Safeguard your sensitive data.*

A proactive approach to data security will help identify and stop breaches of high-value information.

*connectedthinking

PricewaterhouseCoopers

Table of contents

The heart of the matter 4

Even the most sophisticated data breach techniques leave subtle clues that can be used to help improve security — if you know where to look.

An in-depth discussion 6

You can protect only what you are aware exists. That is why a thorough inventory of data and information systems is essential to a successful security program.

The unknown is a real risk to network and data security
Taking stock: Why data inventory is essential
The missing link: Proactively assess your environment for breach indicators

What this means for your business 12

Improve your security posture by detecting breach evidence that other solutions overlook.

The heart of the matter

Even the most sophisticated data breach techniques leave subtle clues that can be used to help improve security — if you know where to look.

Data and identity theft is no longer for amateurs. Today's hackers are organized, motivated, and sophisticated. They often work on behalf of state-sponsored or criminal organizations, have access to state-of-the-art tools, and know how to target specific organizations for information that can be used for financial gain.

At your expense.

We have seen large corporations with sophisticated security systems fall prey to costly — and embarrassing — malicious attacks. Consider, for instance, a large corporation that recently lost a massive amount of data in a security breach.

Attackers leveraged a combination of application, network, and operating system vulnerabilities to gain a foothold on a critical segment of the organization's internal environment. They subsequently installed custom-developed malware that "sniffed" the network, collected sensitive unencrypted data in transit, and transmitted the data via the Internet using a modified version of a common diagnostic protocol permitted in most enterprise networks. This homegrown malware was not detected by antivirus software, and its network traffic did not contain known exploits that would typically alert network intrusion detection.

In other words, the malware was effective. Consequently, the company suffered millions of dollars in direct and indirect financial losses, as well as significant damage to its reputation.

The breach wasn't detected until an in-depth forensic analysis exposed the attacker's tools and techniques. The analysis also uncovered one unheeded clue that huge amounts of data were leaking from the network: The percentage of outbound network traffic comprised by the hijacked diagnostic protocol was far higher during the attack than under normal circumstances.

This case offers an important lesson. Even the most complex hacking and data breach techniques can leave subtle but detectable signatures in network traffic and system behavior. These traces typically will slip by automated tools such as data loss prevention (DLP).

Solid protection against data breaches requires a multipronged approach that includes not only tools such as DLP, but also a risk-based approach to monitoring. In other words, CISOs should focus on monitoring the areas where the most risky data reside. This risk-based strategy must be tightly aligned with business processes and integrated into overall risk management.

To do so, CISOs must know the basic facts about their organization's data, particularly its location. According to PricewaterhouseCoopers' 2008 Global State of Information Security Survey[1], 71 percent of respondents said their organization does not have an accurate inventory of high-value data and where it is stored. That is an astonishing knowledge gap that must be closed.

The first step is to build and maintain a data inventory that tracks where sensitive data resides and how it is communicated. Next, an organization must carefully watch for data "breach indicators" — subtle traces such as unusual network traffic flow, suspicious patterns in system activity, and improper account usage — to rapidly detect and respond to security incidents. A proactive process to identify and act on breach indicators can help close the loop on security and help an organization identify and stop breaches in its environment.

An in-depth discussion

You can protect only what you are aware exists. That is why a thorough inventory of data and information systems is essential to a successful security program.

It may seem obvious, but the key to preventing data breaches lies in the basics: the information in “information security.” Security has become increasingly complex as data portability, accessibility, and mobility increasingly enable this information to move freely across corporate, organizational, and international boundaries.

Every industry has its own form of highly sensitive — and often regulated — information that is at the core of its operations. Depending on the sector, sensitive data could be healthcare records, financial transactions, personally identifiable information (PII), intellectual property, or national security data. This type of data is a moving target: Medical records are digitized and shared among healthcare providers; engineering specifications are passed along to each member of a manufacturing supply chain; payment card data is transmitted between points of sale, card processors, and banks.

If you could confine this type of data within the corporate network and ensure that it is accessible only to authorized parties, guarding it would be easy. In reality, businesses continually create processes and innovations that require information to be captured and shared by a distributed workforce, business partners, third parties, and customers.

Therefore, a sound approach to protecting sensitive, regulated information that is shared with authorized parties requires close alignment of security spending with business objectives.

Without it, security programs can fail — and the fallout can be costly. A breach may lead to direct financial losses, regulatory violations, legal liability, and a diminished reputation among customers, business partners, and the public. In fact, the Federal Trade Commission estimates the annual loss to businesses from data and identity theft amounts to almost $50 billion. Beyond direct financial losses, fines, and lawsuits, data breaches can have a serious long-term impact on a company’s brand and reputation.

The unknown is a real risk to network and data security

Businesses are struggling to simply track and manage their information. That basic fact was proved in a recent study conducted by Verizon Business[2], which aggregated and analyzed several hundred data breach incidents over the course of five years to identify significant trends. The study focused on the sources of breaches, the means by which data were compromised, and the impact to victims.

Verizon Business found that 69 percent of incidents were detected by a third party rather than by the organization. External sources were responsible for 74 percent of these incidents, and 32 percent of incidents originated from a business partner.

More ominously, half of breaches involved an "unknown unknown." According to Verizon Business[3], these unknown unknowns can manifest themselves in several forms:

- A system unknown to the organization (or business group affected)
- A system storing data that the organization did not know existed on that system
- A system that had unknown network connections or accessibility
- A system that had unknown accounts or privileges

These factors readily reveal what an organization does not know about its infrastructure and data. Unknown unknowns are blind spots in the data protection architecture — the people, processes, and technologies that organizations rely on to prevent or detect malicious activities.

Taking stock: Why data inventory is essential

In this turbulent economy, organizations have sought to cut costs, often subjecting information security spending to increased scrutiny. Security investments no longer can be justified as an inevitable overhead or as preventative measures against abstract threats. To ensure that security gets adequate support, it must be integrated into enterprise risk management as an intrinsic part of business processes.

To date, this has proved to be a daunting task. According to our recent global security survey[4], only 25 percent of respondents reported that their security spending is aligned with the company's business objectives. How can this gap be narrowed?

You can protect only what you are aware exists. That is why a thorough inventory of data and information systems is essential to a successful security program.

One of the most fundamental security controls an organization can implement is a thorough inventory of data and information systems. An accurate, complete inventory is essential for the success of any IT risk management effort, including security, business continuity, and disaster recovery.

Moreover, an effective inventory cannot merely track where data is stored. It also must account for the information lifecycle, from origin through disposal, and consider the mobility of data in today's IT-centric world. Data may be encrypted at rest in a database, but what about other points in its lifespan?

A data inventory requires an organization to know how the information is gathered and aggregated and whether it remains encrypted from end to end as it is passed among the database, application server, and client. Furthermore, data can be breached as it is transmitted to a third party or contractor via an external interface. An inventory should account for the scenarios in which data is used and communicated. Security controls that focus only on data at its source or resting points will fail to protect it from all avenues of attack.

Data inventory has a hidden benefit that can have a deep impact on security: When a business undergoes a data inventory, it encourages stakeholders to "think like a hacker." As they identify data elements and categorize their sensitivity and importance to the business, stakeholders will begin to understand the impact of a data breach.

In practice, building and maintaining a complete data inventory can be a daunting task, and controlling information once it has been identified can be more difficult. As a result, many organizations have turned to DLP solutions to help automate these processes. Often, however, they do so too late. A survey by the Ponemon Institute[5] found 37 percent of businesses affected by a data breach acquired DLP solutions as part of their remediation strategy.

Implementing DLP is a worthwhile step toward protecting information from common data-loss scenarios, particularly those involving nonmalicious negligence. When used effectively, DLP tools can identify sensitive data at rest, control its usage at user endpoints, and monitor or block its egress from network perimeters. A DLP implementation also helps force an organization to address IT security with a risk-based approach that assesses the value of its information assets.

Despite these benefits, DLP is not a silver bullet capable of defeating all threats. DLP technology is designed to handle the most common-use cases — typically those that involve user negligence or error — contributing to data breach scenarios. It can stop a user from copying and pasting hundreds of Social Security numbers from an application into a Notepad file, or it can quarantine an unauthorized e-mail containing unencrypted PII before it leaves the network.

But DLP is much less likely to stop the sophisticated obfuscation and encryption techniques that hackers employ to steal data from a compromised environment. This is particularly troubling, considering that Verizon Business' study found that 64 percent of data breaches were the result of hacking and 38 percent were caused by malware[6].

The missing link: Proactively assess your environment for breach indicators

To help close the loop on security, organizations must pay close attention to the often subtle red flags that indicate suspicious system or network activity. These clues can indicate that a data breach has occurred. Organizations should develop a detailed approach to determine the breach indicators in their environment and then implement a process to continually monitor the environment for the presence of these indicators.

When looking for activity that could signal a breach, numerous subtle traces in network traffic and system behavior should raise red flags. Typical system breach indicators can include unusual activities in security logs, suspicious processes, or unusual network connections. From a network perspective, breach indicators can include unusual volumes of traffic, unusual network protocols, or communications with systems or networks known to be involved in the distribution of malware.

There is no one-size-fits-all solution; breach indicators pinpoint behavior that is unusual for a specific environment. The process for monitoring the chosen indicators must reflect the baseline system and network activity expected during normal operating conditions.

You can protect only what you are aware exists. That is why a thorough inventory of data and information systems is essential to a successful security program.

When determining a set of breach indicators for a given environment, it is helpful to consider the data inventory. It is far easier to create accurate, targeted indicators that focus on the most likely paths of compromise for sensitive data than to monitor and control broad swaths of an unknown network.

To be a winning proposition in today’s business environment, a program for identifying and monitoring the environment for breach indicators must leverage existing technology investments in more effective and creative ways. In our experience, many victims of data breaches could have detected their incidents had they followed a more formalized regimen for collecting, analyzing, and reporting anomalous activity, not by implementing the latest security or networking product.

The key is information and how it can be aggregated and analyzed: combining an understanding of common attack patterns with knowledge of what an organization’s most sensitive data is, where it is stored, and how it is processed and communicated.

Sophisticated threats and a difficult economic climate can challenge an IT risk management program. There may be no single solution, but the foundation of an effective security strategy is clear. Businesses must use what they know best — their own data — to design the next generation of security controls.

What this means for your business

Improve your security posture by detecting breach evidence that other solutions overlook.

CISOs have numerous automated security solutions to choose from, but none fully closes the loop on security. PricewaterhouseCoopers believes the missing link can be found in the basics: a company's data.

It is our view that organizations should augment automated security solutions by building and monitoring a comprehensive inventory of their data and information systems. In doing so, they will identify and classify data according to its sensitivity and risk and know where it resides and flows. Then they can more effectively take advantage of data breach indicators to identify and detect signs of breaches that may be overlooked by solutions such as identity management and data loss prevention.

PricewaterhouseCoopers has a long history of helping companies understand their security landscape to align it with business requirements. Across multiple industry sectors, we have helped our clients respond to and decompose targeted attacks. This experience helps us understand gaps in standard safeguards and how to build enhanced safeguards to bridge these gaps. We have experience implementing a wide variety of solutions around controlling and limiting access to data. We also specialize in performing security assessments that highlight how data and systems can be compromised. We know how data breaches happen and how to help prevent them.

As a security adviser, PricewaterhouseCoopers' first concern is to help organizations appraise their security landscape and improve their security posture by making the most of existing solutions. We take the time to help you understand and protect your information environment.

We know that data is your most valuable asset, but if unprotected, it can also be a huge liability.

[1] PricewaterhouseCoopers, 2008 Global State of Information Security Study (October 2008)
[2] Verizon Business, 2009 Data Breach Investigations Report (2009)
[3] Verizon Business, 2009 Data Breach Investigations Report (2009), page 34
[4] PricewaterhouseCoopers, 2008 Global State of Information Security Study (October 2008)
[5] Ponemon Institute LLC, Cost of a Data Breach (February2009)
[6] Verizon Business, 2009 Data Breach Investigations Report (2009), pg 2

To have a deeper conversation on the topic mentioned, please contact:

Brad Bauch	Principal	Houston	brad.bauch@us.pwc.com
Rik Boren	Partner	St. Louis	rik.boren@us.pwc.com
Kevin Campbell	Principal	Atlanta	kevin.campbell@us.pwc.com
Thomas J. Carver	Partner	Pittsburgh	thomas.j.carver@us.pwc.com
Donald B. Christian	Partner	Washington	donald.b.christian@us.pwc.com
Michael Compton	Principal	Detroit	michael.d.compton@us.pwc.com
Shawn Connors	Principal	New York	shawn.joseph.connors@us.pwc.com
Scott Evoy	Principal	Boston	scott.evoy@us.pwc.com
Kurt Gilman	Principal	New York	kurt.gilman@us.pwc.com

Joe Greene	Principal	Minneapolis	joe.greene@us.pwc.com
John Hunt	Principal	Washington	john.d.hunt@us.pwc.com
Jerry Lewis	Principal	Dallas	jerry.w.lewis@us.pwc.com
Mark Lobel	Principal	New York	mark.a.lobel@us.pwc.com
Sloane Menkes	Principal	Washington	sloane.menkes@us.pwc.com
Joe Nocera	Principal	Chicago	joseph.nocera@us.pwc.com
Chris O’Hara	Principal	San Jose	christopher.ohara@us.pwc.com
Fred Rica	Principal	New York	frederick.j.rica@us.pwc.com
Andy Toner	Principal	New York	andrew.toner@us.pwc.com

pwc.com/us

To have a deeper conversation on the topic mentioned, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

This publication is printed on Mohawk Options PC. It is a Forest Stewardship Council (FSC) certified stock using 100% post-consumer waste (PCW) fiber and manufactured with renewable, non-polluting wind-generated electricity.

Recycled paper

© 2009 PricewaterhouseCoopers LLP. All rights reserved. “PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. DH 10 0009