Cybersecurity risks to employee benefit plans

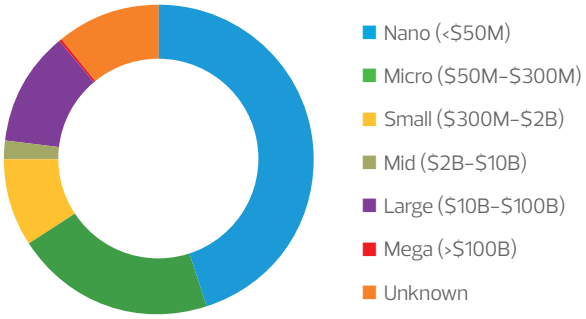
What if you logged into your system to help a client and discovered that everything is encrypted and being held for a ransom of $1.7 million? Or what about that moment when you realize that your organization was just duped into transferring $283,000 not to a client but to a fraudster?

While these situations may sound like exaggerations, they are happening every day. Increasingly, benefit plans are being targeted by hackers; this risk threatens plan administrators, participants, third-party record-keepers and payroll providers. Many organizations feel that they are too small to be targets; however, this perception of safety is tenuous at best. Retirement, health and welfare plans are tempting targets for hackers, but there are steps that organizations can take to protect themselves, their plans and their participants.

Company size does matter

It is difficult to make risk management decisions without understanding the realistic level of risk. Most of the cyber incidents we see in the media are high-profile attacks of large, well-known companies. These cyberattacks are not the rule but the extreme exceptions. Based on the 2019 NetDiligence Cyber Claims Study, which contains an extensive study of insurance claims for damages of cyber-related events from 2014—2018, the vast majority of the claims (about 84%) are from companies with revenues under $2 billion. In fact, most of these companies (about 74%) generate under $300 million. Companies that rationalize their risk decisions by thinking they are too small to be targets are setting themselves up to be victims.

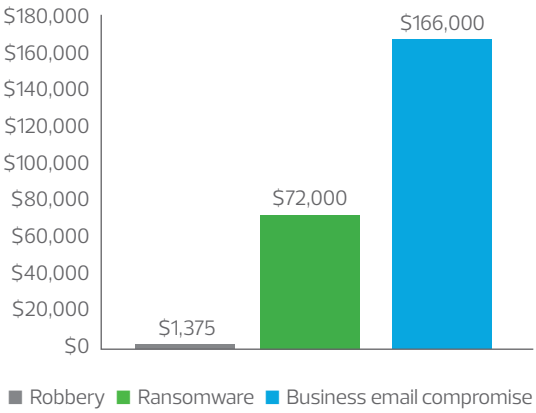
Cyber-related insurance claims by company size, 2014–2018



The cost is real

The financial and reputational damage of a cyber incident can be high, especially for benefit plans where more than $1 trillion in combined contributions and benefit payments flow through retirement plans every year in the United States. There is a lot at risk, and no employee benefit plan is immune. Regulatory claims are becoming more onerous, with the average claim in the last year hovering around $6 million. Notifications telling participants what was lost are becoming more expensive as well.

Average financial loss



The most common cyber incidents that companies are dealing with today are ransomware and business email compromise attacks, which lead to some type of financial fraud. The scenarios noted at the beginning are real, and the numbers can be staggering. For example, an average robbery will earn the thief approximately $1,373. On average, a ransomware attack or business email compromise-related fraud will land the cyber attacker $72,000 and $166,000, respectively. The return on investment is significant and the downside risk is minimal. As a result, companies are targeted via cyberthreats so the attacker can make easy money.

Don't forget the insider threat

While the number has slowly fallen, nearly one quarter of claims had some type of insider involvement, either by employee mistake or through intentional action. It is worth noting that maliciously motivated insider events resulted in more expensive claims. To make matters more egregious (and expensive), the fact that the incident occurred, or the factors that allowed the incident to spread, often reveal that a company's controls were not effective. Regulatory bodies alerted to an incident can declare such a company retroactively noncompliant, then fine it for the total period they feel it was in violation. Costs related to regulatory actions can be further exacerbated if an organization is required to participate in an ongoing assessment program at the organization's expense.

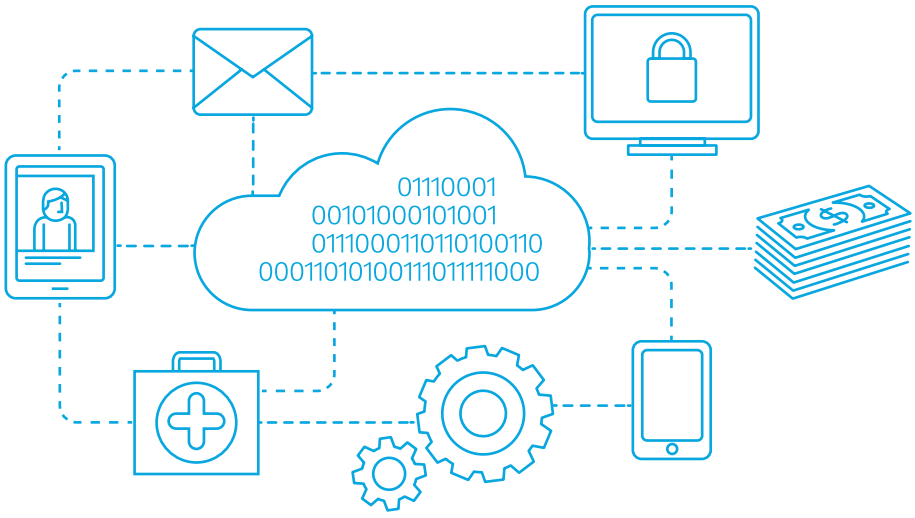
You are the target

Cyber events based on an attack against the user comprise 48% of the claims, while only 39% are related to a technical attack, such as hacking and malware. The attacks that are more focused on us, the everyday user, are more varied, and include attacks such as social engineering, phishing, staff mistakes and lost devices. Despite the everyday user generating the greater risk, most companies spend the vast majority of their time and resources on technical defenses and discount the human risks. The best risk strategies address both technical areas and user awareness and training.

There are a number of threat scenarios that can lead to a cyber incident; however, there are two primary attack types we are seeing over and over.

- **Phishing:** Users are often attacked through emails with links to fake websites. The attacker relies on human nature to gain user credentials and other information to gain unauthorized access to various data and systems.
- **Social engineering and stolen data:** Attackers use social media and corporate websites to perform reconnaissance to develop social engineering attacks against users. These attacks are often well designed so the attacker may be able to represent themselves as a benefit plan client or an internal employee.

These deceptions are hitting benefit plans, often through bogus requests for access, demands to move funds, appeals for contact or contract information, or other manipulations. These breaches are usually considered the company's fault, unless it can be proven otherwise. It's worth noting that end users are most often hacked without the company's involvement. The hacker is gaining access to the participant's assets not by breaching the company, but breaching the user's account directly.



What should you do?

There are a number of considerations and proactive steps that companies can take to help prevent against a cyber incident. While these proactive actions are a good start, remember that attackers continue to develop new techniques to compromise systems and gain access to critical applications that may contain sensitive information. No organization is completely safe against cyberattacks, regardless of the efforts taken to be proactive in preventing an incident. The key is to stop an attack when it is merely a security incident before it becomes a full-blown data breach.

- **Ransomware—to pay, or not to pay:** The question that is frequently asked when a company suffers a ransomware attack is "Should we pay the ransom?" The decision of whether to pay ransom when your company has been infected with ransomware is largely a business decision. While there is no correct answer with how to proceed, there are some key points to consider:
  - Do you have a way to pay the ransom?
  - Are there viable backups?
  - How urgent is the need or timing to become operational again?
  - What types of data are encrypted? Not all data handles the encryption and decryption process well.
  - Ultimately, what is the cost/benefit analysis of paying the ransom versus restoring or completely rebuilding your environment?

- **Social engineering awareness training:** Companies need to make sure that they are implementing security awareness training to everyone involved in the plan administration as well as participants of the plan. Many employees simply do not understand the methods used in social engineering, and this makes them vulnerable to fall victim to such attacks. Do not excuse executives from this type of training; they are the most common targets and can be just as vulnerable. Design the awareness training to include information that you will never ask (i.e., user name and password, account number), as well as how communication will be handled (i.e., you will never call and ask for information). It is also important to make sure that everyone is aware of how to report a potential social engineering or phishing attack.
- **Incident response preparedness:** A response plan is only as effective as the supporting components to make it work. Management should recognize when it is in over its head. The urge to try to manage it internally is overwhelming, but the appearance of delaying a response can cost companies in lawsuits and fines later. It also often leads to the destruction of evidence of the attack, but not the elimination of the hacker from the environment. Companies should do a triage to stop the attack from getting worse, then take their hands off the keyboards and call in the incident response team.
- **Insurance:** This is the last line of defense. Companies should not count on cyber insurance being covered under a general policy; it is often specifically stated that a separate, stand-alone policy is required for cyber incidents. Make sure the policy is covering the most common costs (e.g., ransom payments). Management should make sure that contracts cover fines and that the sublimits are reasonable.

Even despite these proactive steps, attackers continue to develop new techniques to compromise systems and gain access to critical applications that may contain sensitive information. No organization is completely safe against cyberattacks, regardless of the efforts taken to be proactive in preventing an incident. The key is to stop an attack when it is merely a security incident before it becomes a full-blown data breach.

+1 800 274 3978
rsmus.com

gr-nt-as-all-1119