

Summary & “Moving Forward” Issues
from a
Critical Infrastructure Protection Program Workshop
on
Cybersecurity & Liability

Friday, 20 July 2007
Dean’s Suite
George Mason University School of Law

Introduction

On July 20, 2007, the Critical Infrastructure Protection Program (“CIP Program”) at the George Mason University School of Law held a workshop on cybersecurity and issues associated with liability. Those attending the invitation-only workshop were representatives of academia (law, economics and public policy), the US Congress, the federal government, think tanks and trade associations, and senior level executives of major insurance underwriters and reinsurance companies. A focus of the workshop was how the insurance and reinsurance industries measure and assess the cyber risks of firms seeking to mitigate their exposure to cyber-related losses.

This paper provides an overview and assessment of the workshop, and suggests steps that might be taken going forward to promote higher levels of cybersecurity awareness and protection. Reinsurers and insurers (“the industry”) may play a crucial role in advancing the state of cybersecurity practices of the Nation’s businesses. To use an analogy from the “bricks and mortar world”, the industry has played a vital role in advancing the physical security of buildings, assets and people through the development of building and safety codes and product standards. Progress – risk reduction – has been documented through data and information often required by contractual and regulatory structures. However, at this time, there are several impediments to creating a similar, economically viable market for cyber insurance/reinsurance, most of which are associated with identifying and measuring cyber risks. As one participant remarked, the state of the industry’s knowledge in writing policies for cyber risks does not readily transfer from its 150-plus years of experience in the bricks and mortar economy, and “cyber underwriting remains an art rather than a science.” Another attendee pointed out a significant distinction between cyber and conventional physical risks: “Ordinarily, a fire in Cincinnati doesn’t burn buildings in Indianapolis,” but “cyberfires” in one location can and do burn first parties and third parties often in multiple locations and sometimes across legal jurisdictions.

Structure of the Market

The insurance/reinsurance market for cyber liability is relatively immature and evolving, starting some ten years ago with a focus on “dot-com” types of exposures. Insurance/reinsurance has the potential to become an important tool in protecting vital data/information systems and networks, thus increasing the overall security of the nation’s economy. Currently, however, “cyber insurance” is a catch-all term for many different kinds of insurance, covering both first-party and third-party risks such as damage from computer malfunctions, viruses, network outages or congestion, external hacking, internal sabotage and theft, web content liability, copyright infringement, and other areas of potential loss related to technology. Companies often found that their losses in these areas were not being covered by their existing business insurance, and the courts passed conflicting judgments on where cyber-related liability resides. Insurers usually responded by narrowing the terms of ordinary liability and property insurance, and sometimes offered a new product that covered these nascent cyber issues.

Comparable Markets: Other insurance products illustrate how new risks, or perceptions of risks and responsibilities, can change markets. For example, when legal liability for environmental harm first arose, insurers fought coverage because the risk had not been calculated and premiums had not been collected to cover the loss. After the initial shock, insurers began to offer environmental risk insurance, which evolved from a small niche offering in the 1960s to an accepted facet of business risk to be covered today. However, this only happened because government statutes and regulation set standards, making loss calculation possible and widening the risk pool to the point that insurance was profitable to offer. At the same time, regulatory standards and associated business reporting requirements provided data and information needed by the industry to model and appreciate risks and to develop appropriate environmental liability products. In the field of property insurance, the idea that a building can and should be insured against a range of risks has become so commonplace that building codes now parallel the standards for insurability. Such is the potential with cyber liability.

Around 2003, carriers began to expunge the dot-com “internet language” from policies and, driven largely by major events/litigation¹ and new state privacy laws, issued approximately \$350 million in total cyber liability coverage by late 2005. While the market has grown in dollar volume over the last decade, cyber liability insurance remains a very small and unsustainable slice of the industry’s portfolio. Several impediments to growth of the market – and thus higher levels of cyber protection – were identified and discussed:

- In many larger companies, cybersecurity issues have not emerged “from the server room into the board room.” (i.e. Business continuity and risk managers are not aware of the need to buy cyber insurance, and IT managers all think that their own security is adequate. Nonetheless, companies have lost millions of dollars in data losses and other cyber liabilities.)
- Corporate accountability for cyber liability has been unclear, and in smaller firms “O-Level” structures (chief security officer, chief risk officer, chief information officer, *et al*) often do not exist. Such small business can store large amounts of data (e.g. patient information, individually identifiable customer data, etc.), yet do not know that they thus have a cyber-liability or how to minimize it.
- Consensus on what constitutes “best cyber practices” is fragmented across industries.
- Lack of demand for cyber liability products also is inhibited by lack of a comprehensive body of cybersecurity standards.
- The nature of cyber threats and thus risk evolves at an extremely high velocity.

¹ *E.g.*, Ingram Micro, AOL v. St. Paul, Seagate v. St. Paul, Choicepoint, and TJ Max.x. “Nutshell” summaries on these cases are provided as a supplement to this document.

Cybersecurity Metrics

Issues associated with cyber metrics were raised frequently and throughout this workshop. A facilitator read a quote from a transcript of a previous CIP Program event that neatly framed the metrics issue:

Issues of homeland security are of critical importance, but concerns should not be exclusive to government agencies and entities. Like first responders, when bad things happen people immediately look to the government or the insurance/reinsurance industry to maintain or preserve liquidity. The private sector has a critically important role to play in emergency preparedness and in ensuring that our national infrastructure is as secure as possible. The government has data, the scope of which is difficult to imagine. If we could develop a way to work with the government to mine [that data] effectively, we can build even more sophisticated models that will help to provide insurers and reinsurers with additional confidence. [Mr. Harrison Oelrich of Guy Carpenter & Company, 27 September 2006]

Metrics are data and information that, if readily available, would inform the industry, its actual and potential clients, and policymakers about cyber risks. Over time, cyber metrics could form an actuarial body of data that would allow the industry to produce accurate models for, and thus define and price, cyber insurance coverage. This data would facilitate a better understanding of risks, predict behaviors associated with cyber threats, and even construct models of catastrophic “cyber-hurricanes.” More importantly, the availability of cyber metrics allows improvement over time to be measured and drives the development of better cybersecurity standards and practices. Workshop participants discussed the following questions:

- What kinds of data are needed?
- Is the data being collected?
- If so, what entities are collecting the data and are there restrictions on industry access to the data?

Though workshop attendees did not pinpoint specific answers to these data questions, anecdotes discussed during the workshop strongly suggest that data that is “cyber-analogous” to the kinds of “bricks and mortar” actuarial metrics upon which the industry has historically relied and used either is not being collected or currently is not accessible to the industry. Data might be available from cyber devices and networks, but it may be technically difficult or too costly to collect. One participant suggested that the cyber metrics challenges were reminiscent of problems faced by the electric power industry in collecting and providing data that enables modeling and post mortems of large disturbances and outages.² One attendee noted that the manufacturers of cybersecurity software and appliances often incorporate automatic-remote threat reporting into their products. It was suggested that the industry might seek partnerships with these manufacturers so that the industry could have conditional, secure access to *aggregated* threat reports. Such information might allow the industry to see the intensity, duration, frequency, location (jurisdiction), nature and resolution of cyberthreats. Such aggregated data also may have uses in modeling.

In addition, for certain types of risks the data does not exist because the relevant event has never occurred; as with terrorism data in general, insurers lack and will continue to lack meaningful data on a large-scale successful terrorist cyberattack. If the industry had better data on non-cataclysmic losses, however, it would be possible to model larger attacks using methods now employed by reinsurers and risk management groups.

² The US – Canada Task Force’s report on the August 2003 outage that hit the northeastern US and Canada provides an excellent examples of the impediments to obtaining and normalizing disturbance and outage-related data even when it is being collected and maintained by utilities.

Modeling

Professor Kevin McCabe of GMU's Center for the Study of Neuroeconomics ("CSN") and the Mercatus Center made a presentation over lunch during which he suggested a neuroeconomics modeling technique that the industry might consider in lieu of the conventional actuarial data based models. Neuroeconomics is an "experimental study of how emergent mental computations in the brain interact with the emergent computations of institutions to produce legal, political, and economic order."³ Emilia Siravo from Guy Carpenter stated that combining neuroeconomics with game theory might produce cyber liability models that provide value to insurers and reinsurers given the metrics limitations discussed above. Additional discussion of this topic is provided in the final section of this paper, Moving Forward.

Cybersecurity Standards & Professional Certifications

Issues associated with standards and certifications were on the workshop agenda for discussion after lunch, but due to discussion overflow on the luncheon topic, such issues were not thoroughly discussed at the workshop. cursory mention was made of voluntary and mandatory regimes such as COBIT, COSO, ISO 17799 and 27001, NIST, Section 404 of the Sarbanes – Oxley Act, and others. Two participants suggested that as a next step consideration should be given to the mandatory cybersecurity standards that have been developed by the North American Electric Reliability Corporation (NERC) and which will be approved by the Federal Energy Regulatory Commission (FERC).⁴ These cyber standards apply to over 500 entities identified by NERC and FERC as owners-users-operators of the "bulk electric system" and, as such, fall under the scope of new section 215 of the Federal Power Act. A broad spectrum of stakeholders developed the NERC cybersecurity standards by using an American National Standards Institute (ANSI)⁵ process. In the Energy Policy Act of 2005 (EPACT-2005), the Congress specifically required the inclusion of cybersecurity standards in the larger body of electric power reliability standards.⁶ On the same day the workshop was held, the Federal Energy Regulatory Commission (FERC) published a proposal to adopt eight of the NERC Critical Infrastructure Protection ("CIP") cyber standards and further proposed to direct NERC to make specific modifications to other cyber standards. A couple of workshop participants suggested that while statistically significant data and information flowing from these cyber standards may not be available for some time, the insurance/reinsurance industry may find it useful to engage NERC and its members as part of the industry's effort to develop and expand cyber liability insurance.⁷

Another participant suggested that the industry, in its quest for data and information that would better inform the market and models, may wish to examine the role of recognized professional certifications. For example, the industry could identify professional certifications and certifying organizations that are relevant to a company's development and implementation of robust cybersecurity. If these certified professionals could be linked to specific companies (or industries), case studies and models could be developed that advance

³ <http://www.neuroeconomics.net/>

⁴ For more information, please refer to the FERC Notice of Proposed Rulemaking, *Mandatory Reliability Standards for Critical Infrastructure Protection*. 120 FERC ¶ 61,077, 19 CFR Part 39, Docket No. RM06-22-000 (20 July 2007),

⁵ The following is taken verbatim from the ANSI website (<http://www.ansi.org>): "The ANSI coordinates development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. The Institute oversees creation, promulgation and use of thousands of international norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is the official U.S. representative to the [International Organization for Standardization \(ISO\)](#)."

⁶ A summary of the revised cyber standards implementation plan is provided on the NERC website at ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Revised_Implementation_Plan_CIP-002-009.pdf.

⁷ If any workshop participant seeks an introduction to NERC cybersecurity experts, please contact Michael Ebert of the CIP Program at (703) 993-2288 or email mebert@gmu.edu.

cybersecurity's knowledge base. The CIP Program recently completed a review of these and other standards/certifications/risk management issues for a federal agency. We offer to assist workshop attendees with contact information for organizations and selected vendors who set certification requirements and implement training curriculae to those requirements.

Moving Forward

CIP Program Director John McCarthy opened this final section of the workshop by returning to the alternative models theme articulated by Professor McCabe and Emilia Siravo. McCarthy recommended establishing an experimental working group that would employ game theory, neuroeconomics and other concepts to develop a model prototype of cyber insurance markets. Workshop participants who are interested in participating in such a group are asked to call Michael Ebert at the CIP Program, (703) 993-2288 (email mebert@gmu.edu). Experimental models might allow the industry to identify risk categories, market conditions and data needs for different cyber insurance products, thus potentially bypassing the problems identified of unavailable or unusable data. Mr. Leigh Williams of the BITS Financial Services Roundtable and others weighed in favor of further examination and experimentation with “scenario-based game theory models.” If nothing else, working through alternative models may help inform a fundamental data question the answer to which remained illusive at the end of the workshop: *Exactly what kind of data are needed to populate cyberliability models that are acceptable to the industry and its clients?*

Mr. Williams and Dr. Kenneth Friedman of the US Department of Energy also suggested that the insurance/reinsurance industry actively seek partnerships with the US Department of Treasury, the National Labs (specifically DOE's Sandia Lab), and to “talk directly with [the US Department of Homeland Security].” Williams and Friedman⁸ volunteered to facilitate these partnerships, and McCarthy offered the possibility of using an existing CIP Program contract vehicle with DHS as another possible means to engage the agency and its sector specific critical infrastructure planning elements. Time is of the essence, as the Sector-Specific Plans are slated to be sent to the White House around the first of September.

Michelle Boardman, Assistant Professor of Law at George Mason University School of Law who holds both practitioner and government experience, notably with insurance and contract law, suggested that central to the future of cybersecurity third-party insurance, both for gathering data and modeling, is the ability of insurers to forecast how liability for breaches of security will be assessed under the law. In the absence of clear industry standards or legal/regulatory requirements, courts may find that businesses are not liable in tort because their security systems met a bare minimum of industry practice. Moreover, this uncertainty about the finding and amounts of liability make it difficult for insurers to forecast loss amounts and frequency. The insurance industry should consider leading the way in setting standards for cybersecurity. Leadership could take many forms. Initially, insurers could require certain standards of their policyholders in order to maintain cybersecurity coverage and favorable rates. Insurers could offer to certify those with coverage who meet these goals and such certification might have value in assuring the public that a business is responsible. Moreover, while the industry is hesitant about seeking particular governmental standards, where standards will inevitably be adopted, the industry should contribute its knowledgeable views to their formation.

Another suggestion made is to examine the “14 FTC consent decrees” as being possible sources for developing a cybersecurity best practices template. Lastly, several participants urged the industry to very carefully consider whether the political, policy and technical environments would support an industry-backed federal legislative initiative to engender a regulatory framework for cyber. Seeking this kind of federal intervention may be premature and/or produce unintended results.

⁸ Dr. Friedman may be contacted at (202) 586-0379 or email kenneth.friedman@hq.doe.gov.

American Online, Inc. v. St. Paul Mercury Insurance Company

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

347 F.3d 89; 2003 U.S. App. LEXIS 20928

May 6, 2003, Argued
October 15, 2003, Decided

This is an appeal by AOL seeking review of an order of summary judgment in favor of St. Paul Mercury insurance company. After AOL released a new version of access software many consumer class action suits were filed alleging that the software altered their software, disrupted their network connections, caused the loss of stored data and caused their operating systems to crash. St. Paul Insurance company denied coverage, claiming the damages claimed by the consumers were not "property damage to tangible property" as defined by the policy. The district court granted summary judgment to the St. Paul on the grounds that the consumers' underlying complaints did not allege physical damage to tangible property and that any damage from loss of use of the computers as tangible property fell within the impaired property exclusion. The court affirmed the summary judgment, concluding that the complaints involved software problems and software and lost data are not "tangible property," stating that coverage for consumers' loss of use of their computers was barred.

American Guarantee & Liability Insurance Company v. Ingram Micro, Inc.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF ARIZONA

2000 U.S. Dist. LEXIS 7299

April 18, 2000, Decided
April 19, 2000, Filed

Ingram Micro, a computer products' distributor, obtained an insurance policy from American Guarantee Liability Insurance Company, against all risks of direct physical loss or damage to defendant's property and business income. Ingram subsequently suffered a power outage that disrupted operations; as a result some computers had to be manually reprogrammed due to memory loss. However, their claim for the loss was denied by American. American then filed an action for declaratory relief that Ingram's loss was not covered by the insurance policy. Ingram filed a counterclaim for breach of contract. Both parties filed motions for partial summary judgment. The court granted Ingram's motion and denied American's motion, holding that Ingram's computers were physically damaged under the terms of the policy. The court found that physical damage under the policy was not limited to physical harm to defendant's computers, but included the loss of the computers' use or functionality. Because defendant's computers' data was unavailable, services were interrupted, and the programs were altered, defendant suffered physical damage. This case was distinguished from *Seagate* because Ingram alleged property damage that had to be

repaired, while in *Seagate* the damage caused by the defective product did not damage the entire computer.

Seagate Technology, Inc. v. St. Paul Fire and Marine Insurance Company and Cigna Property and Casualty Insurance Company

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

11 F. Supp. 2d 1150; 1998 U.S. Dist. LEXIS 13322; 98 Daily Journal DAR 11477

May 15, 1998, Decided

May 15, 1998, Filed

Seagate manufactures disk drive storage devices for personal computers and small business machines. Amstad, a UK corporation, purchased Seagate disk drives for its personal computers it began selling in 1989. In 1991 Amstad sued Seagate, claiming that the drives were defective. Judgment favored Amstrad. That year Seagate tendered its insurance coverage claim based on the Amstrad action to St. Paul and CIGNA insurance companies. St. Paul and CIGNA both denied Seagate's claim and on June 7, 1994, Seagate brought suit against St. Paul and CIGNA. Seagate's complaint brought causes of action for breach of contract and tortious bad faith based in part on St. Paul's refusal to defend Seagate in the Amstrad actions. On February 20, 1998, Seagate and the insurance companies each sought summary judgment in their own favor. The court found for the insurance companies, noting that the language of the insurance policies indicated that the duty to defend only arose if the damage or injury alleged by the party suing insured could be read to constitute physical damage to the tangible property of others. The court agreed with insurer that incorporation of a defect into the property of another could not constitute the physical damage to tangible property needed to warrant coverage under the policies. The court found that the Armstrong rule was inapplicable to the case, which involved allegations of defective design or manufacture of a product, rather than an inherently dangerous product. The court concluded that as there were no allegations of physical harm to the whole, the underlying lawsuits failed to allege "property damage" within the meaning of the umbrella policies and insurer thus lacked a duty to defend those actions.

United States of America v. Choicepoint Inc.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA

<http://www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm>

February 10, 2006

Choicepoint, a data management company, settled a controversy with the FTC involving Choicepoint's loss of a large amount of customer data. Choicepoint agreed to a

\$10 million fine and also limited its business activities. This included a ban on the furnishing of consumer credit reports to unauthorized third parties. Choicepoint also agreed to create a system of protections to avoid future incidents. These protections included procedures to review third party applications for consumer credit reports as well as a reasonable system of information security protections for customer data. As the stipulation stated, “at a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures.” This program must also include testing.

Remarks of Lydia B. Parnes¹
Director, Bureau of Consumer Protection, Federal Trade Commission
National Association of Mortgage Brokers
2007 Legislative & Regulatory Conference

I. Introduction

Good morning. I am pleased to be here and would like to thank the NAMB for inviting me to speak today. Home ownership is a part of the American dream. Your industry is an important component of providing that dream to millions of consumers. Our job at the Federal Trade Commission is to make sure that consumers have the tools they need to make knowledgeable decisions, and are not treated deceptively or unfairly in the process. We do that through education – educating both businesses and consumers – partnering with industry, and law enforcement. I look forward to continuing to work with NAMB on our many issues of common interest.

Educating consumers and businesses is an essential part of the FTC’s mission. We have both general information on our web site – www.ftc.gov – and specific information where we notice trends or areas where consumers are confused. One such issue was discussed at the last panel – unsolicited phone calls from mortgage marketers using so-called “trigger lead lists.” Many consumers are confused about why they are receiving these calls; others are concerned that their current lenders are revealing their personal information. To address this subject, the FTC released a consumer alert a few weeks ago, entitled “*Shopping for a Mortgage? Your Application May Trigger Competing Offers.*” The alert describes the process of prescreening

¹ The views expressed herein are my own and do not necessarily represent those of the Federal Trade Commission or of any Commissioner.

based on inquiries. It also tells consumers how to stop receiving these calls if they don't want them: by exercising their right to opt out of prescreened offers and by placing their phone numbers on the National Do Not Call Registry.

And we have made sure that those options are meaningful through enforcement. This past fall, the Commission brought a case against a mortgage services company and a telemarketer based in Maryland for violating the Do Not Call provisions of the FTC's Telemarketing Sales Rule.² The FTC charged that these companies called consumers whose numbers were listed on the Do Not Call Registry to market mortgage products and services. The companies settled those charges for a combined penalty of over \$500,000 and a permanent injunction against further violations.

The Do Not Call Registry has been quite successful – the humorist Dave Barry called it the most popular government program since the Elvis stamp. More than 130 million telephone numbers have been registered since 2003. Most entities covered by the DNC Rule comply with the law. For those who do not, tough enforcement is a high priority for the FTC.

Another area of focus for us both in terms of education and enforcement has to do with data security, a top priority for the FTC. We all regularly hear news reports of security breaches exposing consumers' personal information and putting them at risk for identity theft. TJ Maxx, Johns Hopkins University Hospital, and Chase Bank are just a few names from the headlines in the past few months. Identity theft costs consumers and businesses billions of dollars each year. But, it's not just about money – data breaches threaten consumer confidence, both in the business

² *United States v. USA Home Loans, Inc., et al.*, No. 1:06-cv-02850-JFM (D. Md. Oct. 31, 2006); *see* 16 C.F.R. Part 310.

that suffered the breach and in our marketplace as a whole. Many surveys have shown that consumers are less willing to engage in electronic transactions because of the fear that their data will be stolen. For these reasons, it is critical that the business world – and the government – devote the time, resources, and management attention necessary to secure sensitive information.

The mortgage industry is faced with unique challenges in the data security arena. The most serious form of identity theft occurs when a criminal obtains certain sensitive information – like Social Security number, driver’s license, birthdate, mother’s maiden name – and uses that data to open new accounts in the consumer’s name. Of course, your industry *needs* to collect this information about your customers. But, that makes you a tempting target for identity theft. And you may have to keep some of this information for extended periods of time. This means that you must secure data as you collect it, and continually reassess whether your storage methods are adequate as threats and technologies change over time.

The data security challenge can seem daunting, but the Commission has made substantial efforts to help industries like yours meet that challenge. Later, I will summarize some of our education and outreach efforts. But first, I would like to focus on the legal framework governing data security and the Commission’s enforcement program.

II. Data Security Laws

A patchwork of laws govern the confidentiality standards for different businesses and information. For example, the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) protects the confidentiality of consumers’ medical information.³ And the Driver’s Privacy Protection Act (DPPA) limits the sale or disclosure of drivers license

³ 45 C.F.R. Parts 160, 162 and 164.

numbers.⁴

Three federal data security laws are most relevant to your industry. First, the Gramm-Leach-Bliley Act, which requires you to provide annual privacy notices to your customers, also directs you to protect consumers' personal financial information.⁵ The FTC and the federal bank regulators have issued Safeguards rules implementing this requirement.⁶ Second, the Fair Credit Reporting Act contains provisions on the proper disposal of credit report information.⁷ Again, the FTC and the bank agencies have fleshed out these provisions through our Disposal Rule.⁸ Third, the Commission has used the Federal Trade Commission Act, which prohibits unfair or deceptive practices, to act against companies that failed to reasonably protect sensitive consumer data.⁹

Over the past few years, the Commission has brought fourteen data security enforcement actions for alleged violations of these laws and rules. Four of those cases involved mortgage companies, which perhaps underscores the challenges your industry faces in protecting consumer data.

III. Reasonable and Appropriate Measures

The core principle underlying all of our data security cases is that companies must

⁴ 18 U.S.C. § 2721, *et seq.*

⁵ 15 U.S.C. § 6801, *et seq.*

⁶ 16 C.F.R. Part 314

⁷ 15 U.S.C. § 1681, *et seq.*

⁸ 16 C.F.R. Part 682.

⁹ 15 U.S.C. § 41, *et seq.*

implement *reasonable and appropriate procedures* to protect consumers' sensitive information. This is a flexible standard, and allows different types of companies to implement security in ways that are compatible with their organizational structure and operations. It also is adaptable to changes over time – changes in technology, changing threats to data security, changes in a company's way of doing business. The “reasonable procedures” standard also recognizes that breaches can happen despite reasonable precautions. In fact, the FTC has declined to take action against a number of companies that had breaches but had reasonable protections in place.

You may ask what lessons can be learned from the FTC's four data security cases involving the mortgage industry. Let's take a look.

IV. Safeguards Cases

In four of these cases, the FTC enforced the GLB Safeguards Rule. By way of refresher, the Safeguards Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information. How? By developing a comprehensive written information security program that contains reasonable administrative, technical and physical safeguards. The Rule sets forth basic requirements – the financial institution must assign one or more employees to oversee the program; must conduct a risk assessment; must put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; must require service providers, by written contract, to protect consumers' personal information; and finally, must periodically update its security program.

In late 2004, the FTC settled cases against two mortgage companies– Nationwide

Mortgage Group,¹⁰ a mortgage broker in Virginia, and Sunbelt Lending Services¹¹ in Florida – both for allegedly failing to comply with the Rule’s basic requirements for risk assessment and control. The Commission charged that Nationwide stored sensitive customer information on a computer network that was accessible to all employees and accessible through the Internet. And Nationwide did not monitor its network for vulnerabilities that would expose customer information to attack. As to Sunbelt, the FTC alleged that it failed to oversee the security practices of its service providers and loan officers working from remote locations throughout the State of Florida. These cases were not close calls – the FTC alleged clear, specific, and multiple violations of the basic requirements of the Safeguards Rule. The settlement agreements bar the companies from further violations of the Rule and require them to undertake independent audits of their security systems every other year for ten years.

Then, in September of 2005, Superior Mortgage Corporation,¹² a lender with 40 branch offices in 10 states and multiple web sites, settled FTC charges that it failed to provide reasonable security for the sensitive information it gathered from customers. Superior, contrary to statements on its web site, failed to encrypt or otherwise protect sensitive customer information before sending it by email; failed to implement appropriate password policies for company systems containing sensitive customer information; and failed to assess risks to

¹⁰ *In the Matter of Nationwide Mortgage Group, Inc. and John D. Eubank*, (Docket No. 9319) (consent order) <http://www.ftc.gov/os/adjpro/d9319/index.htm>

¹¹ *In the Matter of Sunbelt Lending Services*, (Docket No. C-4129) (consent order) <http://www.ftc.gov/os/caselist/0423153/04231513.htm>

¹² *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) <http://www.ftc.gov/os/caselist/0523136/0523136.htm>

customer information until more than a year after the Safeguards Rule took effect. In other words, it took an approach to data security that was too little, too late.

Finally, in an example of a “low-tech” data security problem, the FTC settled an enforcement action in May of 2006 with Nations Title,¹³ a real estate services company, alleging, among other violations, that the company threw documents containing sensitive consumer information into an open dumpster. Thankfully, the documents did not fall into the hands of identity thieves; they were, however, found by a news reporter. The message is clear: how you get rid of the information is as important as how you store it.

V. Business Outreach

Designing a good information security program is not as difficult as you may think. And the FTC has some tools to help you along the way.

As I mentioned earlier, we offer business guidance and publications on how organizations can protect their customers’ personal data. It’s all available online at ftc.gov/IDtheft. To give just a few examples, we have a publication on computer security to help you identify the most common computer vulnerabilities so you can evaluate your own system to make sure it’s protected.¹⁴ We also have a brochure on the Safeguards Rule, which explains the rule’s requirements and offers specific steps on how to implement them.¹⁵ Should a breach

¹³ *In the Matter of Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens*, FTC Docket No. C-4161 (June 19, 2006) (consent order) <http://www.ftc.gov/os/caselist/0523117/0523117.htm>

¹⁴ *Security Check: Reducing Risk to Your Computer Systems*, <http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm>

¹⁵ *Financial Institutions and Customer Information: Complying with the Safeguards Rule*. <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>

occur, we have material to help you evaluate when and how to notify law enforcement, affected businesses, and individual consumers, including a model letter to send to consumers.¹⁶

Finally, I am very pleased to announce the recent release of *Protecting Personal Information: A Guide for Business*.¹⁷ This brochure articulates five key steps that are part of a sound data security plan: (1) Take stock; (2) Scale down; (3) Lock it; (4) Pitch it; and (5) Plan ahead. Let's talk about what each of those steps entails.

First, Take Stock – you need to know what consumer information you have and who has access to it. What data do you collect? Where do you store it? What do you share with service providers and where do they store that information?

Second, Scale Down – you need to determine whether you really need all the information you gather. Do you need to keep records for completed transactions? Do you use all the pieces of data you collect? Is access to data limited to those who need it to perform their jobs?

Third, Lock It. If you are going to keep it, you have to keep it safe. Electronic security – encryption, firewalls, and other IT defenses – are important, but a comprehensive information security program includes more. Look at the physical security of your building. Do you lock file cabinets, office doors, and outer doors? Are visitors escorted at all times?

Employee training is an extremely important component in your security plan. Employees need to know how to use the electronic and physical security measures in place, and how to avoid old-fashioned scams. A lot of attention has been paid lately to pretexting, though

¹⁶ *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm>

¹⁷ <http://www.ftc.gov/infosecurity>

the practice has been around for a long time. Criminals contact businesses and impersonate their account holders, in order to obtain customer account records. The Commission is currently pursuing complaints against companies and individuals that allegedly obtained detailed telephone records and call information through false pretenses, in some cases posing as a consumer and convincing phone company personnel to send them the records. Employee training should emphasize proper procedures to verify the identity of individuals seeking to obtain business records.

Fourth, Pitch It. You have to make a decision on how to dispose of your information in a secure and timely fashion. Determine how long you need to retain information and then make a schedule for disposing of it.

Too many data breaches have involved information companies no longer needed. Our brochure suggests alternatives for destruction and disposal.

Finally – Plan Ahead. Because security can never be perfect, the last step in creating a sound information security program is to develop a plan for responding to data breaches. Having a plan in place beforehand helps you mitigate effects quickly and in an organized fashion. The FTC provides information to help you determine when it is appropriate to notify consumers their information has been compromised, as well as a model notification letter.

VI. Service Providers

The Safeguards Rule also requires companies to oversee their service providers. You must take reasonable steps to choose and retain service providers that can maintain appropriate safeguards for customer information, and require by contract that they implement and maintain safeguards standards.

Before outsourcing any business function – payroll, web hosting, customer call center operations, or data processing – investigate the company’s data security practices and compare their standards to yours. This applies whether you are outsourcing across town or across continents.

When you are satisfied that the service provider can maintain appropriate safeguards for your customer information, memorialize these standards in your contract. You should also consider including contract provisions that build in the flexibility to revisit standards as threats and technology evolve. After the relationship has been established, include a review of your service provider in the ongoing review of your own security plan.

VII. Conclusion

Creating an effective security plan and fostering a “culture of security” is not complicated, but it does require a commitment. A commitment to security is not only good for consumers, it’s just good business. A recent survey by Ponemon Institute found that the average data breach costs a business about \$4.8 million, and \$180 per lost customer record.¹⁸ And that’s not the end of the loss. Consumers whose information is compromised lose confidence in the company and may take their business elsewhere. One survey found that 20% of consumers who receive a breach notice terminate their relationship with the company, and another 40% say they might.¹⁹

There is no such thing as perfect security. But any business that maintains personal

¹⁸ <http://www.pgp.com/newsroom/mediareleases/2006/ponemon.html>

¹⁹ *Id.*

information about consumers must be proactive in protecting it. I hope my message today has been helpful to you. Working together we can give consumers access to the American dream.

Thank you.



T.J. Maxx theft believed largest hack ever

TJX cos. put number to loss Wednesday, acknowledges it could still go up

By Mark Jewell

The Associated Press

Updated: 11:17 a.m. ET March 30, 2007

BOSTON - A hacker or hackers stole data from at least 45.7 million credit and debit cards of shoppers at off-price retailers including T.J. Maxx and Marshalls in a case believed to be the largest such breach of consumer information.

For the first time since disclosing the theft more than two months ago, the parent company of nearly 2,500 discount stores put a number on how much card data was compromised — and it's a number TJX Cos. acknowledges could go still higher.

Experts say TJX's disclosures in a regulatory filing late Wednesday revealed security holes that persist at many firms entrusted with consumer data: failure to promptly delete data on customer transactions, and to guard secrets about how such data is protected through encryption.

"It's not clear when information was deleted, it's not clear who had access to what, and it's not clear whether the data kept in all these files was encrypted, so it's very hard to know how big this was," said Deepak Taneja, chief executive of Aveska, a Waltham, Mass.-based firm that advises companies on information security.

The case has led banks to reissue cards to customers as a precaution against further fraud beyond cases detected as far away as Sweden and Hong Kong, according to the Massachusetts Bankers Association, which is tracking fraud reports linked to Framingham, Mass.-based TJX, parent company of stores across North America and the United Kingdom.

The only arrests believed tied to the case involve a gift card scam in which 10 people are suspected of buying data from the TJX hackers to purchase Wal-Mart gift cards in northern Florida. The group — who aren't believed to have committed the TJX hack — then used the cards to buy \$1 million worth of electronics and jewelry at Wal-Mart's Sam's Club stores, according to Gainesville, Fla., police.

Information from 45.7 million cards was stolen from transactions beginning in January 2003 and ending Nov. 23 of that year, TJX said in the filing with the Securities and Exchange Commission after business hours Wednesday. TJX did not estimate the number of cards from which information was stolen for transactions occurring from Nov. 24, 2003, to June 28, 2004.

TJX said about three-quarters of the 45.7 million cards had either expired at the time of the theft, or the stolen information didn't include security code data from the cards' magnetic stripes. Starting in September 2003, TJX began masking the codes by storing them in computers as asterisks rather than numbers, the company said.

The filing also said another 455,000 customers who returned merchandise without receipts had their data stolen, including driver's license numbers.

With at least 46 million consumer records accessed, the TJX case outranks the previous largest case tracked by the Privacy Rights Clearinghouse: a June 2005 disclosure by credit card processor CardSystems that hackers accessed accounts of 40 million card holders.

Clearinghouse director Beth Givens said her San Diego-based consumer advocacy organization's list includes data breaches disclosed after a 2003 California law required companies to notify consumers.

The TJX case "will probably serve as a case study for computer security and business students for years to come," Givens said. "This one could be considered a worst-case scenario." One reason for that, she said, is because of TJX's disclosure Wednesday that it believes the hacker or hackers

"had access to the decryption tool for the encryption software utilized by TJX."

TJX also said the hacker or hackers used technology last year that could have enabled them to steal card data during the approval process, when data is transmitted to the card issuer without encryption.

TJX also remains uncertain of the theft's size because it deleted much of the transaction data in the normal course of business between the time of the breach and the time TJX detected it.

"There is a lot of information we don't know, and may never be able to know, which is why this investigation has been so laborious," TJX spokeswoman Sherry Lang said.

TJX says its computer systems were first breached in July 2005 by a hacker or hackers who accessed information from transactions dating to January 2003. TJX didn't find out about the breach until last Dec. 18, when it learned of "suspicious software on our computer systems."

The company then hired outside investigators and notified federal authorities before issuing a Jan. 17 news release. TJX says the monthlong delay in disclosing the breach allowed it to work with security experts to contain the problem.

TJX said in the filing that "substantially all stolen data" from transactions in the period Nov. 24, 2003, to June 28, 2004, were deleted. Lang said the company was investigating why information stolen earlier in 2003 wasn't routinely deleted.

Deleting such information after transactions "should be standard practice" to guard against theft, said Taneja, the security expert, but many firms nevertheless don't follow through.

TJX's filing says the company "does not know who took this action, and whether there were one or more intruders involved."

How far scams like the one in Florida may have spread because of the TJX breach is unknown.

"It's been all over the world," said Bruce Spitzer, spokesman for the Massachusetts Bankers Association. "It's the downstream transactions we've been hearing about," involving thieves who buy stolen data from others, often hackers in other countries.

On Jan. 24, 60 of the 205 banks in the state association reported they had been contacted by credit card companies about cards that had been compromised. The next time the association conducts such a survey, Spitzer expects "it will be near 100 percent" based on recent reports from member banks.

A spokesman for the American Bankers Association said the group had not been tracking such data.

TJX faces an investigation by the Federal Trade Commission, which could fine the company, and lawsuits accusing the firm of failing to safeguard private data.

TJX is the parent company of stores including T.J. Maxx, Marshalls, HomeGoods and A.J. Wright in the U.S., Winners and HomeSense in Canada and T.K. Maxx in Britain.

© 2007 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

URL: <http://www.msnbc.msn.com/id/17871485/>

[MSN Privacy](#) . [Legal](#)

© 2007 MSNBC.com