ASA

Risk Consultants

Research Note

Impact of Data Breaches

By: Divya Yadav

Applicable Sectors: IT, Retail

Keywords: Hacking, Cyber security, Data breach, Malware

Abstract: Data breach has become prevalent across large, mid-size or small business. With the growing emphasis towards big data companies are more than ever securing huge amounts of data that are used for brand segmentation and targeting. But in this process companies forget that they have a bigger responsibility of safeguarding this data from malicious attacks and hacks that exploit user information. This paper reflects on strategies that most organizations can employ to minimize the impact of data breach and pro-actively protect themselves for such breaches and thefts.

ASA

Risk Consultants

Introduction

A data breach is an incident where confidential, private and sensitive financial or personal identifiable information has been compromised by unauthorized access. Data breaches have become a pervasive problem and organizations have a lot at stake. A new study commissioned by Scott & Scott, LLP, a law and technology services firm focusing on data privacy and network security, confirms that the effects of data breaches are far reaching and can be detrimental to a company of any size[1]. While corporations continue to strengthen their firewalls and use security and compliance measures to protect themselves from such vulnerabilities, hackers and cyber criminals always seem to find some way or the other. These attackers are of course usually the United States which makes it all the more difficult for the authorities to catch these criminals and try them in court. "*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*"[2].

Causes of Data Breach

The most common form of data breach that takes place is a targeted attack by external parties. Protecting this huge amount of data from sophisticated hacking techniques can become quite a challenge[3]. "*These targeted attacks are often automated by using malicious code that can*

penetrate into an organization undetected and export data to remote hacker sites"[4].

But attacking an IT system with a malicious code or malware is only the first step, data breach is a result of sequential processes and for the data breach to be successful or for hackers to get any meaningful information out the data all the phases of the hack need to be successful. A study by Symantec shows that most companies focus on preventing incursions but incursion is only a phase and breach can be stopped at any phase to prevent decryption of the data that has been compromised[5]. Here are the phases:

Incursion: This is definitely the first phase when hackers try to break into the company's system through different types of attacks such as SQL injection, malware, password violation, buffer overflow and so on[6].

Discovery: Hackers then try to map out organizational systems to scan for places where confidential data is stored[7].

Capture: Data that is stored in a not strongly encrypted or unprotected system is immediately captured whereas hackers install components called "root kits" to encrypted network access points to capture confidential data that is part of the organization[8].

Exfiltration: Confidential data package is sent back to hackers in its encrypted format and now the hackers have to decrypt this data to get meaningful information out of it[9].

Therefore if organizations focus on all the four phases it becomes easier for them to protect themselves from such infiltrations. Data breach is just not a one step process and its definitely more than just hacking into a system it is also about where and how organizations store their data, how strongly encrypted it is, what kind of user information they decide to store and so on and focusing on all these minute security points can surely help organizations in securing their data.

Recent Trends and Statistics

Recent trends and statistics in data breach have been very alarming. The scope of the recent Target data breach is still under investigation and the latest figure suggest that data for around 110 million customers was compromised as opposed to the previously reported 40 million that included personal information such as email, names, addresses and debit and credit information including the PINs. The magnitude of this breach is enormous and is currently under investigation by the federal government. This breach will not only impact Target's quarterly results and profits but poses for it a greater brand and reputational risk. To mitigate these losses Target is trying to woo customers by offering them additional discounts, free credit card monitoring and identity theft protection. But is this enough for customers? Neiman Marcus has just announced a data breach as well, with no data yet available on the size of the breach. Retailers are clearly under pressure to enhance their online platforms and earn back users' trust. This sentence does not make

sense so I removed it. Social Media sites have been hacked often in the past two years, case in point Twitter and Snapchat. In case of Snapchat hackers posted customers personal information such as names, email and phone numbers on a public website. Snapchat apologized for this breach but information has already been compromised and hackers can use this information to pose as users to extract more sensitive information such as bank account data and so on.

Sony's Play Station data breach was another significant event that took place in 2011 where customer's stored information such as credit/debit card details, addresses, email id was compromised. Needless to say this hack damaged Sony's reputation and it didn't help its already plunging market worth. Xbox is a market leader in gaming consoles but there was a time when play station lead in this arena, bust such malicious attacks leave long term impacts on minds of the customers which sometimes makes the path to recovery very difficult of not impossible.

Studies by Symantec have shown that data breach can happen across any sector. Organizations may have installed highest form of encryption methods but most of them get attacked due to a minor unprotected data point. Some of the stats presented below by Symantec point indicate the pervasive nature of these data thefts.

- Most data breach victims fell prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack; 79 percent of victims were

targets of opportunity, and 96 percent of attacks were not highly difficult. *2012 Data Breach Investigations Report (DBIR), Verizon Business, April 2012*[10].

- The average cost per record of a healthcare data breach in 2011 was $240, which is 24 percent higher than average. Healthcare data breaches are the fourth highest by industry, behind the financial, pharmaceutical and communications sectors. *2011 Cost of a Data Breach: United States, Ponemon Institute and Symantec, March 2012*[11]

  For more trends and exact numbers in data theft please refer to this study by Symantec http://www.indefenseofdata.com/data-breach-trends-stats/.

Business Impact

Data Breaches not only cost financial loss for companies but offer a huge reputational loss risk. Organizations build customers trust over a long period of time and this trust can be lost in a matter of minutes and can be very hard for them to regain. Many breaches result in class action lawsuits and litigations which can take years to resolve. Brand Risk is another potential risk companies might suffer where public perception of the brand becomes negative and it may take time to rebuild brand equity.

Prevention

Cost of data breaches can be very high from notification and business loss to tangible ones like brand and customer loyalty. According to a 2010 study by Ponemon total data breach costs have grown every year since 2006, and in 2010, data breaches cost companies an average of $214 per compromised record, up $10 (5 percent) from last year[12].

But data breach can always be prevented if right measures are taken at every level and policies and processes are in place.

1. Securing more than just IT systems: Organizations sometimes forget to look beyond their IT systems such employee exit policies, remote access, on and off data storage and so on. Policies and procedures for these processes should be in place to fully secure an organization's working environment[13].

2. A comprehensive breach preparedness plan should be prepared in advance as it will equip management and employees to make faster decisions when a breach occurs. When a data breach of massive proportions occurs it leaves the entire organization in shock and most people aren't aware what to do. This readiness plan will help them overcome such paralysis[14].

3. Employees should be fully aware of the BYOD policies or if they are issued office laptops how to safeguard critical information in those systems. In case a system security is compromised they should quickly report it to the higher authorities so that necessary steps can be taken.

4. Data minimization is a good practice since hackers can't get access that is not stored in the systems. Organizations should refrain from collecting information that isn't required and clean the system on regular basis of irrelevant data[15].

5. Continuous risk assessment and audit of internal controls is required to understand if the company is equipped with dealing newer and upcoming risk threats or vulnerabilities[16]. Performing regular penetration and vulnerability testing also helps identify the weaknesses in the system.

6. It is important to be up to date with the latest security patches and updates. These are especially by targeted by hackers and can pose as a severe security flaw in the system[17].

7. It is important to define security requirements upfront with vendors and organizations should have access and control of offshore data storage or services at all times[18].

Conclusion

Data breach can occur in any sector be it retail, healthcare, IT or finance. But integrating security in the long term risk management[19] and business goals is extremely important for organizations to come out of such targeted attacks. Complex systems make it harder to secure every data point and hackers are on a continuous lookout for an unlocked point through which they can spread their attacks. It is an

enormous task, but there shouldn't be any level of complacency when designing the security check points for systems through which transaction of sensitive information takes place. It will forever remain a work in progress and organizations will have to continuously monitor their systems as a single lapse could cost millions, which will make the road to recovery a mammoth task.

References

[1] "The Business Impact of Data Breach". Retrieved January 11, 2013.

ASA

Risk Consultants

http://www.scottandscottllp.com/main/business_impact_of_data_breach.aspx
[2] "Anatomy of a Data Breach Why Breaches Happen and What to Do About It". Retrieved January 11, 2014. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf
[3] "Anatomy of a Data" n. pag.
[4] "Anatomy of a Data" n. pag.
[5] "Anatomy of a Data" n. pag.
[6] "Anatomy of a Data" n. pag.
[7] "Anatomy of a Data" n. pag.
[8] "Anatomy of a Data" n. pag.
[9] "Anatomy of a Data" n. pag.
[10] "Data Breach Trends & Stats". Retrieved January 12, 2014. http://www.indefenseofdata.com/data-breach-trends-stats/
[11] "Data Breach Trends & Stats" n. pag.
[12] "Data Breach Prevention Tips". Retrieved January 12. 2014. http://www.krollcybersecurity.com/resources/data-security-resources/data-breach-prevention-tips.aspx
[13] Data Breach Prevention Tips n. pag.
[14] Data Breach Prevention Tips n. pag.
[15] Data Breach Prevention Tips n. pag.
[16] Data Breach Prevention Tips n. pag.
[17] Data Breach Prevention Tips n. pag.
[18] Data Breach Prevention Tips n. pag.
[19] https://annualcreditreport.experian.com/assets/data-breach/white-papers/security-as-business-risk.pdf