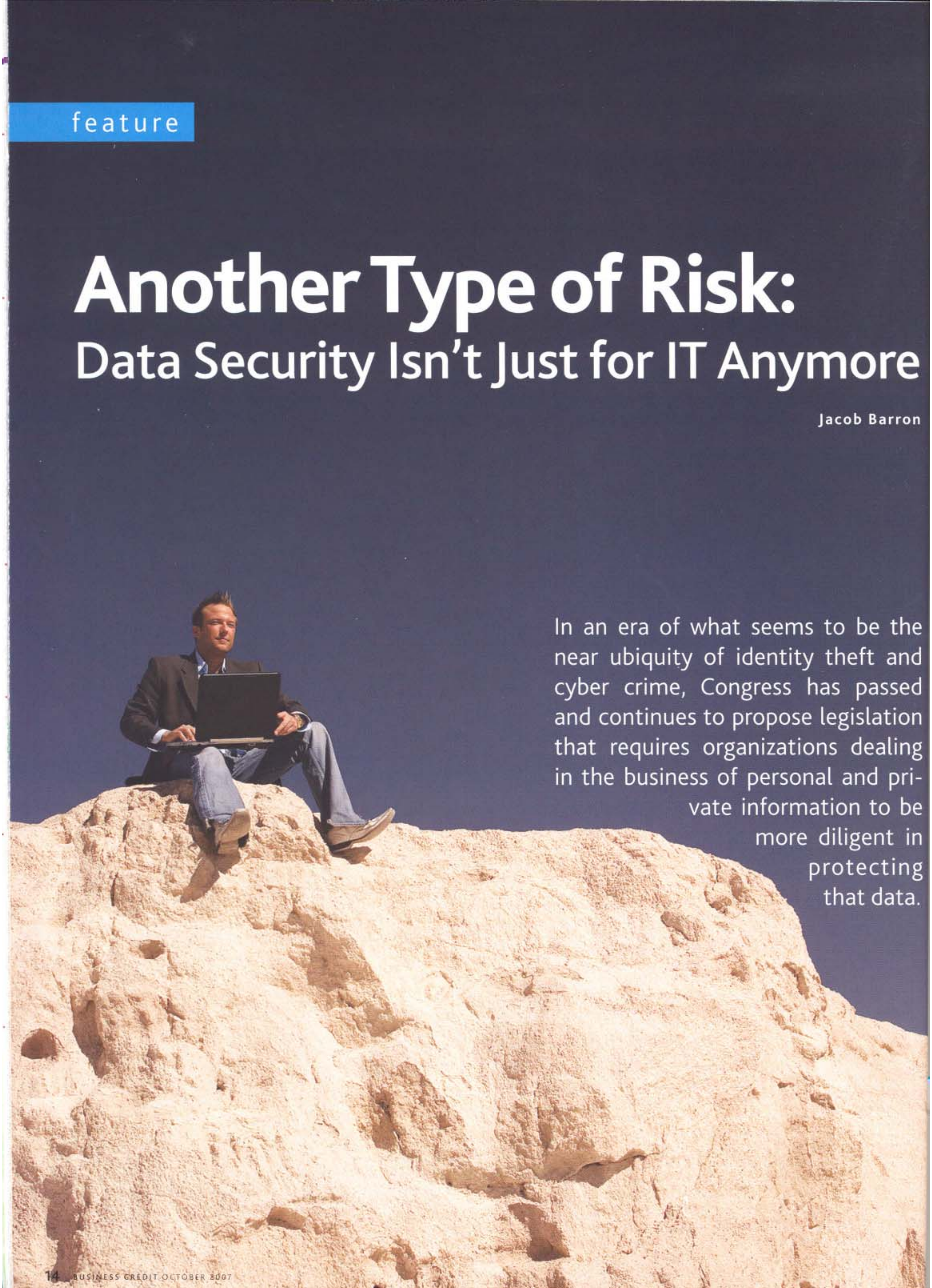
# Another Type of Risk:

## Data Security Isn't Just for IT Anymore

Jacob Barron



In an era of what seems to be the near ubiquity of identity theft and cyber crime, Congress has passed and continues to propose legislation that requires organizations dealing in the business of personal and private information to be more diligent in protecting that data.

Essentially, companies are being made to plug the holes in the hulls of their aging digital systems and make sure customer data doesn't fall into the untoward hands of thieves. But still, organizations that deal in information constitute a broad segment, if not the entirety of the business world. Customer files are kept and disposed of when no longer relevant; data security laws have been built to govern both of these practices.

As the issue has become a more frequent topic of discussion in the media, Congress has become more active in legislating data privacy laws. The means and opportunities to do harm to consumers via identity theft have also increased in number and effectiveness, so many that analysts and congressmen alike believe it's time to update the granddaddy of data security laws, the Gramm-Leach-Bliley Act (GLBA). The act became law in 1999 and marked the inauguration of the era of modern digital data storage and security, consisting of three main components known as the financial privacy rule, the pretexting rule and—the most well known of the three—the Safeguards Rule, which established what was legally required of companies to protect customer and consumer information. The Safeguards Rule required all GLBA-compliant entities to create a detailed security plan to protect the information of present and past customers and consumers.

GLBA only applied to "financial institutions," which, according to the FTC, meant all businesses, regardless of size, that are "significantly engaged" in providing financial products or services, including check-cashing businesses, payday lenders, mortgage brokers, non-bank lenders, personal property or real estate appraisers, professional tax preparers and courier services. However, under newly proposed legislation, these, and some even more stringent requirements, could apply to an entirely new division of businesses and expand the breadth of regulation to include business entities, data brokers and data furnishers.

In the Senate, the Personal Data Privacy and Security Act of 2007, introduced by Judiciary Committee Chairman Patrick Leahy (D-VT) and Ranking Member Arlen Specter (R-PA), would increase the penalties associated with identity theft, make it a crime to willfully conceal a personal data security breach and also require businesses that collect, access, transmit, use, store or dispose of sensitive personally identifiable information in digital form on 10,000 or more U.S. persons to implement a comprehensive data privacy and security policy that includes administrative, technical and physical safeguards appropriate to the size and complexity of the business' dealings.

The House of Representatives also has a similar bill, the Data Accountability and Trust Act, that is, perhaps, a bit more stringent than the Senate bill because it lacks the threshold of 10,000 U.S. persons' data stipulated in the Senate version. Instead, the Act would require any individual, partnership, corporation, association or public or private organization engaged in interstate commerce that possesses personal information to implement a security policy to protect the data that can be scaled according to the size and complexity of the entity's activities. The bill's requirements for what constitutes a security policy are similar to those in GLBA.

The free and unrestricted flow of credit and background information creates as much value as it does vulnerability.

Both of these bills have been placed on the legislative calendar and have yet to be discussed or put to a vote by either house of Congress. The House bill, however, has garnered more cosponsors (26) than the Senate bill (6).

Since nearly all sales and credit decisions are or should be based on the customer's history and the theory that a customer who pays on time repeatedly is less likely to default than one who is consistently late or bankrupt, this could affect a business' record-keeping practices and data sharing, even within the organization. Companies keep records and exchange information in order to get by and make better credit decisions. For this reason, the free and unrestricted flow of credit and background information creates as much value as it does vulnerability. Contact information is vital to the success of the sales relationship to aid in the quick resolution of customer disputes, to get in touch with a delinquent customer or to identify, legally and specifically, who owes what. But, as many others have noted, sensitive customer information tends to trickle down and as beneficial to business as the free flow of credit information is, it also creates many opportunities for a customer's personal information to fall into the wrong hands.

Each of the aforementioned works of legislation aims to strike a balance between the needs of businesses and the privacy rights of consumers. Whether or not either succeeds will not be known for sometime; and while it's uncertain what the future holds for both of these bills, it's in a business' best interest to start early and take measures to secure customer personal data now—if not in preparation for impending legislation, then for the sake of good customer service. Earning the trust of customers and making a pledge to keep their personal data safe from leaks or breaches can ultimately contribute to an all-around better business relationship and make customers more comfortable with buying from a company. And as identity thieves becoming increasingly sophisticated and determined, it makes sense for businesses to take steps now to protect themselves and their customers.

### What's Sensitive?

Sensitive information is statutorily defined as "personally identifiable information" that is transmitted to a financial institution, a result of a transaction with a financial institution or otherwise obtained by a financial institution. However, GLBA stops there in defining the phrase. Proposed legislation would specify what constitute is personal information; most include a first name or initial and last name in tandem with some other identifying piece of information, like an account number, social security number, credit card number, password or driver's license number.

### Inadvertent Disclosures vs. Hacks

When one thinks of the major data breaches in recent history, as in the record-setting TJX breach where more than 40 million customers saw their credit card numbers stolen, we imagine that the perpetrator is from a foreign country, is a genius when it comes to breaking security systems and is typically operating in a basement somewhere, shielded from proper regulation. Put simply, breaches are considered to be the work of highly organized hackers and the truth is that, in some instances, this is true. There are hacks into company systems that take place and that lead to the theft of customer data and are normally followed by a sincere apology from the violated company. Customer information is valuable, and when in the wrong hands, can be used for great, albeit wholly illegal, profit.

Improperly stored information can cause problems for companies, but even when customer data is being transmitted between employees or companies, valuable pieces of sensitive information can leak out.

"Many of [the leaks] are inadvertent disclosures," said Dr. M. Eric Johnson, professor of operations management at the Tuck School of Business at Dartmouth College. "They are a significant problem for a lot of firms." Johnson said that leaks could simply occur accidentally by employees who had no idea that they're making sensitive information vulnerable to a breach.

Johnson said that leaks could simply occur accidentally by employees who had no idea that they're making sensitive information vulnerable to a breach.

He noted that many companies provide employees with laptop computers that double as their own personal computers. If, perhaps, an employee uses a downloadable file-sharing program on that computer, they're exposing the entire hard drive to the file-sharing network. Any personal, identifiable customer information stored on that computer could easily be unknowingly released to the public, said Johnson. Also, as the U.S. Department of Veterans Affairs learned last year, lost or misplaced laptops can cause an uproar and open up a number of customers to potential identity theft.

The same goes for USB thumb drives. As the name implies, thumb drives are small and can easily be lost. Some can also hold a significant bit of information amounting to thousands of documents and what could be a sizeable portion of a company's portfolio. If that drive is lost, all of that information could be used by whoever finds it first.

### Solutions

A number of technological solutions exist to keep a company's data secure from hackers, ill-intentioned or just ill-advised, ill-intentioned employees and other threats. In any organization or credit outfit, information is exchanged and moved on a regular basis. One staff member wants information on another's customer or might choose to exchange it with another member of another department, and so on and so forth. These communications will often contain sensitive customer information and could inadvertently fall into the hands of an employee whose computer is susceptible to hacks or voluntarily open to an Internet sharing service. Newer types of software have sought to control the availability and fluidity of this information by tagging certain pieces, like account numbers or social security numbers, and notifying a supervisor when it is moved or sent in an email.

The level of scrutiny imposed on the data by the software can vary. Some software will stop the sender of the information and ask them if what they're doing is what they really want, which could potentially cut back on accidents regarding certain data. Other software actually notifies the supervisor when the information is sent, which can allow them to take action to correct the problem or to censure an employee who may have violated security practices, whether intentionally or not. "The basic idea is data loss prevention," said Johnson, who added that these programs are both effective and relatively innocuous when it comes to company operations and the flow of customer and credit information from one place to another. "It does depend a little bit on the type of implementation you're doing," he said. "But by and large, this shouldn't be an issue."

Johnson noted, however, that the market for technological solutions to a business' data security problems is fairly fragmented. No one silver bullet exists. "This base of securing data in organizations is kind of a huge and growing topic right now," he said. "There are a bunch of little niche things and solutions out there."

"Right now one of the things that's really hard is what things to invest in," added Johnson. "There are lots and lots of possibilities. There's not really a one-stop shop."

When a company seeks to secure as much data as possible and close all its potential vulnerabilities, the costs of so many different technical solutions could balloon to the point of being inefficient. "The bigger costs are getting it ruled out," said Johnson.

"A lot of financial firms have been investing in laptop encryption, which is expensive," he added. "That fixes just one security problem."

One simple solution that might provide employers with an added layer of security is the use of a webmail service rather than the standard exchange of emails over the company server. Webmail is an email environment where everything is exchanged and stored on the Internet, typically offered by search engines (Yahoo!, Google and Microsoft Networks (MSN) offer Yahoo Mail, Gmail and Hotmail respectively) While it might seem that the having all a company's email out on the Internet would be a bad thing, these web-based email servers can be much more secure than a company's own network.

"Very little, if anything, gets left on the disk said Phillip Rodokanakis, CFE, managin partner of U.S. Data Forensics, LLP. Rodokanakis, a data forensics expert who find hidden information on computers for us as evidence in court cases, noted that the use of webmail makes his job much more difficult. Still, by making messages more difficult to retrieve and his job much harder to complete, Rodokanakis conceded that webmail is good for a company looking to secure sensitive data. "Email used to leave the entire message on the hard drive," he said. "Now it's become exceedingly difficult."

### Limiting Exposure

"What we're seeing on our end is more and more of a collaborative environment," said Rodokanakis, noting that more and more employers are increasing the number of employees who have access to sensitive data so that they can collaboratively work on a project or account. "That seems to be where we're all heading," he said, adding that as more employees receive access to this data, the chances for security breaches and leaks increase.

"In order to have an effective workforce, employees need to have access to that data remotely," said Rodokanakis. "Employees are taking advantage of the employer's desire for them to access this data." This isn't to say that all employees are out to undo their employers by stealing customer data or contributing to a leak to cause a public relations problem, but the fact of the matter is that the more people who handle the data, the easier it is to lose or misplace that data.

As access increases, so does insecurity, so it makes sense that some employers need to take steps to limit access. "They're trying to figure out what information employees need," said Johnson, "and making sure you have just that and no more." However, doing so has a number of negative consequences, including from a human relations standpoint. "You join an organization and you gain access" over time, said Johnson. Once that access is gained, it might be difficult to inform that employee that they're no longer allowed to retrieve that data. It'd be easy for the employee to feel offended by the gesture. If they've worked their way up the organization's ladder and earned the trust of their superiors, a sudden reduction in the amount of access granted to them could also imply a sudden reduction in that trust.

While it might be in the company's best interest to reduce employee access to sensitive data to the very bare minimum, doing so after having already established a more open system might be difficult, and it's up to the organization to decide where to draw the line and how to compromise.

> "A lot of financial firms have been investing in laptop encryption, which is expensive," he added. "That fixes just one security problem."

### A Rolling Set of Problems

Most of the solutions available to businesses looking to curb their data security exposure seem relatively harmless to the free-flow of credit information. Technology might require a delay of a few seconds when exchanging an email with a colleague, but could also save millions in the worst-case scenario of a data breach or serious security issue. In a way, the principles of sound credit management and sound data security are the same: the objective is to reduce risk and keep the company from taking an unnecessary hit, whether that hit is financial or otherwise. As credit professionals continue to get their hands dirty dealing with sensitive customer information, they should be driving and supporting the constant adaptation necessary to maintain data security. As any expert will tell you, the threats related to data security breaches and leaks are never static but constantly evolving. "It's kind of a rolling set of problems and issues," said Johnson. "There are a lot of different types."

"Every time we do something new," said Rodokanakis, "someone else comes up with something" that can break it. The best thing to do is to stay alert and aware of these issues, be careful and implement as many security measures as is feasible, to keep the company name out of the papers and, eventually, perhaps to keep the company out of trouble. ■

*Jacob Barron can be reached at jakeb@nacm.org.*