, and reporting processes across the organization; and
- Demonstrating the value of information security to the organization

Cybertrust's Risk Management Program

Cybertrust's Risk Management Program (RMP), client organizations gain perspective on real information security risks that require action. The process assists with the prioritization and allocation of resources to mitigate those risks and establish a heightened level of confidence conduct to strategic business operations.

TruIntelligence

Effective risk management begins with comprehensive data gathering. Cybertrust's TruIntelligence Security Knowledge Network actively collects and integrates data from multiple sources on a regular basis, both daily and quarterly. With a customer base of more than 700 organizations and locations spread across 30 countries, as well as pre-positioned sensors and monitoring sources around the world, the Knowledge Network gathers data, and actively tracking the most damaging threats and exploits.

Actionable Intelligence

The key to successful information security management is the ability to transform raw data into "actionable intelligence." Cybertrust employs several proprietary models for the analysis of aggregate data, distilling it into real risk information applicable to client organizations. These include a proprietary risk equation, ballistic threat model, and Cybertrust's Risk Index, which delivers an assessment of risk on a global basis, as well as information particular to a single industry or market segment and custom per client organization. Security control strategies and concepts such as early warning and threat analysis systems, policy compliance programs, and essential practices and controls now take actionable form – client organizations actually experience the end result global information-gathering.



Security Management Methodology

Based on its ability to gather data and translate that into actionable intelligence, Cybertrust has developed a comprehensive risk management methodology that integrates a number of critical security activities and disciplines into a formal program that reduces risk and results in a high security posture for the client organization's corporate computing environment. The program incorporates multiple activities including vulnerability assessments of both the externally-facing and internal network environments, physical and human or administrative areas, and the latest, and most popular technical threat vector – wireless. When integrated, these service activities paint a comprehensive picture of an organization's current risk posture, creating a foundation upon which a comprehensive program can be put in place to address deficiencies.

The framework for the program's assessment and remediation process is a proprietary set of standards and control measures known as the Essential Practices, which differ in philosophical concept from what is commonly known as "best practices." Cybertrust's essential practices focus on real risk – risks most likely to be successfully exploited and those risks which will have the greatest impact on the organization – meeting them at an essential level. This establishes a baseline for the organization – practices and controls that must be in place in order for the client organization to function securely. Best practices on the other hand are often too academic, too aggressive to achieve, too expensive, and too impractical; in order to implement and maintain them, the organization would have to devote an inordinate amount of time and money relative to the return on investment, nor an associated increase in the level of the security posture.

Cybertrust's program follows a pragmatic approach that enables customers to achieve significant risk reduction at a fraction of the cost typically associated with enterprise-level security management, and delivers demonstrable results in the form of reporting and certification that client organization's can share with senior management and third parties, such as customers, business partners, and auditors.

The Cybertrust Risk Management Program is a comprehensive and cost-effective approach for reducing risk and addressing compliance pressures. It is delivered to client organizations on a subscription basis, allowing them to keep their security posture current, and providing them the reliability of continuous and dynamic testing and evaluation. Cybertrust stays with its client organizations, facilitating maintenance, advising on new and emerging threats, and assisting in the ongoing management of information security over time.

For further information about these or any of the Cybertrust products and services, please visit the Web site at www.Cybertrust.com, email info@Cybertrust.com, or call directly 1-888-396-8348.

Resources

Federal Trade Commission	
http://www.ftc.gov/	www.consumer.gov/idtheft/
Private	
Anti-Phishing Working Group www.antiphishing.org	ID Theft Center www.idtheftcenter.org
Credit Bureaus	
Equifax www.equifax.com	Experian www.experian.com
Transunion www.transunion.com	