

Update: TJX says data breach worse than previously believed

An ongoing probe shows it happened almost a year earlier than first thought

By Jaikumar Vijayan, Computerworld, February 22, 2007

TJX'S latest diSCIOSure IS not all that surprising, and it points to a near total lack of internal data controls at many large companies, security analysts said.

"When it comes right down to it, very few companies have put in place effective controls that enable them to monitor internal systems closely and ... follow the movement of data" on their networks, said Alex Bakman, CEO of Ecora Software Corp. That makes it possible for such breaches to go unnoticed for a long time indeed, he said.

Standards such as the Payment Card Industry Data Security Standards require companies such as TJX to put in place internal controls over their data via measures such as data encryption and strong access control, he said. But very few of the top companies have yet implemented those requirements - even though they became effective more than 18 months ago.

"The underlying problem is that Companies are treating security as a 'nice to have' as opposed to a 'must have,'" he said "TJX is just the tip of the iceberg. I think we are going to see many more [such disclosures]. It's going to get a lot uglier before it gets any better"

Joel Rosen, CEO of security vendor Tizor Systems, said that TJX is not alone "Many companies that relied on traditional security are PSI coming to terms with the fact that beefing up existing systems is not the answer.

"Without real-time insight into what is happening with the data, these breaches could go unnoticed for a very, very long time," he said. "If companies rely on log data that needs to be sifted through manually, it requires huge effort and time to detect unusual activity..."

The fallout from the breach has been widespread, with banks and credit unions around the country as well as in Canada being forced to block and reissue thousands of cards. The New Hampshire Bankers Association has estimated that as many as 20% to 30% of people in New England may have been touched by the breach.

The TJX breach has also prompted the Massachusetts Bankers Association to more actively campaign for legislation that would hold breached entities liable to card-issuing banks for the costs involved in blocking and re-issuing cards, closing and opening accounts and other similar measures. It has also prompted a smattering of class-action lawsuits.

Such breaches are certainly increasing the discussion about class-action lawsuits against breached entities, said Mark Hayes, a partner at Blake Cassels & Graydon LLP in Toronto and the current chair of the Ontario Bar Association Privacy Section. "But generally the [negative] publicity from the breaches generally exceeds [the] damage that is being suffered from them," he said.

As a result, despite all the talk about companies facing lawsuits because of breaches, there very often is little "cause for action" from a legal standpoint - at least in Canada. Hayes said. "In most of these situations, despite all the headlines" there is relatively little financial damage that consumers directly bear, he said. "Even if you prove liability it is extremely difficult to show damage."