

Strategies to Reduce Your Information Security Risk

Executive Summary

The headlines are full of stories about organizations that have somehow compromised the security of the information used in their business operations. Naturally, you wonder if your contact center is at risk of being hit as a disturbing fact emerges. It is not attacks from outside hackers that are the biggest technology security concern today, rather the risk comes from the actions of your employees - both intentional and inadvertent.

Failing to properly secure the information in your contact center creates the risk of experiencing significant negative consequences. These may include lost revenue opportunities, legal penalties for non-compliance or a negative reflection on your management ability.

With all that is at stake, what should you do to mitigate this risk in your contact center operation? While no system is 100 percent reliable, the SANS Institute recommends implementing five layers of technology protection to ensure the maximum possible level of data security. Proper operational procedures can also help manage your risk of data loss due to theft or carelessness. To determine what changes, if any, are required in your operational practices, you need to explore questions regarding your technology infrastructure, employment practices and information handling guidelines. You can then use this information to create comprehensive operational and information handling guidelines to greatly minimize your risk exposure.



Companies from every vertical industry are becoming more aware of the need to carefully monitor information security levels and so security scans and audits are becoming a regular practice. Intended to identify all possible risks within a specific software application, scans and audits are a critical, unbiased way to help you determine whether or not your technology solutions meet industry standards for secure system and information management and to what extent changes need to be made to secure your environment. Working closely with your technology vendors, the goal of the information security audit is a simple one – to ensure you achieve the highest level of security available working within the framework of your business environment.

With careful preparation and ongoing evaluation, you can keep your contact center out of the information security headlines.

Introduction

Failing to properly secure the information in your contact center exposes you to potentially significant negative consequences. These may include lost revenue opportunities as your operation halts while trying to determine how a security breach occurred and how much information was taken, legal punishment if the loss is due to failure to comply with industry regulations (e.g., Identity Theft and Assumption Deterrence Act (1998), Gramm-Leach-Bliley Act (GLBA) (1999), Fair and Accurate Credit Transactions Act of 2003 (FACTA) (2003)) and a negative reflection on your management ability if the appropriate preventive measures were not in place.

The Threat

You've seen the headlines,

"Businesses Have No Idea How Much Sensitive Data is Leaking Out of Their Organizations" 18 September 2006, SecurityPark.Net

"New Data Theft Scandal Rocks Subcontinent's Call Centres," 3 September 2006, The Observer

"540,000 New Yorkers at Risk of Identity Theft. Names, Addresses and Social Security Numbers of Injured Workers Lost." 24 July 2006, MSNBC.MSN.com

"Investigator Faults VA, Employee for Data Loss." 12 July 2006 MSNBC.MSN.com

"Computers Superglued To Stop Data Theft," July 6, 2006, Newsfactor Magazine Online

"Banks Begin New Secure-Data Effort, Big Financial Institutions To Adopt Shared Guidelines To Protect Customers." 1 February 2006, Wall Street Journal

and you've wondered if your contact center is at risk. Are you doing enough to protect the highly sensitive information your contact center staff deals with every day?

As you read the details of these and other incidents, a disturbing fact emerges. It is not attacks from outside hackers that are the biggest technology security concern today. Instead, the risk comes from the actions of your employees – both intentional thefts motivated by a desire for revenge or personal gain and carelessness that exposes your information to loss or inadvertent theft.

According to a Federal Trade Commission survey conducted in 2003, more than 9.9 million Americans were the victims of identity theft, costing U.S. businesses and financial institutions nearly \$48 billion. No industry or company is immune. The Yankee Group estimates that 50 percent of security problems in 2004 originated from internal sources, up from 30 percent in 2003¹. It takes less than five minutes for such employees as tellers and account managers who have proper access to customer data to steal someone's identity. Some of the world's largest financial institutions have fallen victim to internal hackers. But this new epidemic isn't limited to financial institutions – every business that has a database of customer information needs to be vigilant against deliberate attacks and reckless or even simply unthinking behavior that puts your information at risk.

With all that is at stake, what should you do to mitigate this risk in your contact center operation?

¹ As reported in the *Wall Street Journal*, 01 June 2005.

Protection Through Technology

While no system is 100 percent reliable, the SANS Institute recommends five layers of technology protection or “defensive walls,” that proactive contact centers can implement to ensure the maximum possible level of data security. The necessity and applicability of each of these layers of technology protection will depend on an assessment of the nature of the potential threats and the business risks to the contact center.

The first three and the last defensive wall revolve around your information technology (IT) systems, architectures and business process tools.

Defensive Wall 1 is a network-based, external-facing layer designed to block attacks from outside hackers. Using firewalls, managed security services and intrusion detection software, you can safeguard such web transactions as electronic bill payments. This is the only layer visible to the general public.

Defensive Wall 2 is designed to block attacks at the host-based level. This layer uses personal firewalls, spyware removal and quarantine software to protect internal systems and devices such as PCs, servers and workstations. Defensive Wall 2 provides a level of protection in the event that a hacker manages to get through Defensive Wall 1.

Defensive Wall 3 adds another tier of protection, guarding against any exploitation of security vulnerabilities within the application layer or operating system. It requires configuration management, application security testing, vulnerability management and penetration testing. A crucial component of this layer is the constant scanning of all internal systems and applications.

Defensive Wall 5 consists of tools you can use to minimize your security exposure and maximize operational effectiveness. This layer includes forensics tools such as audit tracking which can help to quickly identify when an attack or security breach occurs and what exactly was compromised. It also provides valuable feedback for the development of future protection plans. You should also have an established disaster recovery plan and redundancy systems in place. In addition to protecting your information, these tools and plans assist with regulatory compliance, providing reporting data specific to the level required by government regulations such as Graham-Leach-Bliley, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley and Federal Information Security Management Act (FISMA).

The fourth defensive wall deals with protecting your systems from people within.

Defensive Wall 4 focuses on safely supporting authorized users. In this layer, all systems are typically firewalled and guarded as entities unto themselves. This is where you define who has access to what databases and systems. A crucial element of this layer is the encryption of data and files. But securing the data is not enough. At level 4, discretionary access control must also be implemented to ensure that your users only have access to the specific applications, databases and various system objects for which they have been approved. As an example of this access control, an agent handling billing inquiries would have access to customer billing history or account information, while an agent in customer service will only have access to limited customer information, such as name, address and service type.

For more information on these regulations, as well as others that may affect the contact center industry, please refer to the SANS website at www.sans.org.

Unfortunately, even with all these measures in place, you are still vulnerable to theft or loss from within – either through the deliberate removal of information by someone who has been granted access to a particular server or through the loss of critical data due to carelessness or ignorance of proper information protection practices. And so you must turn to operational procedures to mitigate these highly unpredictable risks.

Protection Through Operational Procedures

Proper operational procedures can help manage your risk of data loss due to theft or carelessness. To determine what changes, if any, are required in your operational practices, ask yourself the following questions:

1. How are background checks of contact center agents conducted? Are references contacted? Are names checked against criminal databases?
2. How many defense walls will be implemented?
3. Are laptops used and, if so, what type of information is stored on them? If an executive leaves a laptop behind at an airport, what security features have been built in so that no one else can access the confidential information?
4. Do contact center employees sign affidavits saying they will not access customer information for personal use?
5. What system is in place for disabling network access when employees are terminated? What formal processes are in place for handling employee grievances and monitoring employee satisfaction?
6. Is there a list of all contact center employees who have access to sensitive information? How often is the list updated? How often should security checks be conducted?
7. How are passwords set up and how often are they required to be changed? What level of encryption is used?
8. What safeguards are in place with respect to documents (physical and electronic) which leave the building with employees? Is there a check in/check out process for data files?
9. Do you outsource any transactions? If so, how are vendors screened? Can they provide background checks for any of their employees accessing your systems? Do they comply with industry standards for authentication? Do they have any vulnerability that matches the FBI lists of the Top 20 systems issues?
10. Do you have published guidelines for information handling that specifically address practices such as using publicly accessible computers or downloading sensitive data and removing it from your business locations?

Exploring questions such as these and using the answers to document and then adhere to comprehensive operational and information handling guidelines can greatly minimize your risk of data loss due to theft or carelessness.

Conducting a Security Audit — Where Do You Start?

Companies from every vertical industry are becoming more aware of the need to carefully monitor their information security. As a result, security scans and audits are becoming a routine practice. Aspect Software regularly receives security scan review requests from our customers. These scans originate from various verticals, with the highest concentration coming from the financial services sector.

Security scans and audits are intended to identify all possible risks within a specific software application. They are a critical, unbiased way to help you determine whether or not your solutions meet industry standards for secure system and information management. They provide you with a view into how secure your software applications are and to what extent changes need to be made within your network or within the solutions themselves to fully secure your overall environment.

The most common security scan/audit targets are:

- Operating systems
- Databases
- Third party components
- Network access
- User authentication systems
- Physical environment

Your company structure and the type of business you are engaged in will, to some degree, determine the strength of your focus in each of the areas. The security audits that Aspect regularly engages in with customers focus primarily on the operating system, databases and third party components.

- **Operating system** audits focus on identifying missing operating system patches, security patches or undefined ports. They also focus on identifying unsecured access points such as open ports, unprotected user accounts and unprotected files.
- **Database** audits seek to identify missing database patches, unsecured database tables, unencrypted data elements and unsecured user accounts.
- **Third Party Component** audits focus on identifying unsecured versions of third party applications.

The typical audit process is as follows:

- 1) Using security auditing software (example, ISS Scanner), perform security scans/audit on one or more Aspect solutions.
- 2) Provide the results of the audit to your account team accompanied by a description of your internal policy regarding timeframes for addressing or responding to perceived vulnerabilities.
- 3) Aspect will then conduct an analysis of the results to assess the impact of the items identified and provide a detailed response which lists those deemed to be actual vulnerabilities and those vulnerabilities which may appear on the list due to other factors - e.g., a default operating system setting which appears as a vulnerability.
- 4) Aspect works with you to develop an action plan to address the vulnerable areas. If a product change is required to address a specific vulnerability, we define a timeframe for the delivery of this change and provide recommendations for limiting security risk in your environment while this change is in progress.

The goal of the security audit is a simple one - to ensure you achieve the highest level of information security available using Aspect solutions and working within the framework of your business environment.

Guidelines for Your Contact Center Vendors and Solutions

Solutions provided by Aspect Software and other contact center vendors must provide the security and flexibility you need on the product level and at the support level. Factors to consider as you evaluate your contact center vendors and their solutions include the abilities to:

- Comply with your internal security policies.
- Integrate with your existing security systems, for example, your authentication systems.
- Follow your standard practices for network and user access restrictions.
- Restrict the usage of administrative accounts and utilize highly secure password encryption.
- Customize login security banners to provide tailored warnings about the systems and the information for which access is requested.
- Support your existing infrastructure (example, Citrix®) for your networking and distributed application management.
- Support the latest (typically the most secure) third party product versions
- Provide a highly secure remote support access method.

As you are well aware, remote support access provides the quickest possible diagnosis and problem resolution. However, it is critical that this support access occurs in a way that maintains the integrity of your network and system security. Solutions should use a current industry security architecture such as Site-to-Site IPSec VPN Tunnel. Additionally, your vendor should be willing to work with you to identify any customized support practices needed to ensure the remote support access solution works within your corporate guidelines.

Summary

With careful preparation and ongoing evaluation, you can keep your contact center out of the information security headlines. Keys to successfully doing this include:

- Following the Defensive Wall guidelines for protecting yourself against both deliberate destruction or theft and accidental data loss.
- Establishing and following clear technology, personnel and operational guidelines.
- Conducting ongoing security audits to identify potential areas of vulnerability and engaging in a security partnership with your vendors to address them.
- Requiring that all solutions entering your contact center provide flexibility and compliance with your information security policies and practices.

Although there can never be a 100 percent guarantee, following these guidelines and recommendations can greatly mitigate your information security risk.

Links to Additional Information

- Articles cited:

[*"Businesses Have No Idea How Much Sensitive Data is Leaking Out of Their Organizations"*](#) 18 September 2006, SecurityPark.Net - The leading online magazine for the Security industry

[*"New Data Theft Scandal Rocks Subcontinent's Call Centres,"*](#) 3 September 2006, The Observer

[*"540,000 New Yorkers at Risk of Identity Theft. Names, Addresses and Social Security Numbers of Injured Workers Lost."*](#) 24 July 2006, MSNBC.MSN.com

[*"Investigator Faults VA, Employee for Data Loss."*](#) 12 July 2006 MSNBC.MSN.com

[*"Computers Superglued To Stop Data Theft,"*](#) July 6, 2006, Newsfactor Magazine Online

- [About.com list of 2006 Data Breaches](#)
- [CERT Home page](#)
- [National Institute of Standards and Technology \(NIST\) Computer Security Division](#)
- FTC Information on Consumer Fraud and Identity Theft - <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>
- [SANS \(SysAdmin, Audit, Network, Security\) Institute information and security resources list](#)
- [SecurityPark.net - the leading Security News portal](#)

Note: Aspect and Aspect Software are registered trademarks of Aspect Software, Inc., in the United States and other countries. All other trademarks or tradenames are the property of their respective owners.

About Aspect Software

Aspect Software, Inc., the founder of the contact center industry, is the world's largest company solely focused on providing proven, innovative contact center products and services that enable the key business processes of customer service, collections, and sales and telemarketing. Each day, thousands of in-house and outsourced contact centers around the globe conduct more than 125 million customer interactions using Aspect Software products. Aspect Software believes in using the power of technology to positively transform the customer-company experience. That belief has led Aspect Software to accept the challenge of developing the world's most reliable automatic call distributors (ACDs), most trusted dialers, most widely-used and respected workforce management (WFM) solutions, most flexible voice self service systems and the industry's first and most comprehensive unified, multichannel contact center solution. Headquartered in Westford, Mass., Aspect Software has operations across the Americas, Europe, Africa, the Middle East and Asia Pacific. For more information, visit www.aspect.com.

Aspect Software
Corporate Headquarters
6 Technology Park Drive
Westford, MA 01886

978 952 0200
978 952 0201 fax
www.aspect.com

