Anatomy of a Data Breach

Why Breaches Happen and What to Do About It
Introduction
For organizations that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. In fact, more electronic records were breached in 2008 than in the previous four years combined.¹

This growth in data breaches should come as no surprise. In a world where data is everywhere, it has become harder than ever for organizations to protect their confidential information. Complex, heterogeneous IT environments make data protection and threat response very difficult. Yet today’s businesses depend on their security teams to ensure that collaboration and sharing by an increasingly mobile workforce remains safe and secure.

While the continuing onslaught of data breaches is well documented, what is far less understood is why data breaches happen and what can be done to prevent them. This paper examines the three most common sources of data breaches—well-meaning insiders, targeted attacks from outside the organization, and malicious insiders—and goes on to illustrate the ways in which each source gains access to the network, finds and then exposes sensitive information. It also offers a broad perspective on what can be done to stop data breaches, as well as specific recommendations to take preventive action. The section entitled What does it all mean? offers a unique point of view on data breaches based on the industry-leading security expertise, comprehensive global intelligence, and broad experience of Symantec in helping its customers successfully protect their sensitive information.

Why data breaches happen

In order to prevent a data breach, it is essential to understand why they occur. Third-party research into the root causes of data breaches, gathered from the Verizon Business Risk Team and the Open Security Foundation, reveals three main types: well-meaning insiders, targeted attacks, and malicious insiders. In many cases, breaches are caused by a combination of these factors. For example, targeted attacks are often enabled inadvertently by well-meaning insiders who fail to comply with security policies, which can lead to a breach.

![Figure 1. Trends in Causes of Data Breaches, 2004–2008](image)

Well-meaning insiders

Company employees who inadvertently violate data security policies continue to represent the largest population of data breaches. According to the Verizon report, 67 percent of breaches in 2008 were aided by "significant errors" on the part of well-meaning insiders. In a 2008 survey of 43 organizations that had experienced a data breach, the Ponemon Institute found that over 88 percent of all cases involved incidents resulting from insider negligence. An analysis of breaches caused by well-meaning insiders yields five main types:

- **Data exposed on servers and desktops.** Daily proliferation of sensitive information on unprotected servers, desktops, and laptops is the natural result of a highly productive workforce. Perhaps the most common type of data breach occurs when well-meaning insiders, unaware of corporate data security policies, store, send, or copy sensitive information unencrypted. In the event a hacker gains access to your network, confidential files stored or used without encryption are vulnerable and can be captured by hackers. As a result of data proliferation, most organizations today have no way of knowing how much sensitive data exists on their

---

2- Ibid.
3- http://datalossdb.org/
4- Verizon Business Risk Team, op. cit.
5- Ibid.
6- Ponemon Institute, 2008 Annual Study: Cost of a Data Breach, February 2009
systems. Systems that held data the organization did not know was stored on them accounted for 38 percent of all breaches in 2008—and 67 percent of the records breached.  

- **Lost or stolen laptops.** The 2008 Ponemon Institute study found that lost laptops were the top cause of data breaches, representing 35 percent of organizations polled. In a typical large enterprise, missing laptops are a weekly occurrence. Even when such cases do not result in identity theft, data breach disclosure laws make lost laptops a source of public embarrassment and considerable expense.

- **Email, Web mail, and removable devices.** Risk assessments performed by Symantec for prospective customers show that on average approximately one in every 400 email messages contains unencrypted confidential data. Such network transmissions create significant risk of data loss. In a typical scenario, an employee sends confidential data to a home email account or copies it to a memory stick or CD/DVD for weekend work. In this scenario, the data is exposed to attack both during transmission and on the potentially unprotected home system or removable media device.

- **Third-party data loss incidents.** Business relationships with third-party business partners and vendors often require the exchange of confidential information such as 401(k) plan, outsourced payment processing, supply chain order management, and many other types of operational data. When data sharing is overly extensive or when partners fail to enforce data security policies, the risk of data breaches increase. The Verizon report implicated business partners in 32 percent of all data breaches.

- **Business processes automate the spread of sensitive data.** One reason for proliferation of confidential data is inappropriate or out-of-date business processes automatically distribute such data to unauthorized individuals or unprotected systems, where it can be easily captured by hackers or stolen by malicious insiders. Onsite risk assessments by Symantec find that in nearly half of these cases, outdated or unauthorized business processes are to blame for exposing sensitive data on a routine basis.

### Targeted attacks

In today's connected world—where data is everywhere and the perimeter can be anywhere—protecting information assets from sophisticated hacking techniques is an extremely tough challenge. Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. More than 90 percent of records breached in 2008 involved groups identified by law enforcement as organized crime. Such attacks are often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites. In 2008, Symantec created more than 1.6 million new malicious code signatures—more than in the previous 17 years combined—and blocked on average 245 million attempted malicious code attacks worldwide per month.

Measured by records compromised, by far the most frequent types of hacker attacks in 2008 were unauthorized access using default or shared credentials, improperly constrained access control lists (ACLs), and SQL injection attacks. In addition, 90 percent of lost records were attributed to the deployment of malware. The first phase of the attack, the initial incursion, is typically perpetrated in one of four ways:

---

7- Verizon Business Risk Team, op.cit.
8- Ponemon Institute, op.cit.
9- Symantec Data Loss Prevention Risk Assessments
11- Ibid
12- Symantec Internet Security Threat Report XIV
13- Ibid
• **System vulnerabilities.** Many times laptops, desktops and servers have do not have the latest security patches deployed which creates a gap in an overall security posture. Gaps or system vulnerabilities can also be created by improper computer or security configurations. Cybercriminals search for and exploit these weaknesses in order to gain access to the corporate network and confidential information.

• **Improper credentials.** Passwords on Internet-facing systems such as email, Web, or FTP servers are often left on factory default settings, which are easily obtained by hackers. Under-constrained or outdated ACLs provide further opportunities for both hackers and malicious insiders.

• **SQL injection.** By analyzing the URL syntax of targeted websites, hackers are able to embed instructions to upload spyware that gives them remote access to the target servers.

• **Targeted malware.** Hackers use spam, email and instant message communications often disguised as known entities to direct users to websites that are compromised with malware. Once a user visits a compromised website, malware can be downloaded with or without the user’s knowledge. Gimmicks such as free software deceive users into downloading spyware that can be used to monitor user activity on the web and capture frequently used credentials such as corporate logins and passwords. Remote access tools (RATs) are an example of spyware that is automatically downloaded to a user’s machine without their knowledge, silently providing the hacker control of the user’s computer and access to corporate information from a remote location.

Most security teams focus almost exclusively on protecting data by stopping incursions. But incursion is only the first phase of a data breach by targeted attack. To provide complete data protection, all four phases must be addressed.

Four phases of targeted attacks: incursion, discovery, capture, exfiltration

• **Phase 1: Incursion.** Hackers break into the company’s network by exploiting system vulnerabilities, using default password violation, SQL injection, or targeted malware.

• **Phase 2: Discovery.** The hacker maps out the organization’s systems and automatically scans for confidential data.

• **Phase 3: Capture.** Exposed data stored by well-meaning insiders on unprotected systems is immediately accessed. In addition, components called root kits are surreptitiously installed on targeted systems and network access points to capture confidential data as it flows through the organization.

• **Phase 4: Exfiltration.** Confidential data is sent back to the hacker team either in the clear (by Web mail, for example), wrapped in encrypted packets or zipped files with password protection.

The good news is that a targeted attack on confidential data can be defeated at any one of these four phases. Security professionals who focus only on the incursion phase are making an all-or-nothing bet—a wager that, given the reality of today’s wide-open information environment, is likely to fail sooner or later. By taking precautions against the discovery, capture, and exfiltration of data, organizations can significantly bolster their defenses against targeted attacks.
The malicious insider

Malicious insiders constitute drivers for a growing segment of data breaches, and a proportionately greater segment of the cost to business associated with those breaches. The Ponemon study found that data breaches involving negligence cost $199 per record, whereas those caused by malicious acts cost $225 per record.\(^{15}\) Breaches caused by insiders with intent to steal information fall into four groups:

- **White collar crime.** The employee who knowingly steals data as part of an identity theft ring has become a highly notarized figure in the current annals of white collar crime. Such operations are perpetrated by company insiders who abuse their privileged access to information for the purpose of personal gain.

- **Terminated employees.** Given the current economic crisis—in which layoffs are a daily occurrence—data breaches caused by disgruntled former employees have become commonplace. Often, the employee is notified of his or her termination before entitlements such as Active Directory and Exchange access have been turned off, leaving a window of opportunity in which the employee can access confidential data and email it to a private account or copy it to removable media. A recent study of the effects of employee terminations on data security revealed that 59 percent of ex-employees took company data, including customer lists and employee records.\(^{16}\)

- **Career building with company data.** It is common for an employee to store company data on a home system in order to build a library of work samples for future career opportunities. While the motives for such actions may not be considered malicious on the order of identity theft, the effect can be just as harmful. If the employee’s home system is hacked and the data stolen, the same damage to the company and its customers can ensue.

---

15-Ponemon Institute, op. cit.
16-Ponemon Institute, "Data Loss Risks During Downsizing: As Employees Exit, So Does Corporate Data," 2008
Industrial espionage. The final type of malicious insider is the unhappy or underperforming employee who plans to defect to the competition and sends examples of his or her work to a competing company as part of the application and review process. Product details, marketing plans, customer lists, and financial data are all liable to be used in this way.

What does it all mean?
With the steady drumbeat of data breaches making headlines almost daily, it might seem reasonable to regard data breaches as an inevitable by-product of our connected world, a cost of doing business that we must simply learn to live with. A closer view of the facts, however, suggests that this is not necessarily the case. Symantec offers security expertise, a global intelligence network, and real-world experience with customers, and these combine to inform a more hopeful perspective. From this point of view, three important truths must be recognized in order to gain control of the data breach situation.

First, breaches are preventable. In each of the breach scenarios discussed above, there were key points of intervention when countermeasures could have prevented the breach—and, in some cases, did so. Contrary to the impressions left by sensationalist news coverage, there is good cause for optimism.

Second, the only strategies with a chance of success are both risk-based and content-aware. Preventing data breaches is all about risk reduction. To reduce risk, you must know where your data is stored, where it is going, and how it is used. Only then will you be able to clearly identify problematic practices, prioritize data and groups for phased remediation, and begin to staunch the flow of proprietary data leaving your organization.

And, third, preventing data breaches requires multiple solutions that work together in concert to solve the problem. This means much more than defense-in-depth. It means that the solutions you deploy—whether to monitor information, protect endpoints, check technical and procedural controls, harden core systems, or provide real-time alerts—must be integrated to create a centralized view of information security so that you can make correlations and discover root causes quickly and decisively.

How to stop data breaches
To monitor their systems and protect information from both internal and external threats across every tier of the IT infrastructure, organizations should select solutions based on an operational security model that is risk-based, content-aware, responsive to threats in real time, and workflow-driven to automate data security processes. Here are six steps that any organization can take to significantly reduce the risk of a data breach using proven solutions:

Step 1. Stop incursion by targeted attacks. The top four means of hacker incursion into a company’s network are by exploiting system vulnerabilities, default password violations, SQL injections, and targeted malware. To prevent incursions, it is necessary to shut down each of these avenues into the organization’s information assets. Controls assessment automation, core systems protection, endpoint, web and messaging security solutions should be combined to stop targeted attacks. In addition, endpoints should be managed centrally to ensure consistent deployment of security policies, patches, encryption capabilities, and information access.
Step 2. **Identify threats by correlating real-time alerts with global security intelligence.**

To help identify and respond to the threat of a targeted attack, security information and event management systems can flag suspicious network activity for investigation. The value of such real-time alerts is much greater when the information they provide can be correlated with knowledge of actual known threats. Being able to tap into current research and analysis of the worldwide threat environment in real time gives security teams a tremendous advantage in combating external threats.

- Leverage security intelligence services that daily monitor millions of email messages and systems worldwide to analyze internal event data and stay current on the evolving threat landscape.
- Combine security information and event management systems to track network activity, collect incident data from all security systems, and match incident logs against a data feed from security intelligence services to identify known trouble sites and other external threats in real-time.

**Step 3. Proactively protect information.** In today’s connected world, it is no longer enough to defend the perimeter. Now you must accurately identify and proactively protect your most sensitive information wherever it is stored, sent, or used. By enforcing unified data protection policies across servers, networks, and endpoints throughout the enterprise can you progressively reduce the risk of a data breach. Data loss prevention solutions can make this unified approach a reality.

- Implement content-aware *define once, enforce everywhere* policy management with incident remediation workflow, reporting, system management, and security.
- Find sensitive information located on file servers, databases, email repositories, websites, laptops, and desktops, and protect it with automatic quarantine capabilities as well as support for policy-based encryption.
- Inspect all outbound network communications, such as email, IM, Web, FTP, P2P, and generic TCP, and enforce policies to prevent confidential information from leaving.
- Proactively block confidential data from leaving the organization from endpoints via print, fax or removable media.
Step 4. Automate security through IT compliance controls. To prevent a breach organizations must start by developing and enforcing IT policies across their network and data protection systems. By assessing the effectiveness of the procedural and technical controls in place and automating regular checks on technical controls such as password settings, server and firewall configurations, and patch management, organizations can reduce the risk of a data breach. To sustain and improve their compliance posture organizations need to continuously assess how their infrastructure is set up to support IT compliance policies. Leveraging IT policy creation, policy deployment, IT compliance controls assessments, incident management and correlation tools will enable organizations to proactively identify and remediate deficiencies before breaches happen, and in the event of an attack identify and prioritize risks across the enterprise.

- Define IT policies based on data security best practices and industry standards such as ISO 17799, COBIT, NIST SP800-53, Sarbanes-Oxley, PCI DSS, HIPAA, GLBA and others.
- Align IT policies to key security and operations controls, both procedural and technical.
- Automate the assessment of infrastructure and systems against existing IT compliance controls.
- Measure and report on how well the organization is meeting IT compliance controls.
- Prioritize remediation efforts based on measurement and reporting results, identify deficiencies and proactively update the infrastructure and security systems to demonstrate compliance and ensure maximum security.

Step 5. Prevent data exfiltration. In the event that a hacker incursion is successful, it is still possible to prevent a data breach by using network software to detect and block the exfiltration of confidential data. Insider breaches can likewise be identified and stopped. Data loss prevention and security event management solutions can combine to prevent data breaches during the outbound transmission phase.

- Monitor and prevent data breaches via network transmission, whether by malware, well-meaning or malicious insiders.
- Identify transmissions to known hacker sites and alert security teams to prevent the exfiltration of confidential data.

Step 6. Integrate prevention and response strategies into security operations. In order to prevent data breaches, it is essential to integrate a breach prevention and response plan into the day-to-day operations of the security team. Using technology to monitor and protect information, the security team should be able to continuously improve the plan and progressively reduce risk based on a constantly expanding knowledge of threats and vulnerabilities.

- Integrate solutions for data loss prevention, system protection, compliance, and security management to create an operational model for security that is risk-based, content-aware, responsive to threats in real time, and workflow-driven to automate day-to-day processes and close gaps between people, policies, and technologies.
- Leverage security services—including consulting, education, critical support, and global intelligence services—that provide organizations with deep security knowledge and broad security product expertise.

See appendix for the Symantec solution overview on how to stop breaches.
**How to get started**
The first step in creating a prevention and response plan is to identify the types of information you want to protect and where that information is exposed in your organization. Once you have identified your organization’s priority information and determined your level of risk of data loss, the next step is to assess your network and understand what areas of the infrastructure are leaving you vulnerable to external attacks.

For many organizations, this process begins with an onsite risk assessment. The Information Exposure Assessment offered by Symantec provides customers with a holistic and data-centric view of their organization’s information risk. By combining industry-leading advisory consulting services and data loss prevention technologies, Symantec is uniquely positioned to provide customers with not only a detailed analysis of their exposure to internal and external data breaches, but also a quantitative assessment of actual data loss risk across networks, web applications, storage and endpoints. This combined approach allows for Symantec to deliver a detailed and comprehensive risk mitigation plan focused on priority data loss and data exposure concerns. The result is a detailed plan of action that includes guidance on addressing internal and external risks and recommended activities to reduce and eliminate areas of exposure across the entire organization.

**Why Symantec?**
Symantec understands one of the biggest challenges that organizations face today is how to balance the operational demands for information availability with the need to adequately protect that information from unauthorized disclosure. By engaging in an Information Exposure Assessment—a service by Symantec—customers will gain invaluable insight and visibility into their current information exposure risks, and begin to proactively manage that risk in a coordinated approach.

Symantec is the world leader in security with by far the largest global presence of any security software company. We protect more systems, companies, and communities than anyone. Symantec delivers the highest-rated products and services—and more of them. We also we offer the deepest security expertise and the most comprehensive global intelligence. For organizations that need to protect their vital information, respond to threats rapidly, demonstrate compliance, and manage security efficiently, Symantec is the proven leader.
# Appendix

**Symantec information protection solutions matrix.** Below are the methods discussed in the *How to prevent a breach* section of this paper, cross-referenced with the solutions Symantec offers for data breach prevention.

<table>
<thead>
<tr>
<th>Symantec Solution</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| **Symantec™ Data Loss Prevention Suite**              | • Gain visibility into where confidential data is stored and take automated action to protect the data through quarantine, encryption, or Enterprise Rights Management (ERM).  
• Monitor employee activity on the network and at the endpoints even when users are disconnected from the corporate network.  
• Stop confidential data loss. Automatically quarantine, copy, and remove inappropriately stored data. Protect endpoints whether the user is on or off the corporate network.  
• Automatically enforce universal DLP policies with a centralized platform for detection, incident remediation workflow, reporting, system management, and security. |
| **Symantec™ Protection Suite**                       | • Secure your environment against malware, spam, botnets, and other Web 2.0 threats by accurately identifying and addressing risks across platforms.  
• Secure sensitive data and valuable confidential information at the gateway with advanced content filtering and data loss prevention.  
• Protect proactively with real-time security intelligence that provides early threat warnings and protection from newly evolved threats. |
| **Symantec™ Control Compliance Suite**               | • Define and enforce a policy to protect confidential data across the enterprise.                                                                                              
• Automatically evaluate the effectiveness of technical and procedural controls to enforce IT compliance policies.  
• Import asset information and controls data from third-party devices and applications, such as content-aware data loss prevention solutions, to evaluate controls effectiveness.  
• Deliver role-based dashboard reports on compliance by policy.  
• Remediate deficiencies based on risk-based prioritization. |
| **Altiris™ Total Management Suite from Symantec**    | • Align processes with industry best practices to more efficiently manage client and server systems.  
• Complete lifecycle management including integrated deployment, ongoing systems management, and monitoring functions from a centralized console.  
• Combine enterprise asset and service management into a single Web-based architecture, repository, and console.  
• Improve availability and service levels while reducing costs with powerful ITIL-based incident, problem, change, release, and knowledge management tools. |
| **Information Exposure Assessment—a service by Symantec** | • Understand how confidential information is being used and stored across your business.  
• Conduct an in-depth data loss risk assessment to quantify your data loss risks.  
• Perform targeted penetration tests of networks, systems, and applications where critical information is stored.  
• Report on vulnerabilities that may be used by internal and external attackers to gain access to your critical information. |
About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

NO WARRANTY. The information in this document is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This document may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

12/2009 20049424-1