Making Data Breach Prevention a Matter of Policy in Corporate Governance

Afrah Fathima, Badiuddin Ahmed

[1]Asst. Professor, Dept. of CS&IT, [2]Associate Professor & Head, Dept. of Management & Commerce
MANUU, Hyderabad
afra_fathima@yahoo.com, badiknr@gmail.com

Abstract

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. It seems like every week there is another report of a data breach at a healthcare or education institution or in an organization. Whether the culprit is student downloading sensitive classmate information from a school's network or a random burglar who steals back-up tapes containing the information of millions of patients, it's safe to say the potential for significant financial and personal difficulties is very real. School and university networks, and to a somewhat lesser extent those at hospitals, are particularly vulnerable to breaches compared to other types of businesses. Campus networks are at greater risk because they must be open, carry a lot of data, have many access points and support many portable devices, such as laptops, cell phones and PDA's. In light of the disturbing increase in these types of incidents then, it would behoove all campuses to be vigilant yet realistic regarding their data breach prevention policies, personnel and solutions. Organizations are challenged with securing their data and maintaining regulatory compliance while controlling cost, complexity and risk. In this paper, we discuss breach prevention techniques and policies that can help ensure the customers don't make headlines for the wrong reasons. How to prevent a customer data & what to do when he fails, the information security policies. The emerging technologies to prevent data breaching. Keeping in view about the problems discussed above, this paper suggests to make data prevention techniques as a matter of policy in "Corporate Governance".

Keywords: Corporate Governance, data breaching, external attacks, insider threats, information security.

1. Introduction:

Definition "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted, posting such information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. According to the non- profit consumer organization Privacy Rights Clearinghouse, a total of 227,052,199 individual records containing sensitive personal information were involved in security breaches in the United States between January 2005 and May 2008, excluding incidents where sensitive data was apparently not actually exposed. It may be an intentional or unintentional release of secure information to an untrusted environment.

2. It is essential to understand why Data breaches occur

In order to get ahead of the data breach challenge, it is essential to understand why they occur.

Categories of Attackers

Third-party research into the root causes of data breaches, including data from the **”Verizon Business Risk Team and the Open Security Foundation”**, reveals three main types: well-meaning insiders, targeted attacks and malicious insiders. For example, targeted attacks are often enabled inadvertently by well-meaning insiders when an insider's failure to comply with security policies leads to a breach.

Well-Meaning Insiders.

Insiders pose a significant risk to “Data Security”. Recent incidents have shown that unauthorized insider access can result in fraudulent activity & data leakage. Since insiders are granted access to networks, applications and data systems in order to perform their daily activities, it is not easy to restrict their access. 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% 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% of all cases involved incidents resulting from negligence. Therefore we need to:

1. Monitor user access to reduce errors
2. Alert, block & investigate suspicious activity.
3. Monitor sensitive data usage by all users
4. Identify mitigate exposed system
5. Discover systems containing sensitive data
6. Secure web development

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 difficult 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 using malicious code that can penetrate into an organization undetected and export data to hacker sites

The Malicious Inside

Malicious insiders constitute a growing segment of breach drivers and a proportionately greater portion of the cost to business of data breaches. The Ponemon study found that data breaches involving negligence cost $199 per record while those caused by malicious acts cost $225 per record.

1. Stop malicious users before an attack can be launced.
2. Prevent sensitive data leaks
3. Protect Application data stored in databases
4. Detect and patch Application vulnerabilities

3. Data breach prevention techniques: Helping customers avoid data breaches

No one wants to read about their organization -- or that of their customers -- in the headlines following a breach of customer data or other sensitive information. Data Breach Prevention: 13 Best Practices You Should Implement

According to the Privacy Rights Clearinghouse, between Jan. 3 and June 11, there were 71 reported data breaches at our nation's healthcare and education campuses, and the frequency of these types of incidents only seems to be on the rise. Here are some ways your campus can stem the tide

It seems like every week there is another report of a data breach at a healthcare or education institution. Whether the culprit is student downloading sensitive classmate information from a school's network or a random burglar who steals back-up tapes containing the information of millions of patients, it's safe to say the potential for significant financial and personal difficulties is very real. School and university networks, and to a somewhat lesser extent those at hospitals, are particularly vulnerable to breaches compared to other types of businesses. Campus networks are at greater risk because they must be open, carry a lot of data, have many access points and support many portable devices, such as laptops, cell phones and PDAs. In light of the disturbing increase in these types of incidents, the following best practices may help.

1. Conduct a Risk Assessment

Before any solution is implemented, it is important to know your network's vulnerabilities. According to Southwest Washington Medical Center's Security Compliance Officer **Christopher Paidhrin,** officials must understand what type of information might get exposed, who might expose it, how and where it could be exposed, and what applications use it. Once the vulnerability assessment is completed, its results should be communicated to management and executives so they understand the risks involved and are more likely to support proposed solutions.

2. Categorize the Data

Campuses must then identify and categorize what types of facilities have what level of security. **Paidhrin** suggests campuses "Establish a classification standard: Confidential, restricted and public. Sensitive, private or other mid-levels can be added if needed."

3. Determine Who Has Access

Campus administrators and IT professionals must also determine who has access to various types of data, and access should be granted on a need-to-know basis. Access control can be established based on an individual's role in the organization (role based access control or RBAC). In **Paidhrin's** case, staff members at his hospital must have access to on average six-12 applications (out of more than 200 total for his facility).

4. Manage Your Personnel

One common error institutions make when developing their data breach prevention strategies is assuming employees do not constitute a threat. "They harden the perimeter where they have a firewall," says Ken Pappas, Top Layer Networks' vice president of marketing. "The trouble is the bad guys are already in the building." It is important to conduct background checks on staff. Additionally, there must be enough IT and compliance personnel so the campus can satisfy the expectations stemming from laws like the Health Insurance Portability and Accountability Act (HIPAA).

5. Control the Admin Rights

Controlling the administrator rights of a computer reduces the chances of an insider intentionally or unintentionally downloading malware or malicious code. "If you limit admin privileges or you have two users on a device, one of which is Robert Admin versus just Robert, then when you are operating as Robert and you accidentally click on a Web site that is trying to download something bad to your computer, you are protected," says Penn State's Chief Privacy Officer David Lindstrom. "If you need to download software, then you go in as Robert Admin because you are doing it on purpose.

6. Take a Multi-Layer Approach

A single technology cannot provide complete protection. "They need to be secure at the host [e.g. PCs, cell phones, PDAs] and the network," says Pappas. He recommends campuses have firewalls, anti-virus software, anti-spam, intrusion prevention (IPS), network access control (NAC) and possibly IP white lists. IPS monitors all network traffic for malicious or unwanted behavior, and blocks or prevents those activities. NAC provides an end point inspection of devices being connected to the network, while white lists provide a list of known bad IP addresses.

7. Encrypt Information

Encryption is the process by which information is rendered unreadable to anyone who doesn't have appropriate authorization, and it is highly recommended by network security experts. You need to have an encryption system on the machine so when the portable device is removed, it is encrypted with the same password,says.By encrypting documents and database entries so they can only be decrypted in a policy-controlled way at the application layer, that data is encrypted at all other layers — on the network, disk, USB token, etc. he says. "The data defends itself, as opposed to having to travel over protected channels." He also recommends channel and container encryption (Virtual Private Networks [VPN], Secure Socket Layer [SSL], whole-disk encryption) as a secondary mechanism.

8. Track Portable Devices

Because laptops, PDAs, cell phones and other portable devices are often the sources of data breaches, managing this equipment is critical. Some companies have removed the drivers and physically blocked USB ports to prevent usage. Cell phones in some organizations are not allowed in buildings. Although these kinds of extreme measures might not be appropriate in the campus environment, encryption and RBAC with two factor access control (when possible) are excellent solutions. SSL or VPNs can also be used to transmit sensitive information.

9. Monitor Inexpensive Assets

Although items like thumb drives are relatively inexpensive to purchase, they can contain a lot of valuable information that, if lost or stolen, can cost an organization dearly. It is very important to keep an accurate inventory "even if the assets do not rise to a level of expense that might fall under the capital asset category," says Lindstrom. "It isn't about the device, it's about the information." Additionally, identifying high value data and defending it with encryption can free IT staff of the burden of trying to track every PC and peripheral device.

10. Maintain Physical Access Control

Of the 71 reported incidents from Jan. 3-June 11, only 18 were the result of hackers. Many, if not most of the remaining incidents resulted from laptops, portable hard drives, thumb drives or some other piece of computer equipment being stolen or lost. This highlights the need for physical access control. "When people steal machines, we find they take the ones that are easy [to remove]," Lindstrom comments. Simple solutions like locking office doors, installing card access control to a building or office, locking a device to a work station, locking filing cabinets, logging off a computer or having an auto log off functionality can help to greatly reduce the number of data breaches experienced by a campus. An anti-theft solution that remotely tracks the location of a stolen laptop and destroys files is another option.

11. Dispose of Records Properly

Because many breaches are the result of dumpster diving, it is important to shred, burn or pulverize paper files. Additionally, disks, DVDs and old computers should be erased before being discarded.

12. Implement Policies

Employees must be educated on the security policies of a campus, why they are important and how to protect confidential information. The policies should cover telecommuting, and how staff should store and access data from their homes. Audits can be conducted to determine compliance to these policies. It should be noted, however, that often non-compliance is unintentional because staff frequently don't understand their institutions' privacy and security policies, or the policies are cumbersome. Paidhrin suggests that campuses conduct an annual audit of the full IT security function; a quarterly audit or assessment of information samples for integrity (back-up tapes, financial and HR database reviews, and random file testing); and weekly sample audits of the appropriate use of the Web, E-mail and shared drive resources. Third-party IT security experts can help with this process. Other appropriate processes include using "strong" passwords that change regularly (although this is debated in some circles) and password-activated screen savers.

13. Manage Your Vendors

There are many instances when security breaches are not the fault of campuses, but of the outside contractors tasked with either storing, moving or destroying the records. To guard against this type of threat, campuses should interview vendors and review their security policies regarding employee background screening and data management. "If they don't have a security policy, then give them one," says Pappas. "The vendor should provide you with regular reports of the traffic coming into and going out of your network." Regular audits of contractors and security validations are also recommended. Spies say one of the best ways of protecting data is to mask or de-identify the information that goes to vendors. "There are solid solutions that will encrypt data so outside contractors get data that is internally consistent but doesn't contain genuine Social Security Numbers or other identifying information."

4. Year wise classification of Major incidents of Data Breaching

Well known incidents include:

2009

- In December 2009 a RockYou! Password database was breached containing 32 million user names and plaintext passwords, further compromising the use of weak passwords for any purpose.
- In January 2009 Heartland Payment Systems announced that it had been "the victim of a security breach within its processing system", possibly part of a "global cyber fraud operation".[3] The intrusion has been called the largest criminal breach of card data ever, with estimates of up to 100 million cards from more than 650 financial services companies compromised.[4]

2008

- In January 2008, GE Money, a division of General Electric, discloses that a magnetic tape containing 150,000 social security numbers and in-store credit card information from 650,000 retail customers is known to be missing from an Iron Mountain Incorporated storage facility. J.C. Penney is among 230 retailers affected.[5]
- Horizon Blue Cross and Blue Shield of New Jersey, January, 300,000 members [1]
- Lifeblood, February, 321,000 blood donors [1]
- British National Party membership list leak,[6]

2007

- The 2007 loss of Ohio and Connecticut state data by Accenture
- TJ Maxx, data for 45 million credit and debit accounts[7]

- 2007 UK child benefit data scandal
- CGI Group, August, 283,000 retirees from New York City [1]
- The Gap, September, 800,000 job applicants [1]
- Memorial Blood Center, December, 268,000 blood donors [1]
- Davidson County Election Commission, December, 337,000 voters [1]

2006

- AOL search data scandal (sometimes referred to as a "Data *Valdez*"[8],[9],[10] due to its size)
- Department of Veterans Affairs, May, 28,600,000 veterans, reserves, and active duty military personnel [1],[11]
- Ernst & Young, May, 234,000 customers of Hotels.com (after a similar loss of data on 38,000 employees of Ernst & Young clients in February) [1]
- Boeing, December, 382,000 employees (after similar losses of data on 3,600 employees in April and 161,000 employees in November, 2005) [1]

2005

- Ameriprise Financial, stolen laptop, December 24, 260,000 customer records [1]

5. Information security policies as a measure of safeguarding Data breaching:

Instituting information security policies and procedures is the least expensive way to help combat data loss. Policies and procedures are developed to instill a common set of principles for all personnel. That being said, policies and guidelines are also infrequently enforced. If staff members are not educated on these policies and guidelines, then enforcement becomes almost impossible. To start, help your customers by either assisting them with conducting an information security policy assessment or by offering them the service. Solution providers will need to be well-versed in the use of information security baseline standards, such as ISO 27002 (formerly ISO 17799) and COBIT. Having a thorough understanding of these guidelines will help you (the solution provider) position yourself as a trusted advisor to the client.

7. Emerging technologies for Data Breaching:

There are a variety of products available in the DLP (data loss prevention) category that combines software management and policy implementation and control. These products provide an "automated" mechanism that responds to defined attributes for policy management. DLP vendors that offer such products include Next Labs Inc., Orchestria Corp., and Proof point Inc., Vericept Corp., Verdasys Inc. and Symantec Corp. (via its acquisition of Vontu). Their technologies utilize customizable "policies" defined by the organization to monitor, report against, redirect and stop data flow within the organization's network and computing systems.

"All data breaches cannot be prevented but they can be anticipated having policies, processes and personnel in place to report and respond the breach enables the organization to respond optimally."

8. Conclusion

This paper aims to provide a detailed analysis of data breach. The identified core problems include threats to data confidentiality, unauthorized access of resources on the network, control over accidental exposure of data by authorized resource. In this paper a solution to these identified Problems are proposed. While it is nearly impossible to completely stop all data loss and data leakage, there are a variety of options to mitigate the risk and exposure. However, this is not to say that solution providers should just simply throw an assortment of tools, policies and approaches at the problems. The best value a solution provider can bring to the customer is to understand the organization, its challenges and Obstacles, and develop a strategy that integrates fundamental policies for awareness and education with technologies aimed at preventing the unauthorized removal of corporate information assets, and a comprehensive IT risk management assessment to reduce the risk of breaches and exposure.**9. REFERENCES:**

1. **Data Breaching Wikipedia**

   http://en.wikipedia.org/wiki/Data_breach

2. **Data Breach Prevention Techniques**

   http://searchsecuritychannel.techtarget.com/tip/Data-breach-prevention-techniques- Helping-customers-avoid-data-breaches

3. http://media.techtarget.com/Syndication/SECURITY/Sophos_sSecurityChannel_SO23979_Pocket_EGuide.pdf

4. ***Data breach prevention techniques***: Helping customers avoid data **...**

5. Data breach prevention vs. Response

6. http://www.avalution.com/PDF/Data_Breach_Prevention_vs_Response.pdf

7. http://www.imperva.com/solutions/dbp_data-breach-prevention-overview.html

8. "A Chronology of Data Breaches", Privacy Rights Clearinghouse

9. ^ *When we discuss incidents occurring on NSSs, are we using commonly defined terms?*, "Frequently Asked Questions on Incidents and Spills",

10. Heartland Payment Systems Uncovers Malicious Software In Its Processing System

11. Lessons from the Data Breach at Heartland, *MSNBC*, July 7, 2009

12.GE Money Backup Tape With 650,000 Records Missing At Iron Mountain - Iron Mountain

13. BNP activists' details published - BBC News

14. "T.J. Maxx data theft worse than first reported". msnbc.com. 2007-03-29. Retrieved 2009-02-15. *data Valdez* Doubletongued dictionary

16. *AOL's Massive Data Leak*, Electronic Frontier Foundation

17. "Active-duty troop information part of stolen VA data", *Network World*, June 6, 2006

External Links

- "Most Recent Data Breaches", TeamSHATTER, updated regularly
- "A Chronology of Data Breaches", Privacy Rights Clearinghouse, updated twice a week
- "Identity Theft Resource Center - Data Breaches", Updated weekly with statistical analyses
- "Data Loss Database Open Security Foundation's research project documenting data loss incidents worldwide.
- "Office of Inadequate Security", Breach incidents reported in the media and from primary sources, worldwide.
- "Personal Health Information Privacy", Breach incidents from the health care sector, worldwide.
- "Notices of Security Breaches", New Hampshire Department of Justice
- "Maryland Notice of Information Security Breaches", Maryland Attorney General's Office
- "Breaches Affecting 500 or More Individuals", Breaches reported to the United States Department of Health and Human Services by HIPAA-covered (Health Insurance Portability and Accountability Act) entities.
- "Information That Matter", A data breach responsible disclosure project associated with OWASP Singapore.
- "The Breach Blog", Data breach commentary and analysis.
- "SC Magazine Data Breach Blog", The SC Magazine Data Breach Blog.