Anatomy of a Business Data Breach:

Introduction For companies 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 causes of data breaches—well-meaning insiders, targeted attacks from outside the organization, and malicious insiders—and then illustrates each cause to show that breaches can occur in. It also offers a broad perspective on what can be done to stop data breaches, as well as specific recommendations for 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 data breaches, it is essential to understand why they occur. Third-party research into the root causes of data breaches, including data from the Verizon Business Risk Team[2] and the Open Security Foundation[3], 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.[4]

Threat categories over time by percent of breaches. **Well-meaning insiders** Company employees who inadvertently violate data security policies continue to represent a major factor in occurrence 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.[5] 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 negligence.[6] 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 confidential data has been stored, sent, or copied unencrypted by well-meaning insiders, unaware of data security policies, who are captured by hackers. These sorts of exploits typically take advantage of just such data. As a result of data proliferation, most organizations today have no way of knowing how much sensitive data exists on their 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.[7]

• **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.[8] In the 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.[9] 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.

• **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 breach is increased. The Verizon report implicated business partners in 32 percent of all data breaches.[10]

• **Business processes automate the spread of sensitive data.** One reason for proliferation of confidential data is inappropriate or out-of-date business processes that automatically distribute such data to unauthorized individuals or unprotected systems, where it can be easily captured by hackers or stolen by malicious insiders. 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.[11] Such attacks are often automated using malicious code that can penetrate into an organization undetected and export data to 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 an average of more than 245 million attempted malicious code attacks worldwide per month.[12] Measured by records compromised, by far the most frequent types of hack in 2008 were unauthorized access using default or shared credentials, improperly constrained access control lists (ACLs), and SQL injection attacks.[13] In addition, 90 percent of lost records were attributed to the deployment of malware.[14] The first phase of the attack, the initial incursion, is typically perpetrated in one of three ways:

• **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 malware that gives them remote access to the target servers.

• **Targeted malware—**Hackers send emails disguised as legitimate communications from known entities but directing victims to a site that automatically downloads malware, including remote access tools (RATs) that allow the hacker to control the victim's computer remotely. 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.

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

• **Phase 2: Discovery.** The hacker team 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 *rootkits* 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) or 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. On the other hand, by taking precautions against the discovery, capture, and exfiltration of data, organizations can significantly bolster their defenses against targeted attacks. **Four phases of targeted attacks: incursion, discovery, capture, exfiltration**

The malicious insider Malicious insiders constitute drivers for a growing segment of data breaches, and a proportionately greater portion 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 significant 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. All too 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.[1]

• **Career building with company data.** It is not unusual 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.

• **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 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, contentaware, 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. 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. Only 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 "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 network communications, such as email, IM, Web, FTP, P2P, and generic TCP, and enforce policies to proactively block confidential data from leaving the organization through these network exits. • Proactively block confidential data from leaving the organization from endpoints via print, fax or removable media.

Step 2. Automate the review of entitlements to sensitive data. Data breach is often the result of a targeted attack that uses malware to find and export the data—and use of improper credentials is the leading cause of such attacks. By automating regular checks on passwords and other entitlement controls, organizations can reduce the risk of such a breach. In addition, failure to lock down the entitlements of terminated employees in a timely manner is a major contributor to breaches caused by malicious insiders. Automated entitlement reviews can stop such breaches before they happen. Survey tools, controls assessment automation, and security event management solutions enable organizations to prevent breaches that stem from unenforced entitlements. • On a regular basis, automatically send a questionnaire to every manager asking, among other things, "Did you terminate an employee this week?" • Automatically check technical controls on entitlements assigned to the terminated employee, such as Active Directory and Exchange access. • If, after a termination, the disabled credential is used in an attempt to access restricted data or systems, flag the incident for investigation and prevent a potential data loss incident.

Step 3. 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. • Security intelligence services analyze data from billions of email messages and monitor millions of systems worldwide on a daily basis. • Security information and event management systems track network activity, collect incident data from a variety of security systems in real time, and match incident logs against a data feed from security intelligence services to identify known trouble sites and other external threats.

Step 4. Stop incursion by targeted attacks. The top three means of hacker incursion into a company's network are 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, 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, encryption capabilities, and information access. • Automatically scan technical controls across networked servers—including password settings—and report on all policy violations. • Automate polling of administrators to make sure that default passwords are deleted and ACLs are updated. • Use host-based intrusion detection and intrusion prevention systems on servers to safeguard host integrity in case of SQL injection attack and to stop malware from writing to core systems. • Use messaging security to monitor and block the inbound flow of targeted malware. • Centrally deploy and manage endpoint protection, encryption, and network access control to all employee desktops and laptops and implement consistent configuration standards, better operational efficiencies, and improved security protection.

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 malicious insiders or malware. • 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. • Integrated solutions for data loss prevention, system protection, compliance, and security management enable customers 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. • Security services—including consulting, education, critical support, and global intelligence services—provide organizations with deep security knowledge and broad security product expertise. *See appendix for 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 confidential data your organization needs to protect and use that information to measure your risk of exposure. Once you are able to define and prioritize your data risk levels, the next step is to engage stakeholders and form a project team—which should include IT security, compliance, and business data owners—that can evaluate solutions and recommend actions. For many organizations, the process begins with a risk assessment. The Symantec Data Loss Risk Assessment helps organizations quickly identify their confidential information and accurately identify and quantify their risk of a data breach. In a typical engagement, you will be able to quantify your risk of data loss and prioritize your risk by data types, systems, and groups in order to create a data breach prevention and response plan. The Symantec Data Loss Risk Assessment Report identifies top security violations by data type and policy; benchmarks your overall risk profile compared to industry averages; and recommends appropriate business processes, policies, and awareness programs designed to reduce risk.