

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

INTERNATIONAL HEADQUARTERS: 425 UNIVERSITY AVE, SUITE 800, TORONTO, ON M5G 1T6 TEL: (416)979-6701 FAX: (416) 979-3030

Toronto, ON

Mountainview, CA

Burlington, MA

<http://www.sterlinghoffman.com/>

Identity Authentication: Willing to Risk Your Reputation on It?

By Andrea Klein, Chief Marketing Officer, IdenTrust, Inc.

Published in The Sterling Report, January 2008



A damaged corporate reputation translates into huge economic losses that span decreased brand value; low share price; lost customers, partners and strategic relationships and difficulty recruiting and keeping top-notch employees. Some businesses, such as Arthur Anderson, never recover. Corporations, and their financial institutions, need to understand that they can and must manage reputational risk in much the same way that they manage other types of risk – through sound strategies, modeling, business intelligence and technology.

All corporations, regardless of their size or industry, inherently manage varying levels of risk. Successful organizations are adept at managing supply chain, market, legal, operational and financial risk using various management tools and models. Many organizations, however, overlook the need to manage reputation risk, which can prove just as – or even more – costly to rectify if compromised.

Business reputations are vulnerable to unsavory business practices, discriminatory hiring and identity/data breaches that weaken customers' trust in an organization or brand. A damaged reputation can cost an organization in terms of decreased brand value; low share price; lost customers, partners and strategic relationships; and difficulty recruiting and keeping top-notch employees. Simply put, losing your reputation translates into huge economic losses. Recovery can take years; some businesses never recover e.g. Arthur Anderson.

Reputational risk as it pertains to security breaches, whether from mishandling of sensitive customer information, phishing and pharming attacks or non-compliance with regulations is a growing concern for corporate boards and their investors. Corporations, and their financial institutions, need to understand that they can and must manage reputational risk in much the same way that they manage other types of risk – through sound strategies, modeling, business intelligence and technology.

The Value of Reputation

In a Financial Times article titled "The Challenge of Protecting Reputation," Professor Paul A. Argenti of the Tuck School of Business at Dartmouth College asks, "Why is it so easy for executives to think about and plan for financial risks, but still so hard for them to understand that intangible risks to an organization's reputation are far more likely to destroy shareholder value?"

Reputation is all about perception. A reputation is tenuous. Reputation is also thought to be difficult to quantify. However, organizations that have seen their good reputations dissolve, and have worked to repair them, can attest to the high cost of restoring a reputation...or, at the very least, restoring the business lost as the result of a single data breach.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

INTERNATIONAL HEADQUARTERS: 425 UNIVERSITY AVE, SUITE 800, TORONTO, ON M5G 1T6 TEL: (416)979-6701 FAX: (416) 979-3030

Toronto, ON

Mountainview, CA

Burlington, MA

<http://www.sterlinghoffman.com/>

The Ponemon Institute, an organization that studies privacy and information management, recently reported that the cost of recovering from a single data breach now averages \$6.3 million. That figure represents an increase of 31% since 2006 and a nearly 90% increase since 2005. Two-thirds of that cost is spent recovering business that's lost after a breach, a cost that has risen 30% since last year. There is no question that it's getting more expensive to replace customers lost as a result of security breaches.

Breaches by third parties-outsourcers – or members of a company's supply chain – were the second biggest cause of security compromises and are more expensive, according to the report. Companies spent an average of \$231 per lost record on third-party breaches compared to \$171 per lost record in 2006.

Tales of the following companies represent nightmare scenarios that would keep any C-level executive up at night:

- Retailer TJX Cos. announced that it will spend \$256 million responding to the company's data breach that compromised up to 100 million accounts. The payments, announced in 2007, include financial settlements to Visa International Inc., banks and customers – as well as costs associated with upgrading the company's information protection processes and technologies.
- American International Group (AIG) received a backlash from the financial community amid reports of suspect accounting and business practices. "AIG, one of the largest insurers in the world, has been rocked...by multiple investigations into its accounting. The company's shares are down more than 16% since it disclosed inquiries by New York Attorney General Elliot Spitzer and the Securities and Exchange Commission on February 14," Reported CBS MarketWatch on July 8, 2005.
- ChoicePoint, Inc.'s market cap dropped by \$720 million following news that identity thieves had gained access to personal consumer information. As a result of the security breach, the identification and credential verification services provider was ordered to pay a \$10 million federal fine, contribute \$5 million to a fund to compensate consumers who suffered from the breach and submit to external security audits for 20 years. Analysts estimate that ChoicePoint will spend more than \$30 million in direct costs associated with the security breach.
- CardSystems Solutions, Inc. was a billion dollar company before its security breach that compromised 40 million consumer accounts. After the breach, the company was acquired by Pay By Touch™ Payment Solutions, LLC. for a fire sale price of \$47 million.

Two Strikes and You're Out...

So just how tenuous is an organization's reputation? Very tenuous, particularly in the banking industry.

According to the Ponemon Institute's 2006 "Privacy Trust Study for Retail Banking," banks are only one or two security breaches away from losing their customers. While 68% of customers give their bank high marks for protecting their personal information, those customers report that only two security breaches would destroy that trust. Thirty-four percent of respondents would transfer their funds after a single security breach; 45% after two security breaches.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

INTERNATIONAL HEADQUARTERS: 425 UNIVERSITY AVE, SUITE 800, TORONTO, ON M5G 1T6 TEL: (416)979-6701 FAX: (416) 979-3030

Toronto, ON

Mountainview, CA

Burlington, MA

<http://www.sterlinghoffman.com/>

Fifty-eight percent of those consumers surveyed said that a security breach would decrease their sense of trust and confidence in the organization reporting the incident. Only eight percent of respondents did not blame the organization that reported the breach. Surprisingly, 12% said the incident enhanced their sense of confidence in the organization.

And if you think the answer to mitigating reputational risk is to keep mum on minor security breaches, think again. According to the Ponemon Institute, more than 82% of consumers believe that an organization should always report a breach, even if the lost or stolen data was encrypted or there was no criminal intent.

The Value of Reputation in Financial Services

While reputation is important for all organizations, it is especially critical for financial institutions. Many financial institutions, especially smaller banks, are not protecting against reputational risk because they cannot quantify or measure the risk. Instead, they focus on familiar risks that are readily quantifiable and easier to protect against, including market risk, credit risk, liquidity risk and regulatory risk.

Increased phishing and pharming attacks – as well as high-profile news stories of security breaches – are having an impact on how customers interact with their financial institutions, according to a 2005 Gartner survey of 5,000 U.S. adults. For example, some online banking customers are changing their usage patterns, including logging in less frequently and no longer using online bill payment services.

These trends have serious implications for financial organizations and other companies that want to use the e-mail channel to communicate more cost-effectively with their customer base. For example, a bill sent electronically costs about half of what a bill costs when sent through the regular mail.

PLOTting an Excellent Reputation

If financial institutions and other types of corporations are only one or two security breaches away from losing customer trust, how they can adequately protect their organizations? A comprehensive approach to IT security is essential – one that addresses physical security of the data, security of the IT infrastructures on which the data sits, as well as security of the data as it flows between systems and organizations.

Corporations and financial institutions have already implemented numerous security measures to address everything from physical access to single sign-on and provisioning. They now need to move their focus to identity authentication – the new front line of the security battle. To have the flexibility to respond to new types of fraud and resulting regulations, a comprehensive approach to identity management needs to incorporate a globally interoperable solution for trusted electronic payments and other sensitive communications.

Early market efforts primarily focused on access versus authentication. Thus, as long as an individual had the appropriate PIN/password or token to enter, he/she would be granted access. This approach has proven to be short sighted. Companies need to understand and vet credentials – understanding how they were granted – before they can rely upon them.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

INTERNATIONAL HEADQUARTERS: 425 UNIVERSITY AVE, SUITE 800, TORONTO, ON M5G 1T6 TEL: (416)979-6701 FAX: (416) 979-3030

Toronto, ON

Mountainview, CA

Burlington, MA

<http://www.sterlinghoffman.com/>

Solutions that simply authenticate the user to the site, and not who the user really is –while good first attempts – simply do not guarantee trust, and only meet basic compliance with Federal Financial Institutions Examination Council (FFIEC) guidelines and other regulations. To provide identity security on the highest level possible, multi-factor authentication is essential across all levels. Multi-factor authentication uses a single, comprehensive solution that cross-authenticates the user with the site, and secures the two through digitally issued certificates. It is also critical to have validation of certificates against a real-time updated list that indicates whether or not the certificate has expired or been revoked. A Public Key Infrastructure (PKI)-based approach incorporates a protocol that provides real-time validation of a user's certificate status.

A comprehensive system for identity authentication requires policies, legal infrastructure, operational consistency and technology (P.L.O.T) for access that users can rely upon. Of special importance are procedures and guidelines that work across multiple institutions and geographic borders. For identity authentication to provide a trusted business environment, Policies (P) regulating the issuance and handling of digital identities and the legal (L) framework that accepts or rejects those identities must be acceptable and enforceable both domestically and across borders. Otherwise, a corporation or its financial institution could face the prospect of adjudicating possible disputes in jurisdictions around the world should a security breach arise, risking that the contracts being relied upon are not binding – an expensive and cumbersome prospect. Additionally, the Operational (O) environment for controlling the back office support for the digital identities and the Technology (T) used to enable access to the networks for validation must also be globally interoperable and consistent.

Corporate executives, learning from the experiences of their less fortunate peers, are recognizing the true cost of a tarnished reputation. The next and more challenging step for many is mitigating reputational risk, especially as it relates to online fraud and data breaches. The good news for the corporations and their banking partners is that they have many tools at their disposal to affect positive change. Just as in operational risk management, however, the key to success is an enterprise-wide, standards-based and standardized approach.

Andrea Klein is the Chief Marketing Office of IdenTrust Inc., the global leader in trusted identity solutions. She is responsible for the company's global strategy, marketing and business development. Prior to her role at IdenTrust, Andrea was the Vice President for Financial Services Industry Strategy and Marketing at Oracle. She has over 25 years of financial industry experience both from her years at Bank of America and her experience building and running a global industry marketing and professional services organization. For article feedback, contact Andrea at andrea.klein@identrust.com