



Article

Security breach, non-compliance and operational risk: a perfect storm

Mar 01 2007 [IP Governance Task Force](#)

History repeats itself – leaders, time and again, fail to apply available security measures to safeguard commerce, consumers and reputation. This truth is most critical in the world of technology. Those who forget the lessons of history's past are doomed to repeat them. Several moments in history bear out this truism:

1. **The Spanish navy** created the trade routes through the Caribbean to facilitate commerce. Large amounts of gold and silver expropriated from the New World were shipped on these great vessels utilizing the trade routes to transport their precious cargos to the Spanish monarchy. In the beginning security for these trade routes was a minimal concern. It was perceived as an extra expense, for the weight of extra cannons and the cost of utilizing warship escorts was excessive. Yet there were rumors of brazen pirates like El Cid who monitored the trade routes for specific vessels and then, in the blink eye, attacked and plundered the most grandiose of the House of Hapsburg's vessels. The scourge of the Caribbean — marauding pirates — has now exacted its toll upon the high seas of the Internet; hackers have been organizing and perpetuating virtual looting and pillaging for years now.
2. **TJ Hooper**. In 1932, the operator of the tug boat, TJ Hooper, failed to apply a new standard of care and security measure to safeguard its cargo. The company was found negligent at the trial "because they did not carry radio receiving sets by which they could have seasonably got warnings of a change in the weather which should have caused them to seek shelter in the Delaware Breakwater en route." *Lesson learned*: a duty of reasonable care requires adherence to existing standards of care; standards which change as technology evolves.
3. **FTC vs. Nations Title**. Last year, the FTC prevailed in its lawsuit alleging that Nations Title Agency (NTA) made deceptive security claims in their privacy policies contrary to the [Gramm Leach Bliley Act](#). For example, NTA's privacy policy claimed: "NTA, at all times, strives to maintain the confidentiality and integrity of the personal information in its possession and has instituted measures to guard against its unauthorized access. We maintain physical, electronic and procedural safeguards in compliance with federal standards to protect the information." Specifically, the FTC charged that NTA failed to: "assess risks to the information they collected and stored, both online and offline; implement simple, low-cost, readily available defenses to common Web site attacks or implement reasonable measures to prevent hackers from gaining access to their computer network;" amongst other claims. *Lesson learned*: Privacy and security claims can be viewed as false and deceptive if your firm fails to comply with federal standards on safeguarding customer information.
4. **Operational Risks: the Perfect Storm of 2007**. Cyber criminals are accelerating their attacks on common vulnerabilities of the global banking system to fund their terrorism activities despite law enforcement and regulatory agencies' calls for more transparency, disclosure and management of operational risks. On one side of the emerging storm, phishing attacks in the US and UK have accelerated during 2006 with over 50% of US phishing attacks using fraudulent bank domain names. This activity is reflects a failure to effectively implement federal banking regulations on safeguarding bank assets and preventing identity theft. Converging from the other side are operational risks. These are the potential for regulatory fines and/or litigation settlements due to a failure to comply with federal and/or state regulations.

Recent public comments and initiatives from law enforcement and regulators on these issues include:

- The Department of Justice's October 2006 [Bi-National Phishing Report](#) (PDF) delineates the operational risk aspect of the emerging storm with two observations: (1) "A wide range of federally regulated financial institutions in the United States is required to file Suspicious Activity Reports (SARs) with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), whenever they encounter information that indicates a crime affecting a financial institution (including phishing) may have been committed." (2) "Companies that are victimized by phishing may not report these instances to law enforcement. Unlike some other types of Internet-based crime, such as hacking, that may be conducted surreptitiously, phishing, by its nature, involves public misuse of legitimate companies' and agencies' names and logos. Nonetheless, some companies may be reluctant to report all such instances of phishing to law enforcement -- in part because they are concerned that if

the true volume of such phishing attacks were made known to the public, their customers or accountholders would mistrust the companies or they would be placed at a competitive disadvantage."

- Philip Robinson, head of financial crime for the UK's Financial Services Authority. Last December, the BBC reported that Robinson "believed internet banking was generally "safe". But he raised concerns about the banks' apparent lack of transparency when it came to internet fraud. He said they were "wary" about making concerns public in case the information was "misrepresented". They were also reluctant to report incidents to the police, he said, because "the likelihood of fraud being investigated is very low indeed". He said being "open and transparent" was important to "maintain confidence" in the banking system and he would be meeting the Information Commissioner next week to discuss ways of increasing transparency."
- Operational risks and operational losses flowing from identity theft in the February 15 2007 [Basel II Notice of Proposed Rules](#) (PDF) by the US federal financial regulators, or from a breach of privacy, retail customer disclosures, systems security, related hacking damage and theft of information per the June 2006 [Revised Framework of Basel](#) are the subject of new proposed global banking regulations under Basel II from the US federal financial regulators and their peers in the Group of Ten or Basel that include Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, and the United Kingdom. By applying existing federal regulations for safeguarding bank assets from fraud to the battle of identity theft, Boards of Directors can steer their institutions clear of the majority of asset-based identity theft frauds. Alternatively, by ignoring these federal regulations, as standards of care, banks face a fate similar to TJ Hooper with mounting litigation and operational risks.

Cyber Battles and War Plans. Adjusting to real-time battle conditions, where 56% of phishing attacks use fraudulent domain names, and steering a course per the relevant maps issued by regulators for these battle conditions, requires strong Board leadership to chart and implement a new course to preserve the safety and soundness of the financial fleet in cyber space.

In the fog of cyber battles, transparency and accountability is vital for Boards of Directors, CEO's, consumers and rating agencies to have a 360-degree understanding of the safety and soundness of a bank and its information security program. To advance these objectives, the IP Governance Task Force is:

- Establishing an IP Governance Operational Risk Management, Quantification and Rating Model, www.ipgovernance.com. This measures and rates the effectiveness of a bank or credit union in safeguarding its brands and customer identifying information per relevant federal regulations. A case study shows 91 banks and credit unions can safeguard their brands from current infringements and related operational risks for an investment that ranges from .05% of net income for 2005 and 2004, for firms with total assets in excess of \$1 billion, to .77% of net income for 2005 and 2004 for firms with total assets under \$450 million. This investment will minimize the pool of available, matching domain names for future identity theft attacks.
- Establishing the Online Brand Rating. This measures exposure to confusingly similar domain names on a scale of "F" to "A". F ratings mean firms own less than 31% of confusing and infringing domain names. "A" ratings mean firms own 99% of confusing and infringing domain names.
- Recognizing firms with "A" ratings through ProtectingConsumersOnline.com.
- Recommending regular penetration testing of web servers with best of breed tools to mitigate pharming attacks.

It is crucial for firms to apply these standards of care to effectively combat phishing and other forms of identity theft. Such measures will help assure customers that using the Internet for banking, shopping and communications can be a safe and productive means of transaction.

The IP Governance Task Force is a multi-disciplinary team of Intellectual Property professionals providing a coordinated IP Governance solution and competitive advantage for public and private organizations with management, education, advisory, legal, data-mining, remediation, insurance, and rating services. Members include industry thought-leaders from auditing (including prior bank regulatory experience), legal, and technology companies. The Task Force was formed in 2006 to address the safeguarding of intellectual property per federal regulations, primarily in the financial industry.

Related content

Related Articles

- [Business e-mail addresses get Canadian privacy rights](#)
- [TJX reveals larger data breach](#)
- [Vendor Interview: Dave Tilkin, Navigator Consulting Group \(BrokerAudit.com\) document, manage client data and risk](#)

News by Subject

- [Capital and risk](#)
- [Data protection and privacy](#)
- [Systems and controls](#)
- [Financial Crime and Fraud](#)

News by Country

- [Canada](#)
- [United Kingdom](#)
- [United States](#)

External sites

- [June 2006 Revised Framework of Basel](#)
- [Bi-National Phishing Report \(PDF\)](#)
- [February 15 2007 Basel II Notice of Proposed Rules \(PDF\)](#)

Related Rulebooks**[Gramm-Leach-Bliley Act of 1999](#)**

- [Gramm-Leach-Bliley Act of 1999](#)
-