Published Article – Technical Writing

Data Security: Internal & External Risk Factors

Published https://creditunionbusiness.com/data-security-internal-external-risk-factors/

Credit Union BUSINESS
THE ONLY ALL-DIGITAL, ALL-BUSINESS RESOURCE FOR CREDIT UNIONS

Data Security: Internal & External Risk Factors

CREDIT UNION BUSINESS January 19, 2016 - No comments 5 (1 votes)

BY BRIAN BERGLUND

Are your credit union's data security measures up to snuff for 2016? If last year is any indication, the financial industry needs to be on high alert for breaches, both internal and external. There are four major data leak points that your CU should be focusing on. Find out what they are.

Nearly every industry from A to Z, including healthcare, the IRS, hotels, prisons, universities, retail, credit agencies, the FBI, brokerage firms, pharmaceuticals, national security/surveillance and, yes, financial institutions,has been impacted by data breaches at some point during the past year. Unfortunately, 2015 ends withthe all-time high of732 data breaches exposing 176,325,059 records.[1]

According to Paul Ausick from 24/7 Wall Street, as of mid-December, 66 breaches occurred in the banking/credit/financial industry. These breaches exposed more than 5,000,000 records,which is nine percent of the total number of breaches for the year and 2.9 percent of the records exposed.

With the turn of the new year, it is no surprise that companies are on alert. They are ramping up their data security from both inside the company and from outside hacker sources.

Security risks and attacks occur in many forms, both internally and externally. Cyber attacks, phishing (social attacks) and malware are the largest threats from outside the company, as experienced recently by the following businesses.

Data Security: Internal & External Risk Factors

Published https://creditunionbusiness.com/data-security-internal-external-risk-factors/

Nearly every industry from A to Z, including healthcare, IRS, hotels, prisons, universities, retail, credit agencies, FBI, brokerage firms, pharmaceuticals, national security/surveillance and yes, financial institutions are impacted by data breaches at some point during the year. Unfortunately, 2015 ends with the all time high of 732 data breaches exposing 176,325,059 records. (1)

According to Paul Ausick from 24/7 Wall Street, as of mid-December, 66 breaches occurred in the banking/credit/financial industry. These breaches exposed more than 5 million records which is 9% of the total number of breaches for the year and 2.9% of the records exposed.

With the turn of the new year, it is no surprise, companies are on alert and ramping up data security from both inside the company and from outside hacker sources.
Security risks and attacks occur in many forms, both internally and externally. Cyber attacks, phishing (social attacks), malware are the largest threats from outside of the company, as experienced recently by the following businesses.

- Personal information for 1.1 Million members was found to be compromised at Blue Cross / Blue Shield. However, member password encryption prevented access to social security numbers, medical claims, employment records, credit card numbers and financial data.

- Premera Blue Cross / Blue Shield was not as fortunate with a breach that compromised 11.2 subscribers' names, birth dates, social security numbers, bank account info, addresses and other information.

- The billion dollar bank cyber heist affected 100 banks around the world. Employee account credentials and privileges were obtained through phishing (social attacks) tactics. Fraudulent transfers and hijacked ATM machines resulted in a loss of $1 billion.

Significant damage can arise through all data breaches, but the silent, unsuspecting and unreported attacks are most harmful and most prevalent across the globe. Small, medium and large businesses have experienced countless opportunities of theft and malicious intent from downloaded data, stolen encrypted drives, printed records, virus installations and human error. Theft, malicious intent and errors account for the majority of internal security exposure.

In fact, Experian, a global information services group, projects that "employees' mistakes will be companies' biggest threat" in 2016. "Although there is heightened sensitivity for cyber attacks amongst business leaders, a majority of companies will miss the mark on the largest threat: employees. Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls. Employees and negligence are the leading cause of security incidents but remain the least reported issue."

Data Security: Internal & External Risk Factors continued

The growing threat from within. U.S. companies and organizations suffered $40 billion in losses from unauthorized use of computers by employees in 2014 (2). According to ZDNet.com, research conducted by the US Computer Emergency Response Team (Cert) estimates that almost 40 percent of IT security breaches are perpetrated by people inside the company.

Criminal attacks are particularly likely to happen from the inside: one recent study estimated that 90 percent of criminal computer crimes were committed by employees of the company attacked.

- Databases were stolen at Epsilon, compromising 60 – 250 million records. (3)
- The breach at Target severely affected business with 110 million records compromised, and the attack was from the inside network (4)
- 54K members of Molina Healthcare were impacted when a former CVS employee downloaded customer information onto his laptop (5)

Internal or external breaches come in all shapes, sizes from various resources and by various types of cybercriminals. Network monitoring of all systems, files and employee activity greatly increases protection for small, medium and large sized businesses including error, data downloads, and theft of data and devices.

Secure the Network from the Four Major Data Leak Points
Have employees? Have data? Risk happens by unintentional human error and intentional theft. There are four major data leak points.

1. EmailMessagingandInstantMessaging.
2. Internetuseincludingusingoff-sitestoragesolutionssuchascloudsharingand file storage applications (Google Drive, DropBox, etc.).
3. USB/RemovableDriveDevices(thumbdrives,CDs,floppydisks,pictures, external hard drives, etc.)
4. Printingisanotherway,simpleandlessdata,butstillanotheravenuetowalk data right out the front door.

Data Security: Internal & External Risk Factors continued

Security Measures within the Network - A Full Service Internal Security Monitoring / Analysis / Reporting System

It is common that as support activities have grown in volume and complexity, IT budgets have decreased, placing added stress on already taxed systems and personnel. As a result, many organizations are still in firefighting mode, combating compliance issues, data breaches, disparate systems and antiquated manual processes within their business and IT operations.

Security oftentimes falls by the wayside, costing more money, frustration and potential for breaches, leaks, and theft. Strengthening the network with an air-tight full-service security system that offers 24/7 monitoring, analysis and reporting is the first step to deter and prevent internal security risks with employees. Surprisingly, an internal monitoring system does not have to be complicated, nor expensive, but a full-service solution should offer the following features.

Key Focus Areas for Control

These are the main focus areas your organizations needs to understand & control:

1. What sensitive data exists and where is it located?
2. Local drives, network drives, databases, etc. Data is everywhere. Can you locate all sensitive content?
3. 2 What user is taking which actions with sensitive data?
4. Users have the ability to email, message, upload, copy and print all your data at any given time. Do you know that is happening?
5. 3 Where is that sensitive data going?
6. Where did the data go? A question that no one wants ta ask.
7. 4 What policies are needed to mitigate the risk of these actions? Do you have policies or procedures in place to mitigate risk?

Important Features & Effective Solutions for Secure Networks

1. Protect customers' sensitive information.
2. Comply with all government regulations such as PCI, GLBA, etc.
3. Secure communications with business partners, brokers and agents.
4. Automatically encrypt e-mail, endpoints and documents according to user security policie
5. Restrict & monitor access to confidential financial information.
6. Monitor, inspect, encrypt and retain any webmail communications.
7. Monitor user actions and retain forensic evidence of any wrong doing.
8. Inspect and monitor content across multiple protocols like social networks and web mail.

Benefits of Internal Security Monitoring System

1. Reducetheft,misuseofinformation.
2. Successful audits.
3. Understand now, what you don't know (where data is, where it is going, how it is being used).

Preventing employees and external hackers from retrieving proprietary data whether personal information or intellectual property is a high priority that can be a well-managed, simple installation that falls within a reasonable budget. The key is to be sure that all the areas for possible breaches are covered, and audit requirements are incorporated into the full-service plan.