Global Knowledge®

Expert Reference Series of White Papers

Data Breaches: What Can and Cannot Be Done

Data Breaches: What Can and Cannot Be Done

Rich Hummel, CCNA, CCNAW, CCSI

Introduction

A data breach is the transfer of sensitive information, thought to be secure, to an unintended, untrusted location. Data breaches are omnipresent. Whether it's at a corporate or personal level, the threat of information theft is constant. While we hear about high-profile data breaches on the news, data breaches occur almost daily.

The media would have everyone believe that the only industry threatened by hackers is retail business (see Target and Home Depot). The truth of the matter is, most retailers, having seen the impact of cyber-crimes on its victims, have beefed up their security, and attacks on that industry is trending downward. However, government agencies and military contractors, along with a myriad of other industries, find themselves dealing with cyber espionage. Threat vectors now cover all angles, and the landscape is always changing. The obvious challenge is keeping up to date with threats that are in a constant state of flux. Knowledge of the different types of attacks is critical, as is a plan for taking action before, during, and after an attack.

This paper will focus on data breaches at the corporate/enterprise level. We will look at changes in the threat environment and attack continuum, and what can and can't be done about data breaches.

What Has Changed?

Cyber-attacks have been around for as long as there have been networks. In fact, the Internet was developed to provide an alternative should conventional communications networks in the United States come under attack.

The first computer worm was released in 1988 and shut down 10 percent of computers connected to the Internet. The earliest attacks went unnoticed because before the mid-'90s, the Internet was primarily used by academia and connected mainframes. It wasn't until 1995 that a virus, specifically attacking Microsoft Word documents, was released. And it wasn't for another seven years that Bill Gates announced he would secure Windows.

Until fairly recently, attacks were perpetrated by loosely organized hackers consisting of worms, viruses, and spy/malware. Many of the attacks were exercises in system access, data destruction, altering email systems, or installing relatively harmless spyware programs.

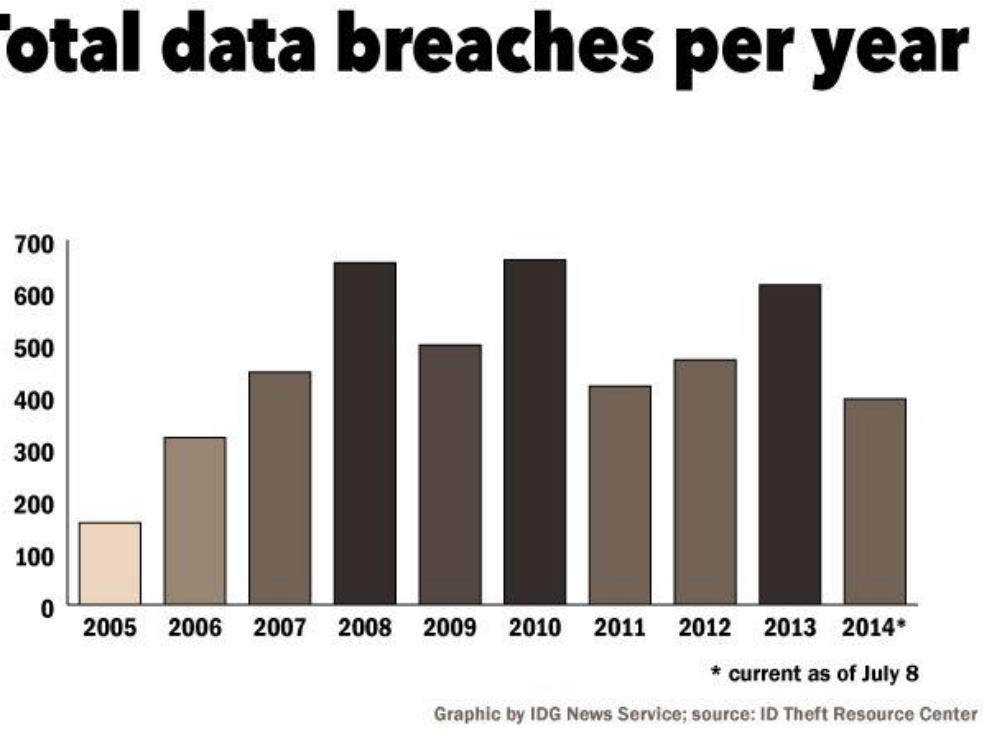

Figure 1: Number of data breaches by year
Source: drforward.com

The landscape has changed dramatically. Hackers are more organized, profit-driven, and often nation-state sponsored. As the Internet has become more profitable, attacks have become more sophisticated. Some of the more common attack methods and reasons for data loss are listed below (discussion of defense techniques and their effectiveness will follow in later sections):

- **Advanced Persistent Threat (APT)**—a concentrated attack by allied hackers focused on a single target. It infects a system and lays dormant and leaves few traces when done. These attacks are generally after the intellectual property of technology companies.
- **Distributed Denial of Service (DDoS)**—typically an attack on an Internet domain. Huge amounts of data flood a system until it is brought to its knees. Legitimate site requests are lost, or the site becomes too slow to function properly. This may not necessarily involve a loss of data, but the cost to its victims is substantial.
- **Cross Platform Malware (CPM)**—malware used to be the concern of those running Windows operating systems. That has changed with emergence of malware targeting Java, Linux, and OSX.
- **Metamorphic and Polymorphic Malware**—malware that has the ability to change code as it works its way through a system. Each version of the code makes permanent changes to its code, but each succeeding version functions the same way as the original. The longer it resides on a system, the more difficult it becomes to detect and remediate.
- **Phishing**—it is what it sounds like. A perpetrator is out there looking to catch a fish. You'll receive an email that looks like it's from your bank, or some other trusted party, asking you to visit their website to update your personal information. The email will include a link to what you think is their website. It will look exactly like the merchant's website. But if you take the time to look at the URL, it will have nothing to do with the website you thought you were visiting. Once you've entered your personal information, the hook is set and they reel you in.

- **Insider and Privilege Misuses/Miscellaneous Errors**—we combine the two here because they are related; the difference being on intent. Misuse of privileges can be by an employee or business partner who is granted privileges and uses those privileges for malicious intent. Errors are can be posting of private information on a public website, or sending information to the wrong recipients.
- **Physical Theft and Loss**—not always the first thing we think about when talking about cyber-crimes, but it is often where a network is most vulnerable. If a hacker was able to penetrate a network, the amount of data available to them is dependent on the response time of the security team and the type of attack. With physical security, once access to a facility's security is compromised, racks of equipment can be removed and accessed.

What Can Be Done to Prevent Data Breaches

We tend to think of cyber security in terms of IT solutions only. After all, it's the IT department they're attacking. In this section we will look at IT security solutions, but we will go beyond that and investigate other aspects of data defense.

Attackers have gotten much faster at breaching systems. Defenders are getting faster too, but they're falling farther behind. Many breaches are detected by third parties other than the victimized organization's IT security professionals, such as law enforcement agencies, specialist fraud detection organizations, or even customers.

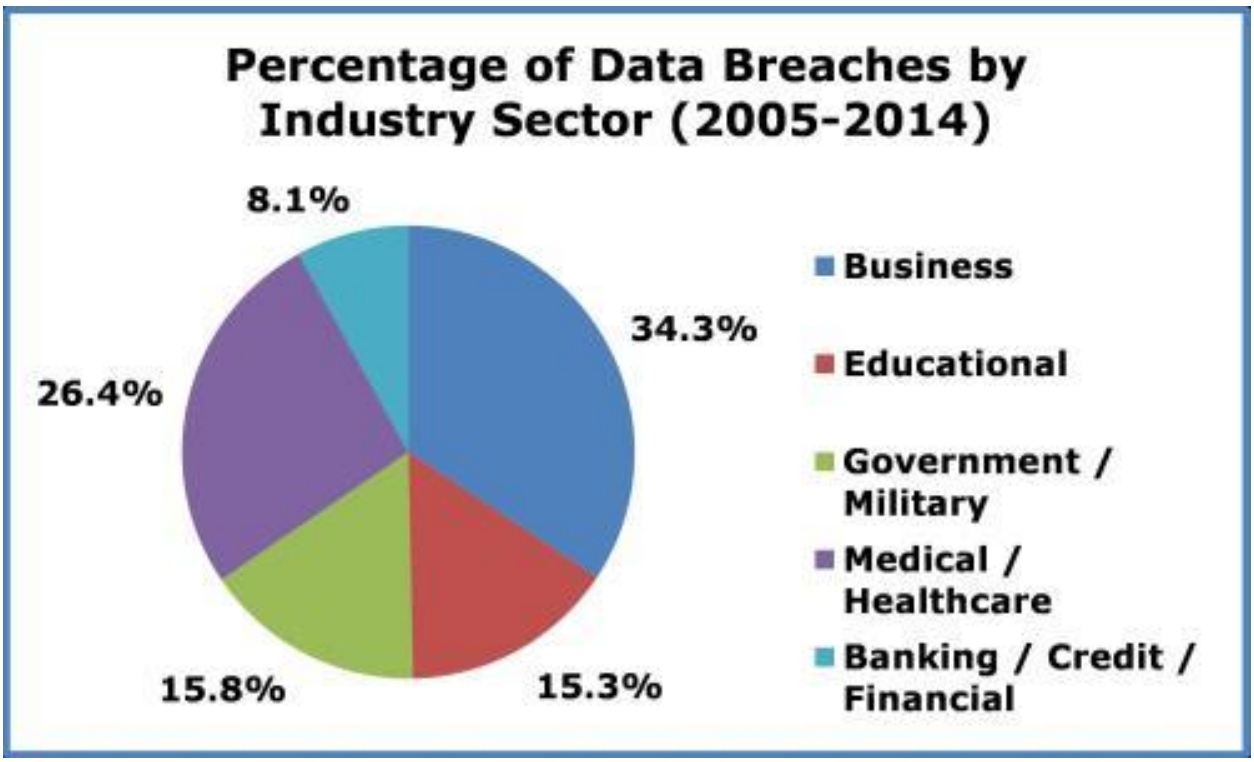

Figure 2: Data Breaches by Industry
Source: fscinteractive.com

The fact that attackers have become more sophisticated requires that we alter the way organizations approach data defense.

But not all data breaches are the results of malicious attacks. The following chart shows the sources of data breaches.

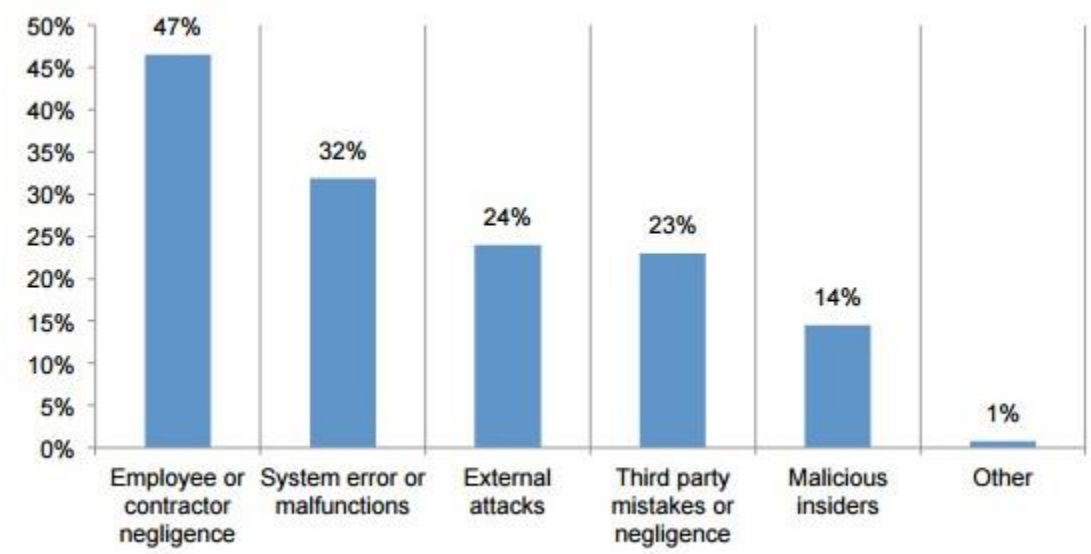

Figure 3: Data Breaches by Source
Source: cognia.com

Let's start by looking beyond the IT security team when assessing an organization's data breach risks. In order to reduce the threat throughout the organization, security must reach beyond the IT department.

- Perform an evaluation of employee exit strategies by the HR department in concert with the IT department, remote project protocol, and data storage practices both on and off site. Then new policies and procedures and physical security appropriate to the findings must be established and enforced.

- Develop and implement a comprehensive data loss protection plan that will enable predefined actions and prevent an organization's operations from grinding to a halt, should a data breach occur. These efforts will demonstrate to your customers and government regulators that your organization has taken proper steps, before an attack, to confront data breach threats. This plan must then be sent to management at all levels to make them aware of the proper steps to take in the event of an attack.

- Educate all employees that have access to data about appropriate handling and protection of sensitive data. Loss of company assets, and personal assets allowed by BYOD practices, exemplify the fact that regardless of the effectiveness of corporate policies that those policies only work when employees follow those rules.

- Hackers can't take what doesn't exist. Minimizing the amount of data an organization stores is a powerful element in reducing the threat of data loss. The rules are very simple:

  - Don't collect information that you don't need.
  - Reduce the number of places where you store the data.
  - Grant employees access to sensitive data on a "need to know" basis, and keep current records of who has access to the data while it is stored on company assets.
  - Completely eradicate the data immediately when it is no longer needed.

- Perform periodic threat and defense assessments. Business models and operational processes change as do risk levels. Determining if new or different risk levels exist can be accomplished through both internal audit and specialized external resources.

- Educate mobile workers on the risks of working remotely. Ensure that the same standards for data security are applied regardless of location, by providing mobile workers with straightforward policies and procedures, ensuring security and authentication software is installed on mobile devices and kept up-to-date, and providing adequate training and technical support for mobile workers.

- Vendors and partners must be held to the same standards as your organization. It's important to define your security requirements upfront with vendors—third-party service providers may be required to maintain appropriate security measures in compliance with certain state and federal regulations. Ensure that your organization maintains control of data at all times, especially with offshore data storage or services.

There are some basic things an IT department can do to protect their data, such as retaining a third-party corporate breach and data security expert to analyze the level of risk and exposure. An evaluation performed by an objective, neutral party leads to a clear and credible picture of what's at stake, without pressuring staff who might otherwise worry that their budgets or careers are in jeopardy if a flaw is revealed. Research shows that organizations with a strong security posture or a formal attack response plan in place prior to the incident can reduce the average cost of a breach.

Don't rely on encryption as your only method of defense. Encrypting data in transit and at rest is a best practice, but, when used alone, it can give businesses a false sense of security. Although the majority of state statutes require notification only if a breach compromises unencrypted personal information, professionals can and do break encryption codes.

Keep current with security software updates (or patches). An unpatched system is, by definition, operating with a weak spot just waiting to be exploited by hackers. Admittedly, applying patches takes time and resources, so senior management must buy into the plan and provide funding and resources.

In order to compete with the current threat environment, IT organizations must change the way they think about security. Historically, security was impulsive and reactive. Today's security paradigm has shifted.

Cisco's acquisition of Sourcefire is a perfect example of this paradigm shift. Cisco's Adaptive Security Appliance (ASA) already provided next generation firewall (NGFW) protection. The addition of Sourcefire Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) provides protection in what is being called the attack continuum: before, during, and after an attack. Sourcefire's FirePOWER service brings contextual awareness by assessing threats proactively, interpreting that data, and then applying the optimal network defense scheme.

Prior to an attack, tools such as NGFW, VPN, and Unified Threat Management (UTM) are used. During an attack, the IDS needs to be able to detect threats from anywhere a threat can turn up. Whether it's on the network, its' endpoints, BYOD's, or virtual machines, the IDS needs to be passively on the lookout for new attacks. Once an attack has occurred, it's time to assess the damage to see how much of the network has been affected. To further the effort, Sourcefire introduces the concept of Retrospective Security. In the past, security worked at a particular moment in time. If a firewall or IPS allowed a malicious entity to penetrate the system, there was no way to re-trace the steps that entity took through your network. Now, with AMP, the process becomes continuous rather than instantaneous.

What Cannot Be Done about Data Theft

There is no way to stop data breaches. We can solve some problems, but the minute one attack is remediated, other, more severe threats arise. There will always be malicious people whose intent is to steal your data. There are so many levels of regress, data theft cannot be stopped. Hackers have become more organized and more sophisticated, making defending data an even more daunting task.

Security will always be a cat and mouse game. As soon as the better mousetrap is built, the mouse will find other ways to get your cheese.

Conclusion

Experts agree that as long as there is data, there will be people trying to steal it. For every defense mechanism put in place, there is someone who will find a way to get around it. Constant vigilance, education of the workforce, and management support are all necessary to implement effective security policies. While a well-trained IT staff is key to protecting data, all employees must understand the importance of protecting company assets, including data.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Cisco Security Training

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Rich Hummel has a bachelor's degree in electrical engineering from New Jersey Institute of Technology, and a master's degree in technology management. He has worked extensively with wireless, video, and cloud technologies.