

Lessons learned from corporate security breaches

Jay Cline

August 9, 2005 ([Computerworld](#))

With information security breaches in the U.S. now reported at a rate of one every three days, corporate privacy and security officers need to take stock about what's happening and what they can do about it.

So what's going on? According to the [Privacy Rights Clearinghouse \(PRC\)](#), 61 U.S. organizations have reported exposures of personal information in the past 180 days. PRC keeps the best list of breaches reported since February's watershed incident at ChoicePoint, where criminals obtained 145,000 customer accounts and sparked a series of congressional hearings on the subject of data security.

What's at the root of these breaches? The PRC reports that the leading cause is external hackers, accounting for half of the incidents. A quarter resulted from stolen laptops and computers. Dishonest insiders, lost backup tapes and negligent employees and business processes accounted for the remaining quarter ([see table 1](#)).

And I think we've seen only the beginning of this phenomenon. Why's that? Two reasons. Nineteen states have now joined California in requiring organizations to notify individuals if their Social Security numbers, driver's license numbers, financial account numbers or other sensitive information is exposed to unauthorized people ([see table 2](#)). Companies effectively must now notify all U.S. residents of breaches affecting their sensitive information, so this notification phenomenon is here to stay.

The second reason is that companies are still learning how to detect and report these breaches. A 2005 Ponemon Institute survey of corporate privacy practices found that only a third of companies use a formal process to monitor and report security breaches. As companies improve these

procedures, they'll be reporting more incidents (see [Opinion: After a privacy breach, how should you break the news?](#)).

What'll be the impact of a continuing stream of publicized security breaches? It won't do anything good for customer confidence. A [Conference Board survey](#) released in June reported that 41% of customers are purchasing less online than a year ago because of security fears (see [Survey: Consumers growing wary of buying online](#)). Trends like this affect all companies, even those with solid security.

But the impact will be greatest on those companies experiencing major publicized breaches. For its part, ChoicePoint has registered \$11.4 million in charges related to its security breach (see [ChoicePoint says data theft cost it \\$6M](#)) and endured a sustained, \$6 drop in its share price. CardSystems International, which suffered an external hack that exposed 40 million customer accounts, is facing financial ruin following the loss of its Visa and American Express clients (see [Visa, Amex cut ties with processing firm hit by security breach](#)).

So what projects need to be at the top of your organization's agenda for the next 12 months?

- Adopt a comprehensive information security program based on the [ISO 17799](#) and Payment Card Industry standards.
- Require any sensitive information stored on laptops to be encrypted.
- Formalize a process where employees can contact a central phone number or e-mail to report suspicious activity with company information.
- Validate the security of suppliers that handle your sensitive information, including backup tapes and documents.
- Train employees on your security policies and procedures and performing periodic spot checks to measure compliance.

Completing these types of projects is no guarantee of avoiding a publicized security breach. But they'll go a long way in properly allocating your limited budgets toward the areas of greatest risk.

Table 1: Root Causes of 2005 Security Breaches

The information security profession believes most breaches occur because of dishonest employees, but recent incidents point to the external hacker as the leading threat.

Root cause of data compromise	Number of publicized incidents since Feb. 2005	People potentially affected	How to reduce this risk
External breach of computer systems	31	42,928,710	Implement a comprehensive information security program
Stolen laptop or computer	15	595,620	Prohibit unencrypted storage of sensitive information on laptops and portable media
Dishonest insiders	6	831,250	Train all employees on how to report suspicious activity
Lost backup tapes	5	5,900,000	Audit your backup supplier

			against strict service levels regarding shipment and storage
Negligent employees or business processes	3	62,900	Document business processes involving sensitive information, train employees and perform spot checks
Unknown	1	6,000	Implement forensics capabilities that log the details of computer and network activity
TOTAL	61	50,324,480	

Source: Privacy Rights Clearinghouse

Table 2: State Laws on Security Breach Notification

Twenty states require notification of individuals if certain types of personal information are exposed to unauthorized people.

State	SSN	Driver's license #	Bank account #, credit-card #	Medical info	Other personal information
Arkansas	X	X	X	X	
California	X	X	X		
Connecticut	X	X	X		
Delaware	X	X	X	X	
Florida	X	X	X	X	X
Georgia	X	X	X		
Illinois	X	X	X		
	X	X	X		

Indiana					
Louisiana	X	X	X		
Maine	X	X	X		
Minnesota	X	X	X		
Montana	X	X	X		X
Nevada	X	X	X		X
New Jersey	X	X	X		
New York	X	X	X		
North Dakota	X	X	X		X
Rhode Island	X	X	X		
Tennessee	X	X	X		
Texas	X	X	X		
Washington	X	X	X		

Source: Jay Cline; most information based on Baker & McKenzie's Web site (www.bakernet.com)