Data Breach Fatigue

As cyberattacks increase in frequency, consumers may suffer from data breach fatigue, a term used to describe the apathy present as breaches become more commonplace. In 2020 alone, 155.8 million individuals were affected by data exposures, potentially leading consumers to become desensitized to news of a breach and unmotivated to protect themselves. In fact, recent research from RAND Corporation found that following a data breach, only half of the survey respondents changed their passwords or personal identification numbers, and 1 in 5 respondents didn't take any action at all.

While consumers may have become weary of data exposure, organizations cannot afford to suffer from data breach fatigue and must remain diligent in their cybersecurity efforts. Nevertheless, 84% of North American chief information security officers believe that cybersecurity breaches are inevitable, according to research from Kaspersky Lab.

Normalizing data breaches or rationalizing their inevitability can pose significant harm to an organization's customers, bottom line and reputation. This article discusses the repercussions of data breach fatigue on organizations and the steps organizations can take to ensure they don't become complacent to cybersecurity needs.

Risks of Data Breach Fatigue

Organizations that have become desensitized to the seemingly never-ending stream of cyberattacks are at risk of suffering major losses. Data breach fatigue and surrendering to the "inevitable" can result in severe damage, including:

- **Loss of trust**—Consumers may not trust organizations that are affected by data breaches. A study by the Poneman Institute found that nearly one-third of respondents stopped doing business with companies following a data breach.
- **Loss of money**—Data breaches can be costly. According to IBM, the average cost of a stolen record is $148. When millions of records have been compromised, it can become quite expensive for companies to recover.

Data breaches also tend to affect small businesses more severely than large corporations. According to the National Cyber Security Alliance, 60% of small businesses fail within six months following a data breach, typically due to significant financial and reputation damages.

Preventive Measures

The constant threat of cyberattacks can be overwhelming for organizations and their employees, resulting in complacency and fatigue. Organizations must stress the importance of cybersecurity to their employees to limit the possibility and impact of a breach. Organizational leaders can take the following actions to help prevent data breach fatigue from spreading to employees:

- **Maintain transparency and awareness**—To get employees involved in cybersecurity, organizations must be transparent and build awareness about the subject. Ongoing educational programs can help employees identify threats and promote a more secure, risk-conscious work environment.
- **Distinguish threat level and type**—Burnout may occur if every issue is treated with the same level of urgency. Establish a hierarchy of threat levels so that employees understand the different repercussions that arise from each type of breach.
- **Ensure consistency**—Security practices should remain consistent throughout every level of an organization. Top executives and entry-level staff alike should have the same understanding of cybersecurity procedures.

In addition to educating the workforce on cybersecurity, organizations should work to prevent data breaches from occurring in the first place. To prevent data breaches, organizations should:

- **Review cybersecurity policies**—Ensure the cybersecurity measures in place are sufficient at preventing breaches. Address policies every time a new vulnerability is identified.
- **Keep software up to date**—Install the latest software updates on all company laptops, smartphones and networks to help ensure that malware and virus protection is current.
- **Back up data**—Data should be encrypted and backed up to secure cloud storage.

If a data breach occurs, organizations should initiate their incident response plan to reassure customers and limit the damage.

Remember, organizations, employees and consumers must remain vigilant to fight off data breach fatigue in today's connected world. By maintaining a positive security culture and staying alert, organizations can minimize the occurrence and damage of data breaches.

For additional risk management guidance and insurance solutions, contact us today.