From : ephost@epnet.com
To :
Date :
Subject : WikiLeaks fuels data breach fears

Record: 1

Title:	WikiLeaks fuels data breach fears. (cover story)
Authors:	RYST, SONJA
Source:	Business Insurance. 1/3/2011, Vol. 45 Issue 1, p1-20. 2p. 1 Chart.
Document Type:	Article
Subject Terms:	*Computer crimes *Data protection *Disclosure of information
Company/Entity:	WikiLeaks (Organization)
People:	Assange, Julian, 1971-
Abstract:	The article reports that recent disclosures by Wikileaks have raised concerns about corporations becoming the next target of potentially damaging information leaks. Wiki-Leaks founder Julian Assange, for instance, have told the "Times of London" that he had enough information to make the head of a major bank resign. A list of the most common forms of cyber attack suffered by companies in 2010 is presented.
Full Text Word Count:	1623
ISSN:	0007-6864
Accession Number:	57578640
Persistent link to this record (Permalink):	http://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=57578640&site=ehost-live
Cut and Paste:	WikiLeaks fuels data breach fears.
Database:	Business Source Ultimate

Managing systems, employee risks vital

RISK MANAGEMENT

Could you get WikiLeaked?

Recent headline-grabbing leaks by the controversial website again have highlighted for companies the complex and fast-changing nature of cyber risk exposures.

Although the highest-profile information released by WikiLeaks has centered on government documents, concerns have been raised about corporations also becoming the target of potentially damaging information leaks.

For example, Wiki-Leaks founder Julian Assange told the Times of London in recent weeks that he had enough information to make the head of a major bank resign. Amid speculation about the identity of that bank, the Charlotte Observer reported in an article titled "Cloud of Suspense Surrounds Bank of America, WikiLeaks" that Charlotte-based Bank of America Corp. recently increased its internal security, taking steps to block access to websites such as Google's e-mail application, Gmail, on company laptops. A Bank of America spokesman referred a request for an interview to a colleague, who did not respond.

"Every security incident that you hear about makes you think twice about what you're doing to defend against those things yourself," said Steve Elefant, chief information officer at the Princeton, N.J., card payment processor Heartland Payment Systems Inc.

Mr. Elefant was hired to tighten up Heartland's information security after it suffered a costly data breach in 2008. Several individuals were indicted in August 2009 for stealing data from Heartland and others related to more than 130 million credit and debit cards. The company ultimately paid around $140 million in data breach-related fines and settlements, though it was able to recover tens of millions in insurance proceeds, Mr. Elefant said.

Heartland has made changes designed to protect it against further data breaches, including end-to-end data encryption and other steps that make it much more difficult, if not impossible, to get from its corporate network into the payment network, where transactions are processed. The networks now are more segmented, physically and logically, so that type of communication can't take place.

"There's more awareness about (data breach prevention) among companies," said Nicolas Christin, associate director at the Information Networking Institute at Carnegie Mellon University in Pittsburgh.

"They've clarified their policies with respect to data breaches, and they've made it clear to their employees that this can be a potential problem," he said.

Some say the WikiLeaks affair offers lessons for companies in how to avoid the release of potentially damaging information.

Bo Holland, founder and CEO of the identity protection network Debix Inc. in Austin, Texas, said existing data regulations are centered around protecting consumers' information, such as Social Security and credit card numbers, rather than protecting corporate intellectual property.

"WikiLeaks, I think, has done a lot to raise attention to this issue, but the government regulations aren't focused in that direction," Mr. Holland said.

Harlan Loeb, director of U.S. crisis and issues management at the public relations firm Edelman Inc., said companies should attempt to understand employee concerns and head off problems that might drive the staff to leak information to third parties.

Mr. Loeb cited the example of an energy company that had contacted him after an employee threatened to disclose damaging information to the press.

The employee had raised his concerns about a pricing issue three or four times to his manager, who essentially ignored him, Mr. Loeb said. The company's chief financial officer intervened, dealing directly with the employee to address what was a misunderstanding. "The manager was so driven by his ego about being questioned that he missed the opportunity to explain something straightforward," Mr. Loeb said.

Nearly half of data breaches involve insiders, and nearly one-quarter of those involve individuals who recently experienced a job change, such as termination, resignation or demotion, according to the "2010 Data Breach Report" from Verizon Business and the U.S. Secret Service.

In addition, roughly half of the breaches in 2009 involved the use of organizational resources or privileges for purposes contrary to those intended-actions typically done in ignorance of policy or for the sake of convenience, personal gain or malice, according to the report.

Managing data risks

In addition to being sensitive to employee concerns, companies can take various steps to keep closer tabs on their information-and those handling it.

Bryan Sartin, director of the investigative response and forensics team at Verizon Business, recommends that companies first consider what data they have and why they have it.

Depending on the business involved, some might not need to maintain their customers' identifying information after a transaction is processed.

For example, some companies use a system in which information from customer credit card transactions is sent out to a so-called black box maintained by a third-party service provider, which then sends it onward to the payment processor for authorization and settlement. Customer credit card data, therefore, never resides in the company's own computer systems.

When sensitive data must be maintained, proper training of employees is vital, experts say.

Daniel Groszkruger, a risk manager at Stanford University Medical Center in Palo Alto, Calif., said his team emphasizes the need for training to include lessons on importance of keeping patient information confidential.

"Employees, particularly new ones, could be ignorant about the risk and almost innocently disclose information that they shouldn't," he said.

Kevin Kalinich, national managing director for cyber liability for Aon Risk Solutions, a unit of Chicago-based Aon Corp., said companies often mistakenly assume their employees will cooperate on cyber security procedures.

For example, the information technology department might make sure nobody can get onto computer networks without a password, but such steps are lacking if employees never bother to change their default passwords into something that is less easily hacked.

To solve that problem, the company might make its computer system lock people out unless they change their passwords every 90 days-but then more than one-fifth of the staff will begin writing their passwords on sticky notes to leave in plain sight near their monitors, he said.

The "most common mistake" is inadequate education and monitoring of employees, Mr. Kalinich said.

Monitoring employees' system use also can help identify problems, some experts say.

Mr. Sartin said he recently met with a company that made a list of the top 10 Internet users in the company-measured by time spent online-and asked those employees why they were using the Internet so much. "Something that simple will probably spread the word fast that Big Brother is watching" the staff's network activity, Mr. Sartin said.

Monitoring essential

Mr. Sartin said many companies invest in resources to enable monitoring, but then they check their logs only for trouble-shooting. Better monitoring, he noted, can help identify problems.

"Security monitoring is never something done proactively," he said. "It always happens reactively to a problem."

Most of the time, Mr. Sartin's team doesn't even need to do forensics to figure out why a company had a data breach, and instead they end up finding evidence of little problems in the logs that the clients hadn't recognized for many months.

For example, he said that examining network logs might reveal suspicious outbound traffic, such as a heavy amount of data being transferred to the same Internet Protocol address every day between 2 a.m. and 3 a.m. Or someone might have connected to the corporate network from a country where the company has no employees.

There are a plethora of security services and tools to help companies prevent unauthorized access and misuse of their information, but companies need to think carefully before just throwing money at a problem, some caution.

"Many security managers proudly exhibit the latest and greatest security tool. You may have bought cutting-edge technology with lots of bells and whistles, but don't assume that it will automatically protect you from changing threats," Khalid Kark, analyst at Cambridge, Mass.-based information technology research firm Forrester Research Inc., said in an August research note.

He recommends that companies use many layers of security rather than relying on only one. "You always need complementary people, process and technology controls," he said.

MOST COMMON EXPOSURES

Companies that suffered a cyber attack in 2010 reported that those events took numerous forms. The most common* attacks last year were:

* Malware infection: 67%

* Being fraudulently represented as a phishing message sender: 39%

* Laptop or mobile hardware theft or loss: 34%

* Insider abuse of Internet access or e-mail (pornography, pirated software, etc.): 25%

* Bots/zombies within the organization: 20%

* Denial-of-service attack: 17%

* Unauthorized access or privilege escalation by insider: 13%

* Password sniffing: 12%

* System penetration by outsider: 11%

* Theft of or unauthorized access to personally identifiable information or personal health information due to all other causes: 11%

* Exploit of client Web browser: 10%

* Financial fraud: 9%

* Website defacement: 7%

* Other exploit of public-facing website: 7%

* Exploit of wireless network: 7%

* Exploit of user's social network profile: 5%

* Instant messaging abuse: 5%

* Theft of or unauthorized access to personally identifiable information or personal health information due to mobile device theft/loss: 5%

* Theft of or unauthorized access to intellectual property due to mobile device theft/loss: 5%

* Theft of or unauthorized access to intellectual property due to all other causes: 5%

* Exploit of DNS server: 2%

* Extortion or blackmail with threat of attack or release of stolen data: 1%

*Respondents could identify multiple types of cyber attacks suffered. Source: Computer Security Institute's "2010/2011 CSI Computer Crime and Security Survey"

TOP CYBER RISK OF THE RISE AGAIN

Malware infection has been the No. 1 attack type reported by survey respondents for six years. In 2010, 67% had such an attack.

2005	74%
2006	65%
2007	52%
2008	50%
2009	64%
2010	67%

Source: Computer Security Institute's "2010/2011 CSI Computer Crime and Security Survey"

~~~~~~~~

By SONJA RYST
~~~~~~~~