The Power to Prevent:
It's the Next Generation

FIDELIS SECURITY SYSTEMS, INC. 4416 EAST WEST HIGHWAY, SUITE 310, BETHESDA, MD 20814

Managing the Evolving Risk of Data Leakage

Fidelis Security Systems

December 2006

© 2009, Fidelis Security Systems, Inc.

Contents

INTRODUCTION…….....3
THE EVOLVING DATA LEAKAGE RISK.....4
THE FACTORS DRIVING DATA LEAKAGE RISK 5
OPTIONS FOR DEALING WITH RISK.....7
UNDERSTANDING THE DATA LEAKAGE RISK.....8
MITIGATING THE DATA LEAKAGE RISK 9
SUMMARY.....10

Introduction

Protecting confidential or sensitive data has been a core business process for many years. Organizations have learned that the unintended disclosure, or leakage, of this information can have large negative consequences, including market, brand, legal, operational, and financial implications. Managing the risk of leakages and preventing them from occurring is critical to comply with regulations, instill good corporate governance, and safeguard an organization's brand and reputation.

In the past few years, there has been a sharp increase in data leakage from large organizations of all kinds including commercial, government, and education customers. According to the 2006 CSI/FBI Computer Crime and Security Survey, unauthorized access to information and theft of proprietary information continues to be two of the top categories of concern regarding reported security breaches with "unauthorized access to information" continuing to be the second-greatest source of financial loss for an organization. In the Deloitte 2006 Global Security Survey, 82 percent of respondents experienced a security breach in the last twelve months with 72 percent of those breached indicating that the estimated amount of damage to their organization, including direct and indirect costs, was in the $1 million range. This increase in data leakage and the negative impact associated with it has become a major issue for large organizations–including commercial, government, and educational institutions.

The risk of data leakage is very real today—it seems as if we read about a data leakage incident in the paper every week. The sharp increase in occurrences is one key contributing factor to the significant media coverage; however another key factor has emerged—the increase in privacy laws and industry operating standards mandated by governments and industry organizations. The State of California was the first in the United States to pass legislation (State Bill 1386) to require an organization to disclose the loss of any personal information of a California resident. This bill has caused many other states to pass legislation to require disclosure of leakage of information and Federal legislation is anticipated in 2007.

Some Examples of Recent Incidents in the Headlines

- Company's source code posted to employee's personal Yahoo e-mail account
- Large retailer settles with FTC after 13 million customer credit cards lost
- Medical facility loses personal identity information on 185,000 patients
- Major University alumni database hacked exposing donors' personal information

- Debit card account information and PINs of 300,000+ bank debit card users leaked with millions of dollars stolen from accounts
- Source code and proprietary design documents from a provider of ID badge systems to the federal government and Fortune 500 stolen
- Names and Social Security numbers of 1.3 million student loan borrowers missing

As technology evolves and organizations rely on it more and more to accomplish their mission, the likelihood of data leakage, and the negative impact that accompanies it, has increased greatly. This risk is so great that respondents in a June 2006 report published by Merrill Lynch identified the leakage of confidential or proprietary information as the greatest overall threat to organizational security. Also by a wide margin, data leakage/extrusion prevention ranked as the top category of promising new security technology according to 62 percent of respondents. This paper discusses this evolving risk of data leakage, or extrusions, and the factors contributing to them. This paper then offers options for dealing with the risk, a guide to understanding the risk in an enterprise, and recommendations to actually mitigate this risk by implementing direct controls such as an Extrusion Prevention System® to manage data leaving an enterprise.

The Evolving Data Leakage Risk

There are two key drivers of this increase in incidents of data leakage—the conversion from physical to digital assets and the increase in available technology channels (such as instant messaging and webmail) over which information moves. Organizations have spent the last couple of decades converting information to digital formats to make it more accessible to employees, contractors, customers, suppliers, and business partners. This digitization has provided huge gains in productivity for all parties involved, but it has also driven an increased risk of exposure.

Even before the age of digital assets that we live in today, various physical security controls were put in place to ensure that an organization's information was properly protected. These controls included policies and procedures to implement access control, physical security, and anti-forgery. These controls still exist today, but organizations have had to adapt and expand these controls to deal with the digitization of these same types of information. In an electronic format, these digital assets present a significantly larger challenge to secure and prevent leaks, either accidental or intentional.

Digital assets are much more challenging to protect than their physical counterparts due to some unique and important differences. Before assets were stored digitally, physical access was

required to take or copy large amounts of information. In the paper age, the asset had to be either taken, at the risk of being discovered missing, or copies had to be made that were typically of a lower quality. In today's networked enterprise, data can be accessed from virtually anywhere and is frequently shared in the course of commerce, which has increased the number of potential threats to digital assets. In the digital age, the original is usually never removed and copies are perfect replicas of the information. These key differences have made digital assets significantly harder to control than their physical counterparts.

Differences between Physical and Digital Assets

Physical Assets	Digital Assets
• Require physical access	• Can be viewed from any location on the network
• Inventory detects loss	• Can be taken without removing original
• Copies typically noticeable and of lower quality	• Copies identical to original

In addition to this increased exposure presented by the digital assets themselves, the proliferation of additional network channels has lessened organizations' ability to control the exposure of data. With the ubiquity of internet-based communications, it has become increasing simple to share these digital assets via a variety of technologies.

E-mail systems were the first widespread mechanism for inter-organizational communication. As recently as five years ago, e-mail was the primary method for exchanging information electronically. Today, the addition of channels like instant messaging, webmail, peer-to-peer, and other real-time communication channels to enterprise communications has provided multiple additional channels over which information flows, and has greatly increased the risk of unintended leakage of sensitive or confidential data. These new channels create additional points for data to leak and when unmanaged, greatly increase the risk of unintended leakage of digital assets.

The Factors Driving Data Leakage Risk

According to the Risk and Insurance Management Society's glossary, risk is the possibility of loss or exposure to loss.

IT security leaders often represent the presence of a risk with this equation:

Risk = Threat x Vulnerability

Risk is a function of the likelihood of a given threat taking advantage of a particular vulnerability to accomplish a particular goal—in this case, disclosure, or leak of sensitive or confidential

information. This equation simply measures the presence of risk and not the resulting impact of that adverse event on the organization, which is often measured by expected value and probability metrics.

A *threat* (or *threat agent*) is the person or process attempting, either intentionally or accidentally, to leak or disclose the organization's information. This could be someone inside the enterprise like a disgruntled employee or a contractor, or someone outside like a competitor or hacker. A *vulnerability* is a technical or procedural weakness that could provide the threat access to information to leak it outside the organization. In this case, the vulnerability is an unmanaged network communications channel. Both a threat and vulnerability are required for there to be risk. If a threat agent exists, but they have no means to leak data, there is no risk. By the same token, a long list of vulnerabilities without anyone interested in exploiting them also equals zero risk. Unfortunately, this is rarely the case. The Gartner Group estimates that "…70 percent of security incidents that actually cause loss to enterprises—rather than mere annoyance—involve insiders," meaning every company has a threat and therefore a risk from their insiders alone. It is also important to note the difference between a risk and the loss incurred when it becomes a reality. *A risk that becomes a reality cannot be managed; an organization can only react to the associated loss.*

Based on this equation, it becomes readily apparent how the risk of data leakage has increased. The first element of risk is the threat. It would be nearly impossible to argue that threats have decreased—in fact likely they have increased greatly. Requirements for productivity gains have made employees work harder and longer on the job. Outsourcing and globalization have eliminated jobs. All of these factors greatly increase the chance that a disgruntled employee or contractor could be motivated to disclose digital assets. To make matters worse, a black market for information like credit card and financial account information has evolved, making it easier for a threat to turn information into a financial profit. Finally, hackers are getting increasingly sophisticated in their approach, developing worms and other attacks that target specific information for export out of an organization.

These risks are important, but the more critical factor in the equation is the vulnerabilities (remember, a threat without a vulnerability is a not a risk). The traditional approach to vulnerability management has been focused on keeping the bad guys out (even though almost all metrics show that the insider threat is by far the largest). Organizations deploy technology, people, and process focused on making sure systems are properly configured and patches are applied; deploy access controls to make sure only the correct people have access to information; and

work on developing a secure perimeter to keep hackers out.

This traditional paradigm, while necessary, has proven insufficient in protecting against data leakage. There are two key reasons for this. First, this approach requires accuracy 100 percent of the time. One missed patch, bad password, or incorrectly configured firewall becomes a vulnerability that a threat agent could exploit. Second, and of significantly more importance, is that this paradigm ignores the fact that employees, contractors, suppliers, customers and business partners have to have access to critical and sensitive data in order for an organization to function. Therefore any network channel, whether authorized or unauthorized, becomes a potential vehicle for information to leak out of the organization.

These network communication channels are multiplying. Traditionally, corporate e-mail was by far the largest network communication channel used for communication outside of the organization. Today, the list of protocols used daily in organizations has skyrocketed and includes e-mail, HTTP, webmail, instant messaging (IM), internet relay chat (IRC), file transfer protocol (FTP), and peer-to-peer technologies (P2P). When unmanaged (as most of these channels are today), the vulnerabilities these channels present greatly increases the risk of unintended disclosure of critical or sensitive information.

Risk	=	Threats	X	Vulnerabilities
Greatly increased risk		• Disgruntled employees • Outsourcing • Globalization • Black market for information • Hackers targeting information		• Existing infrastructure issues • Expansion of unmanaged communication channels including: e-mail, HTTP, webmail, instant messaging (IM), Internet Relay Chat (IRC), File Transfer Protocol (FTP), and peer-to-peer (P2P) technologies

Options for Dealing with Risk

Most organizations strive to either maintain a fixed expected value from a risk or to lower their expected value over time. This rise in vulnerabilities from unmanaged communication channels increases the expected value of data leakage risk, forcing the organization to make a decision on how to handle this leap in the expected value of the risk.

There are four options for managing a risk:

• Accept the risk

• Transfer the risk to a third party

• Mitigate the risk

• Avoid the risk altogether

Looking at the information leakage risk, it is unfortunate to find that two of these are not an option. It is very difficult, if not actually impossible, to transfer this risk. Insurance is the typical method used to transfer risk, and the majority of insurance companies will not insure against the loss of confidential or sensitive data. So unfortunately, transfer is not an option. Avoiding the risk is also not an option. This risk is unlike the risk of skydiving, where a choice can be made not to pursue the activity. Employees (and many contractors, customers, suppliers and business partners) require access to data for an organization to function. Avoiding the risk would require ceasing operations, and therefore is also not an option.

This leaves the organization with two options, either to accept the increased risk delivered by these additional unmanaged communication channels, or to take action to mitigate the risk through the implementation of process, technology, or a combination of the two.

Understanding the Data Leakage Risk

Mitigating the risk of data leakage requires a different approach than the traditional control used to mitigate technology-based threats. Rather than looking at technical infrastructure, patch levels, account configuration, and packets, an organization needs to shift the focus to examining the content of the information flowing across the network. This is a significantly different challenge. Previous approaches have allowed or disallowed technologies, not the content flowing inside of them. For example, the traditional approach is to allow a communication method regardless of its content. Employees are allowed to use e-mail, HTTP, instant messaging, and FTP, but are not allowed to use peer-to-peer technologies. While controlling the channels in use can help mitigate the risk of data leakage, it does not prevent a threat agent from using an allowed technology for unauthorized purposes. To prevent the unauthorized use of these channels, an organization needs to pursue a fundamentally different approach than traditional network management tools. The solution needs to actually inspect the content flowing across channels and analyze it based on business and content rules (rather than technical attributes).

Confidential or sensitive information is spread all over an enterprise including research, development, human resources, sales, and marketing departments. In addition, this data is stored on many different computer types (e.g., desktops, laptops, UNIX servers, Windows servers) in many different formats (e.g., Microsoft Office, PDF, databases, XML, compressed files, design documents and other formats). To mitigate this problem, an organization must identify the types of information it deems critical to protect.

Examples of Confidential or Sensitive Information

Research, Development, & Production—research, design specifications, computer source code, test results, recipes, formulas, production schedules, trade secrets

Financial Information—account numbers, credit card data, mergers and acquisitions, financial models, unreported financials

Marketing and Sales—Customer lists, pricing, market plans, sales targets

Human Resources—Employee data, medical records, salary, payroll, organizational plans

Other Classified or Confidential Information—legal papers, internal memos, business processes

Once the information is identified, business polices can be put in place to determine what information should not be disclosed. In addition to internal policies, these policies will often be driven by legal or industry regulations. For example:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the protection of Electronic Protected Health Information.
- California SB 1386 and similar state legislation require anyone conducting business in California to report any disclosure of personal information of a resident.
- The Gramm-Leach Bliley Act (GLBA) requires administrative, technical, and physical safeguards to protect customer information maintained by financial services organizations.
- The Payment Card Industry (PCI) Security Standard establishes security guidelines required to accept or process credit card transactions.

Once these policies are identified, a technology solution must be put in place to monitor the outbound network traffic and identify whether the content leaving is compliant with organizational policies. However, a solution that merely reports on data leakage does not actually mitigate an organization's risk because:

Risk mitigation requires more than simply reporting on the state of the organizations' compliance position.

Mitigating the Data Leakage Risk

To mitigate the data leakage risk it is imperative that an organization have a process in place that stops data from leaving the network—a process known as extrusion prevention. Many content monitoring solutions in the marketplace today are able to let an organization know when it has

leaked information, which gives a snapshot of the organization's compliance levels. However, the incident they reported on has now occurred, and the risk of non-compliance with internal policies and external regulations has become a reality.

To prevent this reality, an organization needs to implement an extrusion prevention solution that actually mitigates the risk of data leakage before it occurs. Historically, the e-mail channel has received most of the security focus. This is because it was both the most popular and also the easiest to secure. E-mail is one of the few protocols in use today that is not instantaneous. While incredibly fast, e-mail is stored briefly on a corporation's mail server before it is forwarded on to its destination. During this brief time period, it is very easy to analyze the contents of this e-mail for compliance with organizational policies. If this analysis takes a couple of seconds to occur, the underlying e-mail transport (the Simple Mail Transfer Protocol or SMTP) continues to function as designed.

Unfortunately, e-mail is one of the only protocols used widely today that has these attributes. Other channels, like instant messaging, HTTP and webmail, file transfers, and peer-to-peer technologies, are designed to occur in real time. These channels are much more difficult to secure because the content analysis also must occur in real time. The introduction of any significant delay will have a significant impact on the user experience or cause the network session to actually be interrupted.

As these additional channels are large vulnerabilities that drive up the risk of data leakage, a solution must be architected to actually prevent non-compliant communication sessions. This requires the solution to be able to evaluate the content of the entire network session and make a policy decision in real time. The architecture of the solution is incredibly important. For example, a solution that requires the network session to be written to computer disk for analysis will be too slow to prevent on a real-time protocol. It is important to ensure the solution chosen can actually prevent on all network channels, and therefore actually mitigate the risk. An Extrusion Prevention System is the key to mitigating the data leakage risk.

Summary

Increased unmanaged communications channels, when paired with the threat elements present in an organization today, create a significantly increased risk of unintended disclosure of sensitive or confidential information through data leakage. As additional real-time communication channels are adopted, this risk and therefore the expected value associated with it, is continually increasing. As insurance is not available, and access to information is required for an

organization to function, there are two options to handle this increased risk—accept or mitigate. As most organizations are adverse to accept increases in risk, mitigation is the likely approach.

The mitigation of this risk is different than the traditional paradigm used in information security, as it requires making decisions on the content of a network session versus the technical attributes of the network traffic. This requires new processes and technology to examine the content of the network session for compliance with internal policies and external regulations. It is also critical to have technology, an Extrusion Prevention System, that supports prevention for all network communications (not just corporate e-mail) given that reporting on the state of the organizations' compliance position does not actually prevent a risk from becoming a reality.

FIDELIS SECURITY SYSTEMS, the FIDELIS SECURITY SYSTEMS logo, Extrusion Prevention System, and/or other FIDELIS SECURITY SYSTEMS products referenced herein are trademarks of Fidelis Security Systems, Inc. Copying, use or distribution of any material contained herein is expressly prohibited. *Copyright © 2006 Fidelis Security Systems, Inc. All rights reserved.*