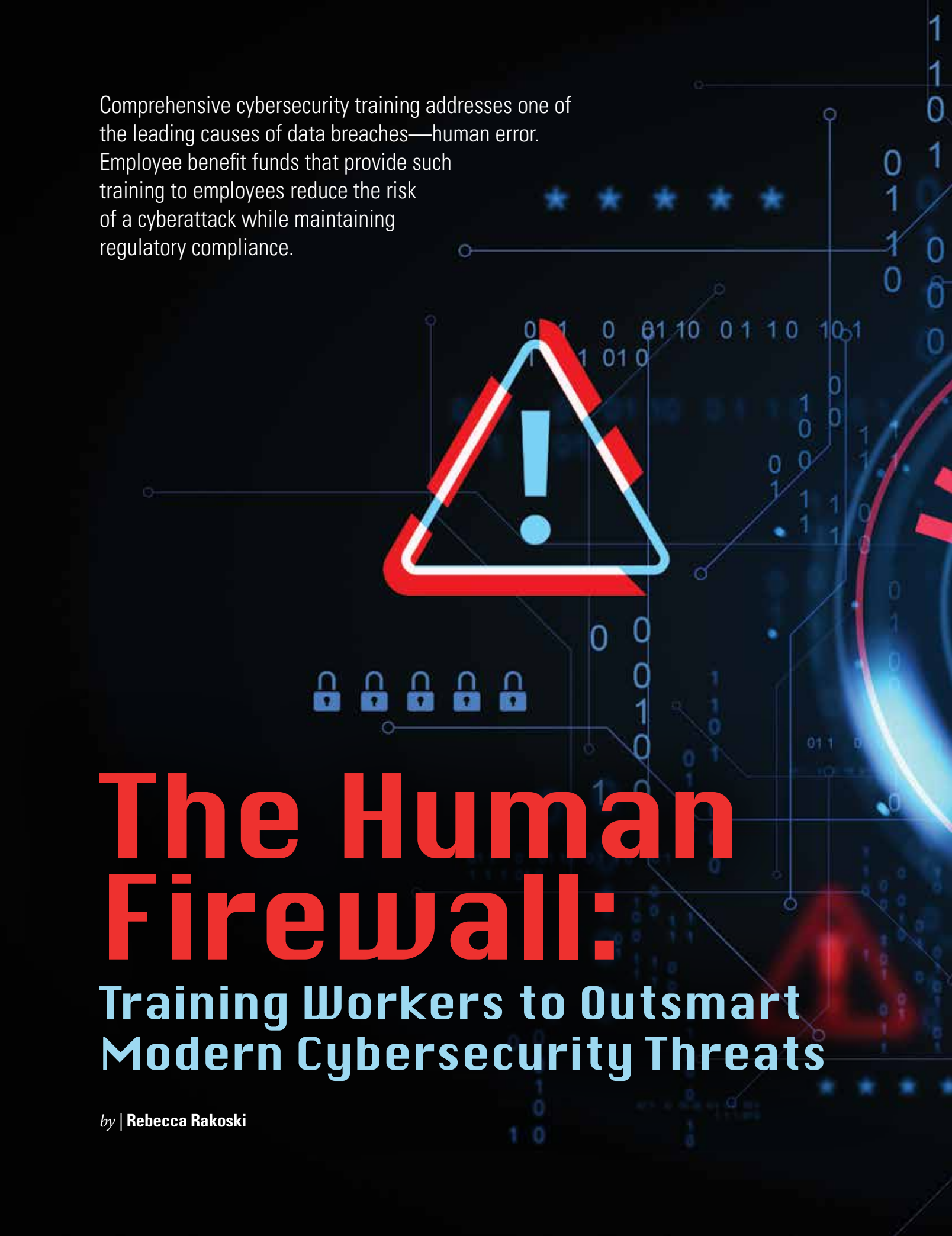
Comprehensive cybersecurity training addresses one of the leading causes of data breaches—human error. Employee benefit funds that provide such training to employees reduce the risk of a cyberattack while maintaining regulatory compliance.



The Human Firewall:

Training Workers to Outsmart Modern Cybersecurity Threats

by | **Rebecca Rakoski**

benefits MAGAZINE

In today's digital environment, cybersecurity cannot be just an information technology (IT) concern for organizations. Instead, it is a critical and fundamental operational, legal and governance imperative. Organizations face increasingly sophisticated cybersecurity threats, from phishing and ransomware to insider risks and social engineering attacks. Not to mention that the advancements in artificial intelligence (AI), specifically generative AI, have changed the game, giving hackers a strong advantage.

Organizations recognize that technology plays an essential role in defense. At the same time, employees treat training as a rote task that is engaged in with a certain amount of annoyance and contempt, which may be understandable given the current blueprint for training. Training videos can be boring and repetitive. More times than not, employees find them funny rather than informative, which means employees treat the training as a "joke" rather than a serious learning exercise. What has not changed, though, is that employees remain the most important and, by extension, the most vulnerable, first and last line of defense. For this reason, providing employees with comprehensive cybersecurity training is not optional. Rather, it is a strategic necessity tied directly to regulatory compliance, organizational resilience and legal liability management.

Legal Requirements

Cybersecurity training is a key requirement under numerous regulatory frameworks, including the Department of Labor (DOL), the Health Insurance Portability and Accountability Act (HIPAA), and state governments.

Department of Labor

The DOL's cybersecurity guidelines are clear that protecting health and retirement plan data is a fiduciary responsibility.[1] This responsibility extends to ensuring that all staff not only understand the threats that they may encounter but also their role and responsibility in protecting fund member data. Even more important, employees play a key role in identifying fraud and fraudulent transfers of funds that could cause an enormous loss to the organization.

This is why the DOL guidelines emphasize the importance of formal cybersecurity awareness training that is routinely updated and documented. And while the DOL guidelines do not specify the type of training required, employees should be both aware of and trained on the organization's cybersecurity program (i.e., its policies and procedures). This ensures that employees fully understand what is expected of them but also makes them a partner in cybersecurity by helping them understand the "why." This ultimately allows employees to be a part of the defensive posture and therefore reduces risk and liability for the organization.

HIPAA

The DOL guidelines are not the only legal requirement for cybersecurity training. HIPAA also requires covered entities and business associates to provide ongoing security awareness training to all employees.[2] HIPAA training is about educating staff on threat detection, password management, malicious software prevention and breach reporting protocols. A failure to train, or even insufficient training, is a most frequently cited deficiency during HIPAA investigations that occur after a data breach.

In addition, failing to train or providing insufficient training (which arguably could compound vulnerability by creating a false sense of security) can play an unfortunate and central role in civil penalties, compliance actions and lawsuits that inevitably follow a data breach.

State Regulations

Federal regulations are not the only game in town. Numerous states have their own privacy laws and proactive cybersecurity regulations, along with enforcement actions and penalties, that require organizations to demonstrate that employees receive meaningful cybersecurity and data protection training.

Cybersecurity Training: An Ounce of Prevention

A well-trained workforce significantly strengthens an organization's security posture. While organizations continue to view cybersecurity as a "tech problem," human error remains one of the leading causes of data breaches, whether

takeaways

- Benefit fund offices must provide employees with comprehensive cybersecurity training to comply with state and federal regulations and protect the organization.
- Benefit funds are attractive targets for cybercriminals because they handle a large volume of sensitive personal, financial and health information belonging to their participants and beneficiaries.
- Numerous regulatory frameworks, including the Health Insurance Portability and Accountability Act (HIPAA), guidance from the Department of Labor and state regulations, require organizations to provide cybersecurity training to employees.
- Cybersecurity training helps employees recognize real-world threats and understand the implications of poor security practices. Training also encourages employees to ask questions and develop habits that support everyday risk mitigation.
- Artificial intelligence (AI) has significantly and rapidly transformed the threat landscape. For example, AI-generated phishing emails now mimic the tone, writing style and formatting of trusted service providers, making them far more convincing.

an employee mishandles sensitive information or falls victim to phishing or social engineering schemes.

Plus, the initial discovery may require tech to triage the problem, but an organization's legal team is candidly the surgeon who will determine how well the organization recovers (e.g., mitigating postbreach fallout, following the time-sensitive requirements/obligations set forth under numerous laws and regulations, handling potential regulatory inquiries and enforcement actions and, of course, protecting the organization from exhausting and protracted litigation in the courts). The legal costs associated with a postbreach response can be staggering and will only increase when preventive measures have not been taken.

Cybersecurity training helps employees recognize real-world threats and understand the implications of poor security practices. Training also encourages employees to ask questions and develop habits that support everyday risk mitigation.

Every employee needs to be considered an integral part of the organization's cybersecurity response team. By identifying suspicious communications, safeguarding credentials and reporting potential incidents promptly, these employees will play a critical role in safeguarding the organization's data and monetary funds, as well as the limits of its legal liability and exposure.

Heightened awareness has been repeatedly shown to reduce the likelihood of successful attacks and/or to improve response times, mitigating the impact of these data incidents. No matter how one looks at it, the fact is that cybersecurity training is a cost-effective investment that an organization can engage in, but it must be considered a solution that works best when applied preventively and not reactively.

Cybersecurity and Benefit Fund Offices

Increased Risk

Cybersecurity training is particularly important for multiemployer benefit fund offices. Fund offices face a unique combination of threats and obligations that make cybersecurity training a critical component in their cybersecurity programs.

These organizations are particularly attractive targets because they handle large volumes of sensitive personal, financial and health information that belongs to their participants and beneficiaries. Data breaches that impact pension data, health plan information, collective bargaining strategies or membership records could have severe consequences, both financial and reputational. In fact, data breaches can damage the integrity of the organization itself.

Cybercriminals also recognize that these organizations may not have the same level of cybersecurity investment as large corporations, yet they control substantial financial assets and maintain vast repositories of member information. Phishing campaigns, fraudulent fund transfer attempts and ransomware attacks have all been directed at unions and multiemployer benefit plans in recent years.

Role of Artificial Intelligence

Moreover, the rise of AI has significantly and rapidly transformed the threat landscape, giving cybercriminals powerful new tools to deceive employees with unprecedented precision

Data Breaches by the Numbers

IBM's *Cost of a Data Breach Report 2025* provides the following statistics on data breaches.

- The average cost of a data breach in the U.S. was $10.22 million in 2025, up from $9.36 million in 2024.
- Sixteen percent of global data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%).
- Phishing was the most common initial vector that attackers used to gain access to systems at 16%.
- Employees' personally identifiable information (PII), which includes names and Social Security numbers, was targeted in 37% of breaches, and 53% of breaches targeted customer PII.

learn more

Education

72nd Annual Employee Benefits Conference
October 25-28, New Orleans, Louisiana
Visit *www.ifebp.org/usannual* for more information

Online Resource

Cybersecurity Toolkit
Visit *www.ifebp.org/toolkits* for more details.

while leaving organizations little to no time to catch up. AI-generated phishing emails now mimic the tone, writing style and formatting of trusted service providers, making them far more convincing than the poorly written scams of the past.

As AI-enabled attacks become more sophisticated and harder to detect, updated and current employee training that accounts for these shifting criminal AI strategies plays even more of a central and defensive role in preventing these schemes, particularly because so many attacks rely on social engineering. In addition, having policies and procedures in place that require staff to have multiple levels of checks before changes are made or funds are redirected is often the last best line of defense from the last defensive lever being compromised by these attacks.

Fiduciary Responsibility

Finally, under federal law and regulation, benefit funds, pension funds, and health and welfare funds are subject to a higher fiduciary standard compared with other organizations. The DOL guidelines speak specifically to this heightened fiduciary duty and state that it applies directly to benefit plans, including multiemployer pension and welfare funds. Ensuring that personnel are properly trained is a key component of that fiduciary responsibility. Failing to do so may expose not only the organization but also its trustees to scrutiny or liability. For benefit funds handling health information, HIPAA obligations further underscore the necessity of training.

Cybersecurity training for employees is so much more than a box to be checked, especially for benefit funds. It is a key element of modern responsibility and an essential safeguard for sensitive information. By engaging in cybersecurity training, organizations not only maintain legal compliance but also reduce risk, strengthen operational resilience and limit potential costly litigation, along with regulatory exposure and protracted enforcement actions. In an era of evolving digital threats, a trained and vigilant workforce remains one of the most effective defenses available and a clear indicator of a mature and responsible organization.

Training Content

Cybersecurity training should cover the following subject matter.

- **Nature of the threats posed**: For example, since AI has changed the threat landscape, training needs to change to address that. Educating staff to identify and respond to suspicious emails, unexpected credential requests or false vendor invoices can stop an attack before any damage occurs.
- **Organizational cybersecurity policies and procedures:** By understanding the "why" behind the training, employees become partners in the defensive posture, actively reducing risk and legal liability for the organization.
- **Legal ramifications:** Employees should be made aware of the consequences organizations face if they fail to address cybersecurity. Including elements of costs and how that could affect the organization as a whole, along with the role and function of cybersecurity, are critical to ensure employees understand the importance of cybersecurity.
- **Reporting:** Funds that want employees to be partners in the war on cyberbreaches should empower employees with knowledge on how to report suspicious activity.

This holistic approach transforms employees from potential vulnerabilities into an empowered and active defensive layer, crucial for mitigating risk and ensuring the organization's long-term resilience.

bio

Rebecca Rakoski is the co-founder and managing partner at XPAN Law Partners LLC, a boutique cybersecurity and data privacy law firm located in the Philadelphia, Pennsylvania region. She reviews and analyzes her clients' legal obligations and works to create tailored cybersecurity and data privacy programs. As a recognized thought leader in data privacy and cybersecurity law, she serves on the New Jersey State Bar Association's Cyber Task Force. She can be reached at rrakoski@xpanlawpartners.com.

Endnotes

1. Department of Labor (DOL) "Tips for Hiring a Service Provider," "Cybersecurity Program Best Practices" and "Online Security Tips," April 2021.
2. Under the Health Insurance Portability and Accountability Act (HIPAA), a *covered entity* is either a health care provider, health plan or health care clearinghouse. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity.