Useful Techniques for Safeguarding Your Benefits Information

Protecting organizational information is a company wide task that includes several departments; however, HR is one of the most important because of data to employees for some company's benefits programs.

While every business has a responsibility to safeguard such information through robust security measures, many do not realize the weaknesses that their Administration systems contain – or rather they are ill equipped to deal with them adequately.

Why Cybercriminals Place a High Value on Benefits Data

Information related to employee benefits also contains a lot of personal information and thus becomes the first target of hacker attacks, especially during open enrollment season. Here's why this data is valuable to cybercriminals:

Control of the Personal Identifiable Information (PII)

This means that your personal identifiable information, or PII, is highly valuable to cybercriminals. This may cover anything from passport information, names and address, and banking and financial data. However when these details get into the wrong hands, criminals can use the details towards its owners identity theft or financial fraud.

Unencrypted Financial Data

In benefits enrollment processes, personal financial information such as direct deposit information, which is held by HR systems. If these criminals penetrate these systems, they can carry out card not present payments, alter payroll funds in favor of some accounts, and perform other transactions.

Read complete article- Practical Strategies for Protecting Your Benefits Data

Furthermore, the odds are that stolen salary information can be used to adjust tax deductions and or fraudulent tax refunds. They can also make unauthorized purchases or open an account in the employee's name using the credit card information and at the end they are able to damage the employee's credit and put him/her through a lot of expenses.

Leverage to Disrupt Business Operation

Besides the impact to individuals, information loss of benefits data is also a risk to your business. It will be advantageous to the cybercriminals as it enables them to perform more sophisticated phishing attacks, impersonate the actual employees or the Human Resource department or even conduct jams on certain business processes.

They may also be able to modify the system choices for the benefits or even submit false claims further making your business experience severe monetary losses and a slow healing period.

Analyzing Some Opportunities of Threats in Performing Benefits Administration Procedures

The legacy systems of benefits administration poses your enterprise to diverse risks in terms of the employee and business data. Some of the key areas of concern for your benefits

administration procedures include:

Data breaches from Third-Party Vendors

This is because benefits administration involves several third-party maintenance industries such as insurance providers, benefits brokers, and payroll services, most of which have access to your system. Even if you may have strengthened your internal security in the right ways, these may not necessarily apply to your vendors. This means that if the data of a vendor has been breached by a cybercriminal, he can have full track to reach the business's precious data that is sensitive.

Unsecured Benefits Platforms

Benefit enrollment solutions are web-based and serve as electronic recruitment tools that allow employees to update their benefits selection. Whereas, if these portals are not secured aptly, they can turn themselves into weaknesses that would further act as an entry point for cybercriminals. Your employees likely employ inferior passwords or do not include second-factor authentication for the sake of having it easy for unauthorized users who steal business data from your business systems or business accounts.

Outdated Legacy Systems

The problem of benefits administration systems can also be pointed to legacy software and hardware, which is also very widespread. If you did not address the issue of knowledge or experience in the area of cybersecurity, you might not be aware of old systems or may avoid upgrading, just to avoid system downtimes. This can put your business at risk for data breaches as hackers already know what to expect, and they will attack your poorly maintained systems.

The Human Factor

Surprisingly, HR teams can also become the weakest link in your security chain by default. Some of them include being tricked into falling for phishing scams, following the poor practice of reaping passwords and leakage of data among others. Thus, even though the technical

protection can be great at its best, it leaves one’s employeesCarbon without proper security training and additional read Carbon error can easily bring down the best of security measures.

Also read related article-

Data Security Risks With Human Capital Management Software

Safeguarding Healthcare Data with Onboarding and Offboarding

Explore HRtech News for the latest Tech Trends in Human Resources Technology