



Just last month, a Colorado bank announced that some 5,000 of its customers could become victims of fraudsters as a result of the Heartland Payment Systems data breach.

After customers reportedly alerted First National Bank of Durango that their debit cards showed fraudulent transactions, the \$399 million company noted in a statement that because of the breach at Heartland – the fifth largest card processor in the U.S. – debit cards that they issued may have been compromised. According to the bank’s website, the company “temporarily blocked all point-of-sale purchases” in an effort to protect customers, further stating, “It is important to note that there was not a security breach at First National Bank of Durango...The breach occurred at a third-party processor.”

And that breach, which was announced in January 2009, not only turned out to be one of the most colossal of cybertheft incidents, but evidently is proving to be one of the worst in terms of long-lasting consequences as its effects are still being felt

Sponsored by
ArcSight

by other financial services companies and their customers. After the announcement that hackers had bypassed network firewalls to penetrate the databases of several large companies, including Heartland, the personally identifiable information (PII) of more than 130 million credit and debit card holders was stolen. Albert Gonzales has been indicted and pleaded guilty to the crimes, but officials at First National Bank of Durango have reportedly surmised that his partners avoided using their customers’ card numbers immediately because of the media coverage that followed. Hence, the reason their patrons are being hit only now.

If First National Bank of Durango’s announcement is a harbinger of things to come, other financial institutions and their patrons even now might be victimized by fraudulent activity related to the Heartland breach, which already has cost that company tens of millions of dollars in legal costs, fines from Visa and MasterCard and damage to the brand’s reputation. But, it’s not as if companies in the financial space don’t have enough to deal with already when it comes to safeguarding critical corporate and customer data.

During an SC Magazine Financial Services Roundtable, which was sponsored by security and compliance vendor ArcSight and held late last year in New York, leading information security professionals discussed the economy’s effects on their overall risk management plans, the ways they are refining IT security strategies in light of tightening belts, and what might be in store for future security campaigns. For them, data breaches like the one at Heartland account for only a fraction of the cybersecurity areas they fret about.

Under pressure

“I don’t feel that my job security is what it was two years ago,” said featured speaker of the Financial Services Roundtable Mark Sokol.

Head of operational risk at a large financial services company and a member of the board at the Financial Services Information Sharing and Analysis Center (FS-ISAC), Sokol used his own feelings to point out that the typical corporate worker in today’s questionable economy poses a greater risk to organizations and, therefore, is a bigger worry for IT security pros. Stress, uncertainty and concerns about personal finances just might drive end-users to engage in cybercrimes.

“Is somebody who works for a bank more enticed to sell identity data to make ends meet?,” he asked the group during the event, which was organized to enable the financial market’s security leaders to exchange advice and insight. Whether driven by malicious intent or because of simple oversight, theft or exposure of PII by insiders is a rising problem for companies, he contended.

Yet another result of the still tenuous economic state are threats to data resulting from increased merger and acquisition activity, added Warren Axelrod, formerly business information security and chief privacy officer with Bank of America and currently one of the project managers of the Financial Services Technology Consortium’s (FSTC) Software Assurance initiative. He said during the Roundtable that because of the tough economy, mergers/acquisitions and countless layoffs are causing massive changes in employees’ responsibilities. As a result, IT security pros are being forced to monitor access rights more regularly, as well as establish and follow more stringent processes of review and approval to grant and revoke access privileges – procedures that usually involve technologies to help automate and audit the process.

Alphonse Edouard, vice president of IT for Dune Capital Management, agreed, noting that mergers often also highlight the need to adhere to numerous regulations – maybe even some that one may not have worried about before the unification of various companies. Though compliance is a major concern for CISOs across all industries, for the financial services space in particular such mandates as the Red Flag Rules, the Payment Card Industry Data Security Standard, the *Sarbanes-Oxley* and *Gramm-Leach-Bliley Acts*, or even possibly more strict guidance from the Federal Financial Institutions Examination Council (FFIEC) all are directives with which IT security pros must ensure their companies are in line.

Beyond regulations and insider threats, there still are other cybersecurity problems. Sokol, who shared some statistical data at the Roundtable, noted a huge rise in the occurrence of malware, a leap in malicious website creation, a jump in zombies/botnets, an escalation in subversion techniques to launch attacks, increases in breaches exploiting unpatched networks, and over 20 countries arming themselves for cyberwarfare. And these various data theft attacks reportedly can cost

ACROSS THE BOARD

Security pros discuss how they are refining IT security tactics, and more, reports **Illena Armstrong**.

companies \$1 million or more. Then there's the worry of state-sponsored attacks on critical infrastructure companies – think Operation Aurora, recently launched from China against Google and others. Yet, by waiting for alerts from intrusion detection/prevention systems, many companies still react much too late to stop data loss.

“I don't want to go to my CEO's office and say, ‘I got great news. Our intrusion detection system detected this breach and we lost a million records.’ We have a problem,” Sokol said at the event.

Much of that problem has to do with the fact that “the bad guys” are still compromising organizations through known means, such as application vulnerabilities or simple misconfigurations, he added. And this is in spite of the fact that many studies on software development have proven the financial benefits of fixing bugs earlier rather than after release, said Reed Henry, SVP of marketing and business development at Arcsight. Those leading the fray “are bringing security into the discussion much earlier than they used to – not only because they are aware of compliance requirements and know it will cost less to implement earlier in their cycle, but also because they realize they gain far more useful results from security that is given priority earlier,” Henry explained.

Another opportunity that some IT security pros still are missing is working with other business units to support their corporations' overall commercial aims. Getting the right



stakeholders around the table to discuss business initiatives and the security needed to make them fruitful is crucial.

“Computing is making its way into every department and onto every desk, so more and more perspectives are already involved in technology decisions,” said Henry. “Security has been far less likely to be successful when dictated from an IT department.”

Engaging with key business units and aligning IT security plans with corporate projects from the start will help give data protection needs and associated expenditures priority, then.

“Are there basic things we could do to improve security in the organization? What do we do about it and is it a technical problem or is it a business problem?” asked Sokol during the Roundtable. “It's not about us spending money on technologies. As risk management executives, we have to ask ourselves what are we doing to help our companies be profitable, generate revenue and ... [meet overall] business goals?”

Not just a cost center

Detecting an intrusion too late is unacceptable to most financial organizations – there's too much too lose. For Dune's Edouard, security is about what you do before an incident occurs because, he said at the event, a cyber event will occur. In reaching this understanding then, information security leaders must decide their companies' security needs and make the right tactical and strategic calls to fulfill them.

“Our priorities flow with the dynamics of the business,” said Edouard. “If I was a utility company, the dynamics don't change. If I sell electricity, the dynamics don't change. But in the financial space or health care, the dynamics are up and down.”

The right IT security managers understand this constant shift, he added, so their objectives will change with corporate needs. This is when security done right is comparable to the scaffolding used during construction – it has to be in the right place at the right time and remain there

for however long it's needed.

“Let's face it: Anyone who thinks that they'll never get breached is in a dream world,” he said. “It's just a question of how do you manage a breach before and after, what are some countermeasures you're going to put in, and what are the dynamics of your business because security has to be matched up with what is generating capital.”

Moreover, any security outlay that is lined up with corporate goals likely will not be viewed as extra spend. And that's a good thing considering the still rough market.

“Security in the past often was characterized as a roadblock or a hurdle to overcome. And this was not too far from the truth. This has changed as security technology has really improved,” said Henry.

For Edouard, simplifying the infrastructure and then implementing both the most logical and best of these security solutions, as well as applying the right security strategies with the help of business colleagues, is the foundation of good risk management planning.

“Simplicity is the highest form of sophistication. The more simple you make your environment, the more sophisticated your environment gets, and that's where your cost-savings come in,” said Edouard. “In my work, I have to simplify [the business infrastructure], but I have to secure it and I have to manage the risks around it. As long as people have to access data, you'll always have the risk.” ■

NEW THREATS AND CHALLENGES FACING TODAY'S SECURITY PROFESSIONALS

As participants in SC Magazine's recent Financial Services Roundtable highlighted, cybercrime, in the form of confidential data breaches, continues at many institutions. However, the discussion pointed out several relatively new trends that impact security professionals. First, insiders are now often seen as a bigger risk to the business than external hackers. Next, today's attacks impact organizations more broadly and for longer than in previous years. Finally, in such a hostile environment the goal of IT security is to enable more revenue and profit, not just defensive support. Compared to prior generations of online attacks, these present new challenges for security professionals.

Borderless Networks Increase Insider Threat

With mergers and acquisitions on the rise in the banking industry, many employees fear

layoffs and may be more willing to steal confidential information in exchange for money. Making this easier is the increased access to applications and data that most employees and even contractors have now. Borderless networks have increased business productivity and communications, but have also exposed more holes for data to leak through. As legacy applications are exposed to the public via Web front-ends, weak controls such as shared administrative accounts will increase the risk of unattributed fraud and theft.

Breach Aftershocks Extend the Impact of Attacks

Though the Heartland breach is long past, banks continue to be hit by the aftershocks. As more organizations become linked via networks and connect their business processes, we can expect to see problems in one firm affect its partners. The effects may not be felt immediately, as new cybercrime techniques tend not to be "smash and

"As banks and processors become increasingly attractive targets for cybercriminals, the most forward-thinking institutions are adopting cutting-edge techniques to protect themselves."

grab" operations. Instead, smart humans guiding sophisticated technologies can gain access to high-value targets quietly and over time.

Offense vs. Defense

And yet, despite an increased risk of attack and more sophisticated techniques, the job of the IT security professional is to help optimize the business, not just protect the crown jewels. Business units need the Internet to connect to partners and customers, to become more responsive, and to move into new markets. IT must ensure that this happens safely. Online financial applications and transactions must be trusted, or else the Internet will cease to be a platform for financial innovation.

While these trends may seem worrisome, the good news is that security professionals by nature are built to adapt to new threats and the industry has responded. New solutions are available and current solutions continue to evolve to manage

these risks, and these solutions are being used at financial institutions today. User monitoring solutions can analyze a contractor or employees roles and privileges, compare these to actual activities, and then automatically apply risk models to find those people and events that are most likely to cause harm. Pattern matching, historical trending, and behavior-based malware detection can find and stop bots long before traditional AV signatures can be developed. The same techniques can detect internal and online fraud as well. These techniques can be used everywhere in an organization to secure confidential information and processes even when traditional security measures no longer apply. As banks and processors become increasingly attractive targets for cybercriminals, the most forward-thinking institutions are adopting cutting-edge techniques to protect themselves.



RICK CACCIA

Vice President, Product Marketing, ArcSight

Rick has spent 15 years designing and managing infrastructure systems, with a focus on security and identity management. Prior to ArcSight, he led product management at Symantec for email and web security products.

DOWNLOAD NOW

[Whitepaper: Combating Fraud & Data Theft in the Financial Services Industry](#)

[Case Study: Fiserv](#)

[Case Study: Experian](#)

ArcSight 

ArcSight Headquarters: 1-888-415-ARST
© 2010 ArcSight. All rights reserved.