Benefits Insights

Brought to you by the insurance professionals at
National Insurance Services

Cybercrime and Benefits Plans

According to recent estimates from the University of Maryland, there is a cyberattack every 39 seconds. Data breaches and cyberattacks are daily headlines—and employee benefits plans are no exception to that threat.

In fact, employee benefits plans are even more vulnerable as the coronavirus pandemic continues. Organizations and benefits providers are relying heavily on electronic access, ultimately creating new vulnerabilities.

The Risks

Virtually any type of employee benefits plan is vulnerable to hackers. The plans can be exposed to risks relating to privacy, security and fraud.

Retirement, savings and health plans are attractive targets for cybercriminals seeking access to plan assets and the personal information of participants and beneficiaries. Sensitive information is valuable information when it comes to cyberattacks.

Benefits plans are at risk as a result of the following factors:

- **Personally identifiable information** such as Social Security numbers, birthdates and email addresses have significant value to hackers. That information can be misused over a long period of time since it is permanently associated with an individual.
- **Financial information,** including enrollment data, account balances, direct deposit information and compensation are highly attractive. Hackers could target those online accounts to request loans, distributions and withdrawals.
- Lastly, there are **multiple attack points** for hackers since benefit plans are connected to several outside service providers, such as those that offer retirement plans, health insurance, vision insurance, dental insurance, short-term or long-term disability insurance, and flexible spending accounts.

Some examples of cyberthreats include phishing, malware and ransomware attacks. Lost or stolen mobile devices, laptops and flash drives that hold personal information are additional tangible threats to benefits plans.

The Consequences

Cyberattacks on benefits plans can have substantial consequences for all parties involved. Consider the following:

- Significant costs may be incurred in detecting the extent of the breach, investigating and managing the incident response, recovering compromised data and restoring overall system integrity.
- The theft of personally identifiable information and other plan assets may result in monetary losses to participants, beneficiaries, the plan, the plan sponsor and service providers.
- Organizations may experience operational disruption and reputation damage as a result of a security breach. Additional costs will be incurred to respond to and resolve either of those issues.
- Breaches of health plans may result in potential violations of the federal law that restricts release of medical information, exposing the plan sponsor and service providers to fines.

NIS
National Insurance Services

Mitigating Risks

As many employees and providers may be working from home, it's especially important to understand cyberthreats and how to proactively protect sensitive organization and employee information. To mitigate cyber risks, consider the following measures:

- **Properly monitor technology.** To better protect and control data, it's important to maintain up-to-date technology across the organization. Identify current vulnerabilities by conducting a gap analysis, penetration testing or other assessments.
- **Educate employees.** Start with properly training employees, especially those who are working remotely, on how to handle personnel data. This could be as simple as compiling and sharing cybersecurity tips. Think about physically protecting electronic devices and information (e.g., locking laptops and hiding information on camera) in addition to secure document storage and destruction. Pay special attention to common risks like passwords, attachments and Wi-Fi networks. Employees should always be vigilant, but may have their guards down while working from home.
- **Educate participants.** Similar to the points above, it's important to educate participants about cybersecurity and different kinds of potential threats. It's a good idea to thoroughly explore and ask questions about service providers' security policies.

To shift cyber risks, consider the following measures:

- **Review contracts.** Legacy contracts don't consider modern-day cyber risks. It's important to review contractual arrangements to ensure vendors provide an appropriate level of protection against cyber risks.
- **Obtain comprehensive insurance policies.** Cyber liability insurance covers financial losses that result from data breaches and other cyber incidents. Most policies include both first-party and third-party liability coverages. It's important to review and understand business insurance policies to understand whether additional coverage is needed.

With many employees working remotely as a result of the pandemic, plan sponsors should consider updating work-from-home policies to include cybersecurity clauses.

Other Considerations

Open enrollment season is a good time to carefully review organization and vendor security technology and policies, along with any contracts, insurance or other coverage. All parties involved should have adequate data protection strategies in place.

Always be prepared for the worst to happen. In the unfortunate event of a security breach, it's important to be prepared with a basic communication and action plan. Even better, incorporate security breaches in an organization's comprehensive reputation management plan. Keep in mind all internal and external audiences, and appropriate actions to protect information and restore overall system integrity. If not handled quickly and appropriately, reputational damage could be an additional threat to all parties involved in employee benefits plans.

To learn more about mitigating cyber risks in today's digital world, contact National Insurance Services today.