Organizational & Personnel Risk Management

Defuse Troubled Employees
Minimize Identity Theft’s Effects
It’s Time to Redefine HR’s Role
Minimize the Effects of Identity Theft on Individuals and the Workplace

By Rich Scott

Chances are good that you or someone you know had their personal information compromised online. More than 30 percent of data breach victims later go on to experience an identity crime. In fact, cybersecurity firm Proofpoint determined that by mid-2018, 33 percent of U.S. adults had fallen victim to identity theft, which is a crime that occurs somewhere in the world every two seconds.

The Equifax breach of 2017 was among the first mega breaches that rattled consumers on a national scale and brought identity theft awareness to the forefront. The deluge of sensitive data falling into the hands of cybercriminals has not slowed down since. It has, in fact, accelerated. During the first half of 2018, according to the website Breach Level Index, 3.35 billion online records were compromised. This marked a 72 percent increase over 2017.

Even if you or your organization has not already suffered a breach, data everywhere remains vulnerable. It is likely only a matter of time before everyone reading this is directly impacted.

Addressing Digital Risks

Almost everything we do is captured and transmitted across the web. Personally identifiable information, payment data, purchasing habits, medical information, account passwords and more are all out there. And each day brings more devices and accessories to capture them. Multiply those devices by the number of employees in your organization, and you start to realize how challenging it is for IT and information security teams to keep data safe.

Now that bring your own device policies are the norm, each employee is using his or her own laptops, tablets and smartphones for business and personal purposes while connected to the
organization’s network. In fact, research firm Clutch found that 86 percent of employees view and send work emails via their personal devices. Another 67 percent access shared potentially confidential documents on their smartphones.

Mobile devices are just as susceptible to cyberattacks as the desktop computers employees use every day. Therefore, smartphones and tablets should be subject to the same vigilance regarding cybersecurity. One wrong tap is all it takes to download a virus that could infiltrate the network and allow bad actors to view and manipulate confidential information.

Data Breach Consequences

The financial consequences of a data breach for an organization are devastating, averaging $7.91 million in the United States. However, the fallout goes well beyond monetary damages.

An organization that suffers a data breach will face serious and long-lasting reputational damage. This can lead to lost customers, broken partner relationships and general distrust. Adding to this, people who fall victim to a security or fraud incident will seek help from whomever they view responsible for failing to protect their personal information, be it an employer, retailer, health care organization, social network or financial institution.

As government agencies have come to recognize the negative impacts a security incident can have, scrutiny of state, regional and international regulators has increased. To see what is being done to ensure data protection is prioritized, check out the National Conference of State Legislatures’ linked list of security breach notification laws, Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union’s General Data Protection Regulation (GDPR).

Identity Theft’s Impact

Identity theft is also a real and serious consequence of data breaches. Anyone whose information is exposed as a result of a breach becomes a potential victim of fraudsters—forever. There is no expiration date for the personal and sensitive information that lands on the Dark Web.

Cybercrime is not the sole means of identity theft, either. Low-tech criminal identity theft rings engaged in mail theft, trash-picking and forging IDs remain active and successful.

At any given moment, you, or one of your employees, can have had their identity compromised. When someone’s identity is stolen, it takes an average of six months and 100-200 hours of effort to recover. Much of that time will be spent when the identity theft victim should have been working, which disrupts performance and productivity.

Identity theft also takes a serious toll on the victim’s emotional well-being and relationships with others. According to the Identity Theft Resource Center’s 2018 Aftermath study,

- 59.2 percent of victims were depressed,
- 77.3 percent felt increased stress,
- 83.7 percent said they could not trust others and felt unsafe, and
- 84.1 percent reported issues with their sleep habits.

These factors directly correlate to happiness and effectiveness in the workplace. Combine them with the absenteeism required to fix identity theft issues, and it is easy to see the extent of collateral damage from data breaches.

How Human Resources Can Mitigate Identity Theft Risks

HR teams can step up to help their organization and its employees become much more vigilant with the resources they need to prevent and respond to an identity crime, if necessary. But promoting safe online behavior while working with IT to improve cybersecurity trainings will only do so much. There is really only one way to significantly reduce the risks data breaches and identity theft pose to the workforce. That is offering identity theft monitoring and protection as a standard nontaxable and nonreportable benefit.

A survey conducted by Willis Towers Watson found that 63 percent of employers plan to offer such a benefit by 2021. Not only is protecting employees’ identity a smart business decision, it is a high-value, cost-effective, progressive benefit that everyone can appreciate.

By rolling out identity theft protection, organizations guarantee their employees’ personal information is being monitored for fraudulent activity. This empowers individuals to put a stop to issues before they turn into full-blown identity theft.

As an added bonus, workers receive peace of mind from knowing they have an experienced support team behind them if their identity is compromised. This reduces stress. Last, for the organization’s bottom line, employees covered by identity theft protection will not need to miss work to resolve issues.

Rich Scott is chief commercial officer for EZShield + IdentityForce, which provides digital identity protection and cybersecurity solutions to organizations of all sizes. Scott is on LinkedIn.