# Shore Up Benefits Cybersecurity During Open Enrollment

The challenge of keeping employee data safe may be greater this year

By Joanne Sammer
September 2, 2020

Employee data that HR departments and benefits vendors collect during open enrollment is a gold mine for cybercriminals. This year, the challenge of keeping this information safe may be greater, as the COVID-19 pandemic has increased data vulnerabilities that criminals can exploit.

"Since the start of the pandemic, the number of benefit plan members using mobile apps, submitting electronic claims, and taking advantage of virtual enrollment and virtual health care (https://blog.ifebp.org/index.php/pensions-and-benefits-in-the-new-future-of-work) has greatly increased," according to the International Foundation of Employee Benefit Plans.

"From a hacker's perspective, employee benefits data that contains personally identifiable information or even protected health information can be very lucrative," said Riaz Lakhani, senior director of compliance and technology risk management at cybersecurity company Barracuda Networks in Campbell, Calif. This data can include such information as prescriptions, retirement account balances, beneficiaries' names and emergency contacts, he said.

"Employee benefit plans are vulnerable [to cybercriminals] because that's where the money is," said Rob Projansky, a partner with law firm Proskauer Rose in New York.

Should a breach occur, employers could face significant repercussions, such as legal or regulatory action, remediation costs and damaged relationships with employees. For example, "in 401(k)-plan-related cases where someone obtains an employee's password and is able to get a distribution from the account, participants have argued that the employer bears some responsibility," Projansky said.

With so many employees continuing to work from home and away from routines and resources that an office provides, employers and their employee benefits vendors face new data vulnerabilities. In addition to regularly reminding employees on the proper way to handle, store and destroy documents, employers should emphasize additional vulnerabilities, such as how information on paper and computer screens can be picked up by cameras during video calls.

*[SHRM members-only HR Q&A: How can I ensure my company protects personal employee information? (www.shrm.org/resourcesandtools/tools-and-samples/hr-qa/pages/cms_011864.aspx)]*

### Cast a Wide Cybersecurity Net

To protect employees' benefits data, think broadly. All aspects of administering benefits, including the enrollment process, employee behavior and vendor security, should be scrutinized. Here are four key actions:

**1. TIGHTEN UP ENROLLMENT AND ADMINISTRATION.**

Employers can reduce opportunities for data to be stolen or compromised by modifying their open enrollment and administrative processes. For example, safeguard data more effectively by eliminating paper forms and instead using online enrollment that requires passwords and multi-factor authentication.

In addition, requiring employees to actively enroll online instead of allowing them to default to the previous year's benefits selection "forces employees to log in and actively enroll in or decline benefits and review their home addresses, e-mail addresses and personal information to ensure their accuracy," said Melodie Bond-Hillman, director of HR and administration with cybersecurity solutions company XYPRO Technology Corp. in Simi Valley, Calif.

Bond-Hillman also suggested that employers limit the open enrollment period to minimize the amount of time the benefits portal is open to employees and more vulnerable to a breach.

She recommended reducing the use of employees' Social Security numbers as much as possible in benefits administration and instead assigning employee identification numbers.

Employers and their benefits vendors must also be vigilant and look for unusual activity in employee benefits plans, and they should automatically confirm plan changes directly with employees, Bond-Hillman advised.

**2. KNOW WHAT DATA IS BEING KEPT.**

Employers must understand exactly what data they have and where it resides, both internally and with vendors. "We can only protect what we know," Lakhani said. "If an organization cannot pinpoint where its sensitive data lives, it will struggle to secure that data."

New trends in employee benefits can create fresh avenues for data sharing. For example, the growth of telehealth use during the pandemic involves data transfers that could be subject to breaches.

"Sort data into 'buckets' so you can understand the risks to that data," Projansky said. With that information, employers can target staff training and reporting, add loss-prevention technology, and take other actions to protect the data.

**3. TEST EMPLOYEES' PHISHING RESPONSES.**

In the middle of a pandemic, distracted employees working from home may not be as vigilant as usual. As a result, they might more readily click links or provide information in response to phishing e-mail, phone calls and voice mail that use deception to obtain confidential data and personal information.

Hackers try to make their communications look or sound like they are coming from a trusted source. For example, they often make their e-mail appear to be coming from the same domain, or network, as the recipient's so they are perceived as trustworthy.

Conduct regular training on data security while continually sending reminders on what employees need to do to protect employee benefits data. Lakhani also recommended sending test phishing messages to employees to see how they respond.

"We all know not to click on links or share sensitive data with an unknown sender, but [employees may] receive what may look like an e-mail from a colleague from another department asking for details on their benefits," he said. Employers should point out telltale signs that such e-mail may be a scam, such as if the sender asks for a reply that requires the employee to share his or her Social Security number.

**4. DON'T FORGET VENDORS.**

Vendors, many of whom are also likely to have employees working from home, can also create vulnerabilities for an employer's benefits plan data and information. "Every vendor that receives and handles employee benefits data creates a potential opportunity for loss," Projansky said. Therefore, employers should be having discussions with vendors about how the vendors are managing cybersecurity and

responding to emerging vulnerabilities.

It is also a good idea to audit the vendor-selection process periodically to make sure there is an adequate focus on cybersecurity. For example, employers can have vendors complete detailed questionnaires about their cybersecurity practices and follow up with an evaluation of each vendor and any subcontractors the vendor uses. "Can you comfortably answer how mature each vendor's cybersecurity program is?" Lakhani asked.

**Protect an Investment**

Employee benefits are a key part of every employer's brand and value proposition. Few things would undermine employees' faith in an organization more than a data breach that causes economic harm to those employees or violates their privacy, no matter how rich the benefits package may be.

Making sure benefits plans are as invulnerable as possible to data theft should be a cornerstone of these programs.

*Joanne Sammer is a New Jersey-based business and financial writer.*

*[Visit SHRM's resource page on Open Enrollment (www.shrm.org/ResourcesAndTools/Pages/open-enrollment.aspx).]*

**Related SHRM Articles:**

‘Vishing’ Attacks on Remote Workers on the Rise (www.shrm.org/ResourcesAndTools/hr-topics/technology/Pages/Vishing-Voice-Phishing-Attacks-Remote-Workers.aspx), *SHRM Online*, September 2020

How to Maintain Cybersecurity for Your Remote Workers (www.shrm.org/resourcesandtools/hr-topics/technology/pages/how-to-maintain-cybersecurity-for-your-remote-workers.aspx), *SHRM Online*, March 2020

The Cybersecurity Challenge (www.shrm.org/hr-today/news/all-things-work/pages/the-cybersecurity-challenge.aspx), *SHRM Online*, October 2019

401(k) Plans: A Cybersecurity Afterthought (www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/benefits-cybersecurity.aspx), *SHRM Online*, February 2018

13 Ways to Reduce Cyberattack Vulnerability (www.shrm.org/resourcesandtools/hr-topics/technology/pages/13-ways-to-reduce-cyberattack-vulnerability.aspx), *SHRM Online*, July 2018

Guarding Benefits Plans from Cyberattacks (www.shrm.org/hr-today/news/hr-magazine/0917/pages/how-to-guard-benefits-plans-from-cyberattacks.aspx), *HR Magazine*, August 2017

**Related SHRM Resources:**

*Open Enrollment Guide & Resources (www.shrm.org/ResourcesAndTools/hr-topics/benefits/Pages/Open-Enrollment-Benefits-Guide.aspx)*

Email Address

CONTACT US (WWW.SHRM.ORG/ABOUT-SHRM/PAGES/CONTACT-US.ASPX) | 800.283.SHRM (7476)