Security Breaches:
The Risk & How To Mitigate It

Every day new security breaches make the headlines. No company, organization or industry is immune as is evident in these recent high profile data breaches:

- **Anthem, 80 Million Records Breached**
- **Japan Airlines, 750,000 Records Breached**
- **Home Depot, 56 Million Records Breached**
- **JP Morgan Chase, 76 Million Records Breached**
- **Ebay, 145 Million Records Breached**

FBI Cyber Division assistant director, Joseph Demarest, recently issued a warning to companies: "You're going to be hacked. Have a plan."

According to a recent study by the Ponemon Institute, almost half of organizations have suffered at least one security incident in the past 12 months. The implementation of new payment technologies, the increase in ecommerce, and widespread cloud adoption have all contributed to weak links in data security.

It's Not Always Hackers

It's not just malicious cyber attacks or criminal activity that companies need to prepare for; the majority of breaches originate within companies due to human error or employee negligence. Data leakage from business processes or IT failure is commonplace, and device loss is a pervasive problem.

Companies rely heavily on network security to protect their data, but firewalls and monitoring systems can do little to prevent a breach when the access to data is not restrictive enough within an organization. To protect your data, you must know where it is, who has access to it, and who defines that access. You must also put processes in place to revoke access when an employee leaves the company or transfers to a different role. Alerts need to be triggered when mass quantities of data are being transferred. Routine audits of user accounts need to be made to ensure the right people have the right access levels to data so that unauthorized or unsecured access is not permitted by the system.

Attacked From The Inside

A recent leak of client records at Morgan Stanley illustrates this point. In an effort to get ahead, an employee allegedly downloaded 350,000 client records though a back door using a report he had access to, though he did not have access to the records directly. He then took those records and transferred them to his home computer. Morgan Stanley's data loss prevention system caught the breach within eight hours and identified its source, however that wasn't enough time to prevent it from making its way to the Internet. If access roles were better defined, this person would not have had the ability to download the data in the first place. Companies need to establish procedures for safeguarding consumer data and limiting access to that data only to staff members who truly need it to perform their job.

Employee driven breaches are not always intentional. Emails are regularly sent in error to the wrong recipients. Sensitive documents get misfiled and shared with the wrong user groups. Employees unwittingly download malware. Implementing data loss prevention software can block sensitive information from being shared and controls can be established to watch for data transfers out of an organization, but a company must be vigilant in its data security to counter human error.

Loss and theft of employee mobile devices and laptops is also difficult to prevent, however encryption can protect company data stored on those devices. By locking down devices and treating them as corporate assets, even BYOD can be managed. A secure container can separate corporate data and applications from personal ones.

Stolen credentials are often a way in for data hackers. Two factor authentication and account lock out procedures can make it more difficult to exploit employee or customer passwords. Automatic password expiration policies can also help mitigate password theft, but can overburden help desk staff if not managed well. The same applies to companies having the ability to reset passwords on a mass scale as soon as a breach becomes known.

Accountability Has Shifted

Previously IT departments were responsible for managing data security, but with the enormous publicity surrounding data breaches, customers, shareholders, and regulators are now holding business leaders accountable when companies are hit. Top executives at both Target and Sony were recently forced to step down after their high profile data breaches were reported. There is now increased pressure on management teams to have technology and security plans in place and to detect and contain breaches when they do occur.

The Real Costs Of A Security Breach

In 2014, the average data breach cost an organization $5.9 million. These include hard costs such as legal services for compliance and lawsuit defense, audit and consultant services, free or discounted services to victims of the breach and identity protection services. There is also the intangible cost in the loss of consumer and shareholder confidence and goodwill in the company that was breached. These produce far reaching consequences that result in customer churn and a loss of future revenue.

The Solution

Identity and access management solutions can help companies minimize the risk of massive data breaches and provide powerful controls for a response when they do occur. A properly implemented IAM strategy will address risks and responses in a multi-layered approach. From access governance, certification and auditing to real-time threat detection, the IAM solution needs to be carefully designed and orchestrated to provide the strongest balance of prevention and response while aligning with the organization's goals and practices.

For more information on assessing your company's data breach risk and how to mitigate it, contact IDMWORKS for an assessment today.

IDMWORKS

888 - 687 - 0436

BLOG: IDMWORKS.COM/BLOG

SALES@IDMWORKS.COM

WWW.IDMWORKS.COM