ONCE MORE UNTO THE BREACH

Data security breaches have taken on a new dimension with the rise of "hacktivists," and require new levels of preparedness

BY MARK SEIFERT, BRUNSWICK, WASHINGTON, DC
AND JOE CARBERRY & BRANDON BORRMAN
BRUNSWICK, SAN FRANCISCO

It's 3:00am and your phone rings. It's your IT department. Hackers have exploited a weakness in your security and accessed company databases, stealing an unknown amount of confidential information. Included are employee salary information, product plans, and sensitive management e-mails. On YouTube, the mysterious group PrivSecRevenge has claimed responsibility for the intrusion. The group has posted thousands of confidential files on a public website and promises more are coming. They claim this is a reprisal for your company's "reckless" behavior in handling the privacy of millions of customers' information. Your nervous IT manager asks: "What do we do?"

No company should wait until that moment to start thinking about how to handle the public aspects of its approach to privacy and data security.

While data breaches have become an unwelcome part of modern business, there has been a shift this year in the type and scale of issues related to privacy and data security. Organizations that have been forced to publicly confront such issues include Sony; Citibank; RSA (the security division of EMC, which provides security to 90 per cent of Fortune 500 companies); the US Senate and Central Intelligence Agency; the European Commission; the European Union's emissions trading system; and the United Nations.

Heightened scrutiny from customers, shareholders, and regulators is requiring businesses to reexamine their approach to security. To complicate matters, new "hacktivist" entities, such as the "Anonymous" collective and Lulz Security (aka LulzSec), are upping the ante by making political – and very public – statements against corporations and governments through their hacking activity. This environment has brought privacy and data security issues to the fore. It is now a management-level issue, impacting both the reputation and financial position of the companies involved.

In the United States alone, between 2005 and 2011, there were more than 2,300 data breaches exposing 535m records, according to the Privacy Rights Clearinghouse. A report by the Ponemon Institute in March 2011 found that the average cost of a data breach in the US had risen to $7.2m, or $214 per record compromised. In addition, more and more countries are responding to these concerns with increased legislative and regulatory oversight. This, in turn, is driving up the costs of data protection around the world.

SIGNIFICANT DATA BREACHES

□ = 1m records lost, colored by breach type (hack, stolen, lost or fraud)

Heartland Payment Sytems
130m records lost – Hacked
Jan 20 2009

TJX Companies
94m – Hacked
Jan 17 2007

TRW
90m – Hacked
June 1 1984

Sony Corporation
77m – Hacked
April 26 2011

CardSystems
40m – Hacked
June 19 2005

Rock You
32m – Hacked
Dec 14 2009

US Dept. of Veterans Affairs
26m – Stolen
May 22 2006

HM Revenue & Customs
25m – Lost
Nov 20 2007

Sony Corporation
25m – Hacked
May 2 2011

T-Mobile
17m – Lost
Oct 6 2008

Canada Revenue Agency
16m – Stolen
Nov 1 1986

Bank of New York
12m – Lost
Sept 6 2008

GS Caltex
11m – Lost
Sept 6 2008

Dai Nippon Printing Company
9m – Fraud
March 12 2007

Fidelity National Info. Services
8m – Fraud
July 3 2007

TD Ameritrade
6m – Hacked
Sept 14 2007

Chilean Ministry of Education
6m – Hacked
May 11 2008

Data Processors International
5m – Hacked
Dec 8 2008

Source: Nathan Yau, http://flowingdata.com

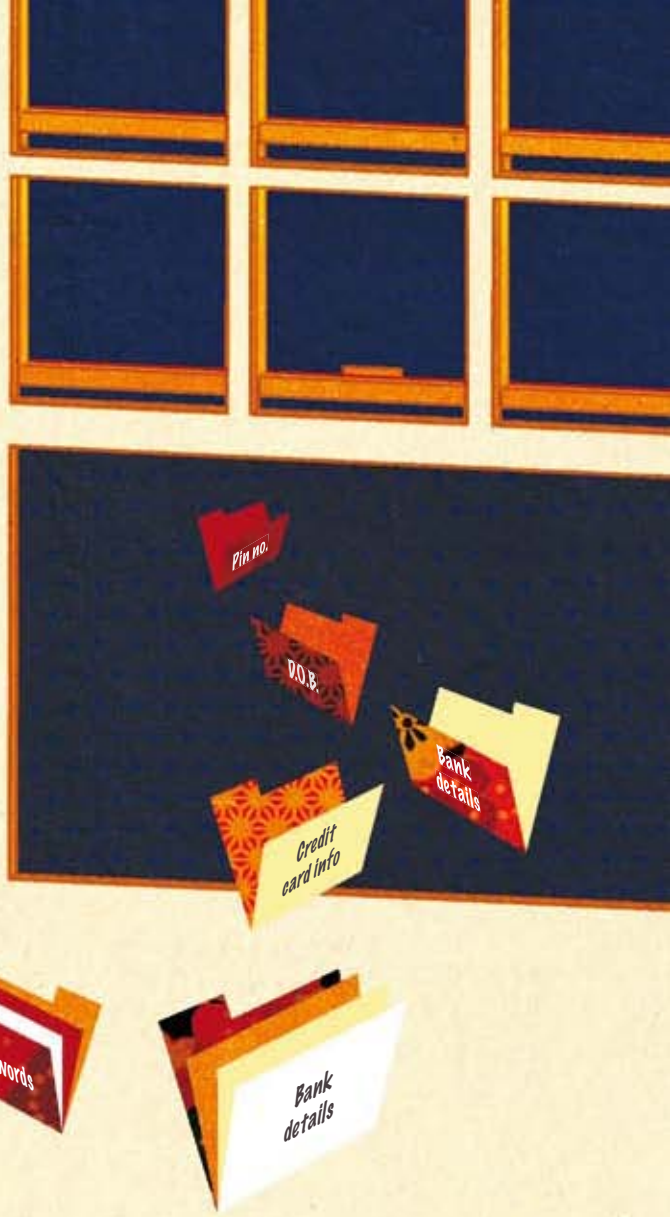
The largest cost component of a data breach is the loss of customers after an event, according to the Ponemon study. In a poll by Harris Interactive, 91 per cent of respondents stated that they would not return to a business where their personal information was stolen. Costs of breaches vary by industry. The top three sectors in 2010 in terms of average per-record cost were communications ($380), financial ($353) and pharmaceutical ($345).

There are regulatory penalties too. "Enforcement actions are on the rise," says Marcy Wilder, a partner at Hogan Lovells, and one of the leading healthcare privacy lawyers in the US. "The new federal health data breach notification law has led to a dramatic increase in investigations. Earlier this year, the Massachusetts General Hospital was hit with a $1m fine after an employee left documents containing information about 192 patients on the subway. Managing reputational risks with a proactive strategy is often a critical part of managing the related legal risks."

In spite of the costs, many companies are not effectively preparing against the risks. In a global survey of businesses by PwC, *CIO Magazine* and *CSO Magazine*, CFOs and CIOs revealed that 63 per cent either had no plan to deal with the risk of a data breach or believed their existing plan was ineffective.

The cited costs for data breaches do not include the very real expense of reputation damage that inevitably follows such an event. Marc Groman, Chief Privacy Officer for the United States Federal Trade Commission, says that consumer awareness of these issues has risen dramatically over the past few years and for good reason. "When you lose consumer data, this is not merely a number or a record that you've lost – there are real people behind these records and they care deeply about how you take care of their information," he says.

While acute crises can be painful, the real impact of information issues reaches far beyond immediate events. Security or privacy issues leave an indelible impression that can result in significant long-term barriers for organizations, including reduced business opportunities, costly regulation and litigation, and damaged trust between the company and their customers.



LIVING UP TO CHANGING EXPECTATIONS

Ultimately, the way an organization handles its private information – and the way it communicates how it is handling that data – can strengthen or destroy the trust of its customers and business partners. As such, organizations that deal with large amounts of data must actively manage and take responsibility for three distinct areas:

"Consumers equate good service with good privacy. Once that goodwill is gone, however, everything changes"

Chris Hoofnagle, privacy expert and lecturer at the University of California Berkeley School of Law

HACKTIVISM: A NEW TWIST FOR DATA SECURITY

Beyond the operational havoc, "hacktivists" also can inflict a second cost on their victims by announcing their feats to the world. Below are quotes from two of the most famous hacktivist groups, Anonymous and Lulz Security (LulzSec).

In response to an announcement by the United States Federal Bureau of Investigation that they would be stepping up enforcement against hacking, Anonymous attacked a number of defense contractors and US government agencies:
"Any private corporation[s] supporting US military or law enforcement operations are legitimate targets in our eyes ..."
eWeek, August 18 2011

Lulz Security defaced the website of a defense contractor in June of 2011 in response to a report that the US was considering classifying hacking as an act of war in certain cases. According to a LulzSec statement, anyone working with law enforcement against hacktivists was fair game:
"White hat sellouts, law enforcement collaborators, and military contractors beware: We're coming for your mail spools, bash history files and confidential documents."
SC Magazine, August 19 2011

PayPal, an online payment site, was the subject of a denial-of-service attack after it stopped processing donations for WikiLeaks following the controversial publication of US diplomatic cables. Anonymous and Lulz Security took credit for launching the attack:
"Quite simply, we, the people, are disgusted with these injustices. We will not sit down and let ourselves be trampled upon by any corporation or government. We are not scared of you, and that is something for you to be scared of. We are not the terrorists here: you are."
http://pastebin.com/LAykd1es July 27 2011

In response to the arrests of alleged members, Anonymous posted online:
"These governments and corporations are our enemy. And we will continue to fight them, with all methods we have at our disposal, and that certainly includes breaking into their websites and exposing their lies.

We are not scared any more. Your threats to arrest us are meaningless to us as you cannot arrest an idea ... It is our mission to help these people and there is nothing – absolutely nothing – you can possibly to do make us stop ... We become bandits on the internet because you have forced our hand. The Anonymous bitchslap rings through your ears like hacktivism movements of the 1990s. We're back – and we're not going anywhere. Expect us."
http://pastebin.com/RA15ix7S July 21 2011

- Acquisition of data: How does the company acquire its data? Does the company clearly and effectively inform its users and obtain their consent?
- Use of data: Why is the company collecting this data and how will it be used? Will it be sold to other parties and, if so, how will they use it?
- Data security: What actions is the company taking to ensure against misuse or theft of private information? Is the information in their care truly safe?

Privacy and security are often in the eye of the beholder. Customers, investors, advocates, and regulators all have expectations of organizations that deal with personal information. They may differ on policy and even on the definition of terms, such as the meaning of PII ("personally identifiable information"), or on who must receive notification in the event of a breach.

A company's privacy statement encapsulates its approach to all of these issues. It tells customers how it will treat their information and why it should be trusted. If a privacy policy statement is incomprehensible or buried, a company is missing an opportunity to tell its story before a crisis arises.

Adding to the confusion are constantly evolving views of what privacy means. Users have an expectation that their information remains private, is protected and that they will retain control of how it is shared. But they will increasingly forgo some anonymity in exchange for improved services and convenience. They want to understand what is being done with their information through disclosures made in plain and understandable language. They also want to control how it is used and to trust that organizations holding their data are going to be good stewards.

Those failing to live up to these high standards will face the ire of all groups – from self-policing industries, to regulators, to activist groups looking to punish entities operating irresponsibly. It may be as simple as a sub-group of users blasting out tweets or blog posts with their opinions – good or bad. Or it may be more complex, and in some cases more dangerous. Existing or newly formed activist groups – hacktivists – may choose to make an example of your organization.

It may seem tempting to classify all advocacy groups agitating against you as opponents. You may, however, benefit from thinking of some of them

as stakeholders in your organization. After all, they have demonstrated their power to affect your business by inserting barriers and costs into operations. True, some will never see eye-to-eye with any company. But many act in the interests of consumers and might respond to engagement and dialogue. In return, their opinions may inform your business strategy in a productive way.

As a matter of practice, companies should engage with customers directly. As Michael Blum, General Counsel and CPO of Quantcast and former Chair of the Privacy Group at law firm Fenwick & West, says, "Talk with your customers. Invite them into the dialogue. Speak using your privacy policy and listen ... Your blog and user comments will become part of this conversation, in which the clearest voice will be your actions."

TRUST IS A TERRIBLE THING TO WASTE

Trust is critical when it comes to how much information customers are willing to give up. According to Chris Hoofnagle, a privacy expert and lecturer in residence at the University of California Berkeley School of Law, reputation can help determine why some companies have been able to gain access to large amounts of consumer data, while others – some with arguably more privacy-protective services – can fail.

"Consumers will accept even pretty aggressive information collection if it is done by a company that is trusted," Hoofnagle says, adding that the top-ranked companies for privacy trust, such as Amazon, have very good reputations for customer service. This can be true even when consumers do not have a clear idea of exactly how a company will use their information. "Consumers equate good service with good privacy," he says. "Once that goodwill is gone, however, everything changes."

No matter what you make, sell, or serve, if you have data, your organization is potentially at risk. Privacy issues and data breaches can jeopardize your organization's most valuable relationships. Understanding the landscape and preparing to handle the inevitable public dialogue can significantly reduce the risk to your organization.

There is good news. As privacy and security have become more visible and important, they are now a core element of trust among stakeholders, especially your end users. Effective management of issues can be a powerful part of building a respected, valued and trusted corporate brand.

Done well, privacy and security can be seen as an opportunity, not just a risk.

Joe Carberry is a Partner in Brunswick's San Francisco office, **Mark Seifert** is a Partner in Washington, DC and **Brandon Borrman** is a Director in San Francisco. All advise on privacy and data security.

THE RIGHT QUESTIONS

When preparing to deal with complex privacy and data security issues, there are rarely any universal right answers. Every company and every situation requires a unique set of decisions. However, for senior leaders, there are some pertinent questions to ask:

1. What are you doing to build trust *now*?
Building trust is nearly impossible to do once something has gone wrong. It is best to tell your story before a problem arises. At least, it will increase the odds that people believe it later when you need them to. At best, it will serve to establish a robust foundation of trust.

2. Do you know what you need to know?
Companies addressing a security problem should start by understanding what their universe looks like and what is important to the stakeholders in it. Risk assessments and policy reviews can help define the starting point for additional efforts, as well as help identify any gaps.

3. Are you prepared to handle the worst-case scenario?
When something goes wrong, it is critical to get your response right the first time. If not, you will spend days or weeks undoing early mistakes before you can even begin to recover and rebuild. Preparing ahead of time to manage an incident response – from media to customers to policymakers – is essential. In these cases, success is usually proportionate to preparation.