CPA
Practice Advisor

reduce the risk of a data breach. Here's how.

Apr. 01, 2024

By Dr. Sangeeta Chhabra

Here's a sobering stat for accountants and business owners alike: 74% of data breaches occur due to human errors, encompassing mistakes, privilege misuse, stolen credentials, or social engineering.

But there is hope—through proper training, your firm and ultimately your clients can significantly reduce the risk of a breach.

Do staff follow data security policies?

fostering a culture of data security awareness throughout the organization.

As mentioned above, human error remains the largest cause of data breaches—whether it's unwittingly clicking on malicious links, succumbing to phishing scams (which are getting more advanced by the day), or mishandling sensitive information. While technological safeguards undoubtedly play a critical role, they alone cannot entirely mitigate these risks. This is precisely where comprehensive employee training assumes its pivotal role.

Benefits of employee training

1. Minimized exposure to data breaches

When employees are well-trained, they're less likely to be targets of cyberattacks, lowering the risk of data breaches and the costs involved. Additionally, simulating mock data breaches helps prepare staff for such situations, enabling quicker responses and reducing containment time.

2. Financial

Although training necessitates an initial investment, its expense pales in comparison to the aftermath of a data breach, which encompasses legal expenses, regulatory penalties, and damage to reputation.

In cases where personal data is compromised and staff lacks training in managing such incidents, the information regulator can levy huge fines, along with potential imprisonment, depending on the gravity of the violation.

3. Enhanced compliance

Many regulations mandate that organizations offer cybersecurity training to their

4. Enhanced staff engagement

When employees feel empowered to safeguard the company’s data, they exhibit greater confidence and job satisfaction.

Foster a culture of communication: Encourage employees to discuss data security among themselves, fostering an open dialogue in the workplace. This enables them to ask any questions they may have, as I often say, “No question is a silly question unless it goes unasked, leaving you feeling uncertain.” The more at ease your employees are with communicating and voicing even minor concerns, the better prepared your company will be to address data security challenges.

What does successful training look like?

Cybersecurity awareness

It’s crucial for employees to understand various cyber threats they might encounter. It includes recognizing phishing emails, understanding social engineering tactics, identifying malware, and being aware of other common attack methods. Additionally, they should comprehend the significance of data security to your organization.

Data protocols

Clear guidelines on how to handle sensitive data, whether in digital or physical form, are essential. Employees must learn the secure storage, transmission, and disposal of data. Familiarity with audit trails, authentication procedures, and session management contributes to overall data safety.

Password and access management best practices

Training should encompass best practices for creating strong passwords and

Processes for handling client data or payments

Instructing staff to adhere to specific steps, such as verifying the credentials of individuals requesting data access, confirming their affiliation with the stated company and department, and requesting documentation like bank verification letters or company registration documents to validate company bank details, is crucial. Providing a checklist for reference can significantly mitigate risk levels.

Actionable insights for implementation

Putting effective employee methods into practice can be simplified by adhering to these practical guidelines:

Personalize training programs

- Craft training sessions that cater to your organization's unique requirements, considering the data you manage and the regulatory standards of your industry. You may incorporate additional governmental regulations such as GDPR or POPIA to underscore the significance of data protection from external regulatory perspectives.
- Moreover, customize training modules to align with specific departments such as administration, accounting, human resources, and development. By doing so, you can effectively address the distinct data handling practices and emphasize the importance of data security relevant to each group.
- When considering delivery methods, weigh the benefits of online employee training against in-person programs to determine the most suitable approach for your organization's needs.

Stay current with regular updates

- As cyber threats continue to evolve, it’s imperative that your training program

cybersecurity threats.

Fostering engagement

- Enhance training sessions by making them interactive and engaging. Incorporate real-world examples and scenarios to make the content more relatable to employees’ everyday experiences.
- Encourage active participation from staff members to ensure their engagement throughout the training.
- Facilitate a Q&A session afterward to encourage discussion and dialogue. Employees may share experiences or insights they’ve encountered, offering valuable perspectives and potential solutions that could benefit the company.

Monitoring and assessment

- Consistently track the performance of your training program and solicit feedback from employees to enhance its effectiveness.

Establish safe reporting channels

- At some point, an employee may misplace their phone or inadvertently click on something that triggers issues. A swift response can significantly mitigate risks, but it depends on employees feeling secure in reporting problems without facing repercussions.
- We all make mistakes. Swiftly securing data following an error is crucial to minimize the potential loss of customer, employee, or company information.
- Ensure employees understand that reporting problems promptly is preferable, as it may prevent a breach if addressed in time and assure them that it’s safe to do so.

The bottom line: A culture of data security

and financial resources—and preserving the trust of your clients.

ABOUT THE AUTHOR:

Dr. Sangeeta Chhabra, co-founder and director of Ace Cloud Hosting, is a leader and innovative entrepreneur with more than 20 years of experience in the IT sector. She has positioned the company as a leading global provider of IT and managed cloud services, celebrated for its QuickBooks hosting tailored for the accounting sector, as well as its Managed Security Services and Public Cloud offerings for SMBs and enterprises. Under her leadership, Ace Cloud was honored as the Best Outsourced Technology Provider at the *CPA Practice Advisor* Readers’ Choice Awards 2023, among other accolades. Beyond her professional successes, Dr. Chhabra is a passionate advocate for women’s empowerment and is committed to fostering an inclusive environment at Ace Cloud.

Accounting • Security • Small Business • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.