Committee on Veterans' Affairs
May 25, 2006
Testimony of Avivah Litan
Vice President & Distinguished Analyst, Gartner Inc.

"Data Protection is much less Costly than Data Breaches"

Executive Summary

A huge theft of personal data from the U.S. Department of Veterans Affairs (VA) makes it clear that the Social Security number cannot be relied on as proof of identity. Enterprises should use this data only as part of overall "identity scores." The compromise also illustrates just how unprotected some of the nation's most sensitive data is.

Event:
On 22 May, the U.S. Department of Veterans Affairs (VA) acknowledged the theft of personal information on approximately 26.5 million people, including names and addresses, dates of birth and Social Security numbers. The information was held on computer equipment stolen from the home of a VA employee, who had taken the information home without authorization.

Analysis:
Industry research suggests that most of the individuals whose information has been stolen in this incident will not fall victim to fraud or other crimes. The thieves apparently wanted the computer equipment, and likely erased the data on it to make it easier to sell. Still, the records may have been retained and could be sold in bulk to other criminals, who in turn can use the information to create synthetic identities (by combining the Social Security numbers with new names and addresses) or make withdrawals from the bank accounts of the wealthiest individuals. Individual wealth can be easily determined by visiting www.freecreditreport.com — a U.S. government Web site set up, ironically, to help prevent identity theft — and registering for a credit report using a stolen Social Security number and other personal data.

Even though only a relatively small number of individuals will likely be directly affected by it, this incident — the largest theft of Social Security numbers documented to date — should serve as yet another wake-up call for U.S. legislators, who are currently debating identity-theft-related legislation. New laws should hold enterprises accountable for damage caused by their failure to screen for identity theft when issuing new accounts, benefits, credentials, loans and other instruments, and for not employing sound security practices around the storage and handling of sensitive personal data.

This incident also shows that the Social Security number has become an extremely unreliable piece of information and cannot be trusted to be unique to an individual. As many as one in seven adult Social Security numbers in use in the U.S. may already have been compromised.

Recommendations

Enterprises that have an interest in identifying individuals accurately, including financial service providers, healthcare providers and educational institutions: Do not rely on Social Security numbers alone as proof of individual identity. Consider the Social Security number as only one of several data elements that help to create a score for an

identity.

Enterprises that must store sensitive data about customers and other individuals: Protect the data by focusing on strong access controls, data encryption, host intrusion prevention systems, regular security audits and continual vulnerability assessments.

Attachment 1:

Data Protection is less Costly than Data Breaches

Summary

Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused. The Payment Card Industry security is a good example of industry data security standards and provides enterprises that manage or store cardholder data with good justification to increase data protection.

Analysis

The recent spate of customer information compromise and data theft provides security managers with plenty of ammunition to justify putting in more-stringent security measures around sensitive information. However, the price tag for such protection can cause sticker shock, and Gartner clients frequently ask: *How can I convince management to approve the expenditure required to better protect customer and business-sensitive information?*

Gartner analyzed the publicly disclosed costs of several recently disclosed incidents and developed estimates of additional relevant costs. We made "ballpark" estimates of the cost of three typical strategies for avoiding such incidents. These strategies are not the only ways to protect data, nor are they the only solutions to all information theft problems. Every business is different, but you can use these scenarios as starting points for developing your justification for security expenditure.

The Cost of Dealing With Failure to Protect Customer Data

A number of data points provide an indicator of the cost of allowing customer information to be exposed through a compromised business process. ChoicePoint (see Gartner research note: "ChoicePoint, Bank of America Cases Should Spur Regulation") mistakenly granted record access to an illegitimate business that exposed and potentially abused 145,000 customer accounts. In the first and second quarters of 2005, the company reported $11.4 million in charges directly related to the incident. This works out to $79 per account in direct charges for legal expenses, professional fees and communications to affected customers. Adding in the embedded costs of cleanup and recovery, systems modifications to provide after-the-fact security improvements and other related indirect costs, Gartner estimates the cost of this exposure to ChoicePoint will be in the range of $90 per exposed account.

Furthermore, ChoicePoint's total market capitalization also dropped by $720 million immediately after the disclosure and remains down more than $350 million. While Gartner doesn't believe market cap fluctuations provide reliable indicators of the impact of individual events, the actions a company will take (or not take) to address the concerns of shareholders, boards of directors, regulators and other external parties can often multiply the financial impact of a large compromise.

When smaller quantities of account information are exposed, the costs per account can work out to much-higher numbers, as the legal and professional fees are amortized across a smaller base. In 2002 (see Gartner research note "FT-18-1317" ZD Settlement Shows Cost of Deficient Privacy Protection"), Gartner estimated that the cost per account — when some 5,000 accounts were

compromised — was closer to $1,500, not including market cap fluctuation. For very large compromises (greater than 1 million accounts), we estimate the direct cost per account will be closer to $50, but such large compromises raise the very real prospect of liability lawsuits, and customer and supplier desertion leading to financial failure. CardSystems (see Gartner research note "G00130308" "CardSystems Flaw Shows Deep Credit-Card Security Problems") had up to 40 million accounts compromised and is barred from accepting Visa and American Express cards, which essentially spells a death sentence for any card processor. CardSystems was eventually bought by another payment company, Pay By Touch.

New Disclosure Costs

The U.S. Congress is considering several identity-theft related bills, and if passed, could impose stiff penalties on corporations that experience data breaches but don't disclose them.

The Cost of Protecting Customer Data

The Payment Card Industry Data Security Standards (PCI DSS) serves as a good example of a private sector response to the data security problem. PCI has expanded the original "Digital Dirty Dozen" into several hundred requirements, but most of these simply codify standard practices, such as the use of firewalls, vulnerability management and antivirus systems. As Gartner noted in "G00125063" "Visa's CISP Is Mostly Reasonable but Has Some High Hurdles," the requirements for encrypting stored cardholder data (or demonstrating effective compensating controls) have been the most difficult to meet. However, as Gartner pointed out in research note "T-22-3173" "When and How to Use Enterprise Data Encryption," encrypting stored data has become more feasible and less costly over the past 18 months.

Other advances have been made in security, such as host-based intrusion prevention (see Gartner research note "G00127317" "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention") that can provide effective security when encryption is not possible — controls that are effective at stopping attacks, not just passing compliance audits. PCI compliance is a good reason for many companies to start implementing these newer technologies, because excuses of undue complexity and unreasonable costs are no longer acceptable. (Other industries and sectors, including the government sector, need to follow the lead of the card industry and adopt standards similar to PCI).

Not all data compromises have been because of the lack of technical controls, nor can all attacks be prevented by technical controls:

- ChoicePoint's failure was the result of not extending information security into the customer registration and validation process.
- Other compromises, such as incidents at Bank of America and Wachovia, have been caused by authorized insiders taking illegal or fraudulent actions.
- The compromise of veterans' data by the VA is in part, an example of a poor business practice that allowed an employee to bring home the (unencrypted) records of over 26 million veterans.

Security processes (see Gartner research note "G00130303" "Prevent Targeted Attacks") must be extended to protect against targeted attacks that may come from a variety of external and internal sources. For many businesses, the hardest and most costly step will be to improve deficient business and IT processes, which has to be done before deploying security technology.

To address the question of demonstrating the return on investment (ROI) of protecting customer data to meet (not just to pass the audit) the PCI DSS requirements, Gartner developed three straw-man protection scenarios to illustrate typical costs: encrypting data, deploying host-based intrusion prevention on all servers, and contracting for a strong security audit and continual vulnerability assessment service. These scenarios provide different levels of both protection and deployment complexity. However, all go beyond simple PCI compliance to reach strong protection of customer data.

Encrypting stored data can provide the most-robust data protection, but if that's unfeasible because of undue cost and complexity, enterprises should deploy comprehensive host-based intrusion prevention systems (HIPS). However, successfully deploying HIPS requires strong server configuration control and additional administrative cost and complexity. Another option for enterprises is strong security audits to validate that the organization has deployed satisfactory mitigating controls, reducing the need for data encryption or HIPS. None of these options are mutually exclusive, but implementing all three will still be less expensive than having to respond to a large-scale data breach.

We make some rough estimates of deploying these protections across a large processing environment that might have as many as 1,000 servers used to handle the processing of transactions involving 100,000 customers. The cost of protection for smaller systems will be less in total but higher on a per-account basis, while larger processors will see higher totals but much-lower per-account costs.

Encrypting Stored Data

Most data theft attacks would have failed if the stored information was encrypted and the encryption keys were sufficiently protected. Network-based encryption appliances can minimize the impact of encryption on existing applications but still require significant integration effort (see Gartner research note "G00129566" "Use the Three Laws of Encryption to Properly Protect Data"). For large processing systems, Gartner has seen estimates of $200,000 for encryption appliances and an equal amount for professional services. Additional fees for process and procedure development and other ancillary concerns would increase the costs to about 20 percent to 25 percent. Gartner estimates that an expenditure of $500,000 would be feasible for protecting large (100,000 or more customer records) processing systems. This level of protection would cost about $5 per customer account in the first year, with approximately $1 per account per year in recurring costs.

Host-Based Intrusion Prevention

When account data has been compromised by direct access to stored data (whether live data or on backup media), encryption may be the most-robust solution, albeit probably the most complex to implement. However, many attacks take advantage of server vulnerabilities to launch attacks against data. If all servers in the processing system (not just the servers holding the data) were protected with effective HIPS, more than half of the reported compromises could have been prevented.

The cost of deploying HIPS includes the cost of the HIPS software agents and the labor required to configure, tune and monitor activities to ensure that business operations are not affected by false blocking actions. For large processing systems, in which as many as 1,000 servers may need to be protected, negotiated annual prices of $350 to $500 per server are feasible, depending on operating system mixes. In typical environments, startup and configuration professional

services should require, at most, six person-months of contract labor or, on the order of $200,000 at the high end. An overall HIPS expenditure of about $600,000 could have prevented large-scale attacks; much less needs to be spent when fewer servers are involved. For 100,000 accounts, this works out to be about $6 per customer account, with recurring costs on the order of $2 per account per year.

More-Vigorous and More-Continuous Security Audits

The PCI DSS program requires Level 1 merchants (typically those establishments processing more than 6 million card transactions per year) and processors to undertake annual audits, and quarterly scans of their networks. Processors must use preapproved security assessors, and large enterprises may use either third-party assessors or their own internal audit departments. The costs of audits using third-party assessors for large companies are typically upward of $60,000. The cost of subscribing to an annual scan service at a large company is about $10,000 to $15,000 for more than 128 IP addresses.

For smaller companies, the audit costs of third-party assessors can range from $5,000 to $25,000, and an automated scan service can cost as little as $1,000 a year. But the business value of low-cost security audits is highly questionable, even though they can satisfy PCI DSS compliance requirements.

Businesses serious about protecting customer data (and avoiding the costs of incidents) should not stop at the minimum level mandated by the PCI. By having a more-detailed annual audit, performing vulnerability scans weekly and using a managed service provider to monitor perimeter security controls and key internal servers, enterprises would detect deficiencies (in controls and processes) more quickly and be provided with recommendations for fixes that would prevent attacks. These actions can be viable, although less-effective, data protection options when encryption and HIPS are not feasible, and they can be designed to ensure that adequate mitigating controls are in place.

For a large processor, the costs of these types of services would be about $300,000 to $400,000 per year ($150,000 audit, $50,000 weekly vulnerability scans and $150,000 managing 20 sensors), but this would include the existing cost of demonstrating PCI DSS compliance. Of course, problems pointed out by such audits would need to be fixed. However, fixing problems before the public finds out about them is invariably less expensive than solving them afterward — the fallout also could be potentially damaging. Thus, the recurring cost per year of this approach is in the range of $3 to $4 per account, independent of the fix-it costs that are spent as a result of the audit's findings.

Bottom Line

A company with at least 100,000 accounts to protect can spend, in the first year, as little as $6 per customer account for just data encryption or as much as $16 per customer account for data encryption, host-based intrusion prevention and strong security audits combined. These unit costs will be reduced drastically if these strategies are applied to protecting millions of customer accounts. This compares with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach. Likewise, these costs may escalate dramatically if proposed legislation mandating fines for each exposed and damaged customer account is imposed. Protecting your data is well worth the investment — with or without Payment Card Industry or other compliance requirements.