Employee Benefit News
ebn

Cyber security: What are criminals doing with your information?

By Daniel Freund

Nearly 90% of American adults were Internet users as of January 2014, according to the Pew Research Center. This trend has been spurred along by decreasing personal computer costs, a spike in online-enabled mobile devices and greater speed and access in communication activities and banking.

The rise in Internet usage corresponds to an increase in data stored online, including all sorts of sensitive personally identifiable information, including names, dates of birth and social security numbers. While fraudsters and scammers have always been around, these bad guys now have greater access to data than ever before. With recent data breaches such as the one at the Office of Personnel Management making headlines, it's more important than ever to ensure that you are putting up your best defenses against potential cyber threats.

Cyber threats exist from pre-meditated attacks and from opportunistic individuals. In the first instance, think of a black market that is constantly scanning for vulnerabilities in websites and companies, or even disgruntled employees willing to sell sensitive information on the black market to the same kind of people. In the second instance, think of someone who happens to see someone else's user name and password on a piece of paper and uses that information to access a bank account and its funds.

The more opportunities there are to access data, through additional users or applications, the larger the target becomes for these bad guys to find a way in.

The costs of cyber attacks

If your role in the health care industry puts you or your company in charge of client data, you are already aware of the importance of safeguarding this data, owing largely to HIPAA. Benefit administrators and benefits enrollment software vendors are aware of and legally mandated to comply with HIPAA. Yet, the cyber threat I'm discussing is a more generalized threat to online data, as credentials are created to access accounts containing PII. The costs of these threats are not always connected to a federal fine or direct monetary loss.

Client trust: If a data breach occurs on your system, clients will lose trust in your company and its ability to appropriately safeguard data, which may lead to retention issues and a decline in business.

Business reputation: Chances are, you have competitors offering a similar service. If it comes out that you've experienced a breach, your company's reputation will suffer in comparison to others out there. Expect your competitors to learn from and capitalize on your mistakes.

Enabling future fraud: Anytime data records are accessed in a cyber-attack, the data can be applied several years down the road to future fraud, putting both consumers and companies at risk of loss. For instance, if an individual takes over the account credentials of a broker or system administrator and accesses PII such as name, date of birth and social security numbers, that individual can sell such data on the black market, which can then be used to open bad insurance policies or for other forms of identity theft down the road.

Your best defense

The people who live and breathe security and especially cyber security will tell you that cyber-attacks cannot be completely prevented. Rather, systems can be put into place to avoid attacks as much as possible and to mitigate the effects if a breach should occur.

One of the key advantages of outsourcing enrollment and benefits management is the partner company's responsibility for and management of data security. Further, such software companies likely have systems for data security and cyber security in place already. At a high level, software providers should be securing physical access to computers and servers while also setting up and monitoring firewalls and auditing user activity.

No matter how reliable the software vendor, business users have to comply with secure policies in order to ensure data security at all points of entry. What does this mean? Stop writing your passwords on post-it notes.

Daniel Freund, CFP, ChFC, CLU, is president of Common Census, Inc.