How to retain trust with your employees after a breach

Matt Cullina

Matt Cullina is CEO at IDT911, Scottsdale, Arizona, USA.

A spate of high-profile data breaches has spurred talk about the financial burdens of the current cyber threat environment. Research conducted by IBM revealed that the average consolidated total cost of a data breach is $3.8m, a figure that represents an increase of 23 per cent over the past two years (source: www-03.ibm.com/security/data-breach/).

Less tangible costs also must be considered when it comes to calculating the toll a data breach has on an organization. Employees' trust, slow to build but quick to lose, is likely to take a significant hit as they watch their workplace become the subject of scrutiny and scorn. Morale could slip. They also may be left to grapple with additional fallout if their own personal information was part of the exposure. Companies that experience a breach have many action items in front of them, but the road to recovery starts with rebuilding employee trust, and HR plays a crucial role in this process.

Upon learning of a breach, employees' first questions likely will center on the security of their own information. Was staff data part of the breach? Has their information been compromised? This initial step – confirming the security status of any employee data held by the company – is important for employers, as it provides them with a launch pad to begin shoring up employee confidence.

If workers' information is breached, the company is expected to be under an entirely different level of scrutiny than that if only consumer data are exposed. Companies, even those with a solid breach response plan, must be prepared for a considerable increase in engagement when the exposure involves employee data. The reason? Once the organization communicates to those employees involved in a breach situation, there is typically a "hair on fire" moment internally as people turn their attention to worries about fraud and identity theft. Being ready for this phenomenon is crucial for maintaining a foundation of trust.

The difference in a company's strategy becomes apparent when comparing general consumer breaches against breaches where employee data are compromised. In a consumer exposure, notification letters offering support – identity protection, credit monitoring, telephone resources, etc. – typically generate a response well under 10 per cent, sometimes even under 5 per cent. It simply is not top of mind for many people. By contrast, response rates in employee breaches are almost always in double digits, with some breach

notifications triggering responses as high as 30 per cent or more. Knowing this and understanding the importance of good communication when it comes to rebuilding workers' trust, employers are best served if they proactively think about how they will support employees after a breach.

One best practice when responding to an exposure that involves employee data is to change how notification is provided. It is a little impersonal to simply send a letter via snail mail or e-mail. Instead, a straightforward discussion involving as many facts as can reasonably be divulged, held in a live interaction with employees, is usually the best approach. Depending on the number of workers, it may make sense to break the conversation into multiple sessions so that employees have ample opportunity to ask questions and get information on what they can do to protect themselves going forward. It is a strategy that also demonstrates to employees that the company is genuinely concerned and intends to provide resources that are meaningful. Staff should be given the chance to voice their frustrations during these conversations, but they should also be encouraged to offer their feedback and seek solutions.

Even without a breach clouding the picture, employers can nurture a trusting environment by reinforcing the organization's culture of information security; ensure that employees understand that protecting sensitive data is one of the company's top priorities. Follow this with training that gives employees effective detection mechanisms that enable them to spot potential exposure situations and avoid them. As with other forms of training commonly given to employees, data privacy training is becoming core strength in many organizations. This strategy not only is good for the company and its business with external customers but also hones the skill sets of its workforce. Even if a breach does occur later, education workers received on breach recovery skills will give them confidence in their ability to quickly follow the response protocol and mitigate potential harm.

As companies review their privacy protection and breach response strategies, other steps may also be prudent to help safeguard employees' personal information. Employers in industries with higher data risks, such as healthcare and the financial sector, are increasingly offering identity protection proactively as an employee benefit that is either paid for by the employer or available for employees to purchase as a voluntary plan. These programs give employees a leg up ahead of an event, with identity monitoring working in advance of potential threats and knowledge that experts are available to help them through any jam. If an employee's personal information is breached – by a retailer, a physician's office or any other outlet – the benefit provides peace of mind for employees and extends the trust they have already established with their employer.

About the author

Matt Cullina is chief executive officer of IDT911.