Data Security Executive Summary

Stats

- In the summer of 2017, Equifax lost data on over 143 MILLION Americans, the largest breach of **highly sensitive data** in history.
- The number of U.S. data breaches tracked in 2016 hit a record high of 1,093, according to a new report released by the Identity Theft Resource Center (ITRC). This represents a substantial hike of 40 percent over the 780 breaches reported in 2015. The **business sector** accounted for over 45 percent of those breaches.
- Between 2005 and 2017, there have been over 8 thousand data breaches exposing over 1 billion records including social security numbers, dates of birth, driver's license numbers, etc…
- The FBI reports that social media is becoming the preferred source for identity thieves.
- Employees are being fired or forced to resign due to inappropriate social media posts on outlets such as Facebook, Twitter and Instagram.

Threat Examples

- Phishing scams are the most common types of social engineering attacks used to obtain personal information. Phishing includes suspicious emails with attachments that may include viruses as well as link shorteners that embed links into an email and redirect users to suspicious websites pretending to be legitimate. A phishing email will incorporate fear and a sense of urgency to manipulate the user into acting promptly.

Individual Impact Examples

- A woman applied for a job at a local Target department store and was denied. The reason? She already worked there – or rather, her Social Security number already worked there. Follow-up investigation revealed the same Social Security Number was used to obtain work at 37 other employers.
- Audra realized she had a problem when she got a statement from the IRS saying she owed $15,813 in back taxes even though she had not worked since her son was born. *How do you prove that you are you?* Audra Schmierer said. It's like you are guilty until proven innocent. Audra's SS# was used by 81 people in 17 states.

Plan of Action Needed

Businesses and organizations must become pro-active, not reactive, when it comes to data security and preventing a breach. Making employees aware of the dangers of social media is crucial in the fight against identity theft and organization liability.

Preventing data breaches and identity theft takes more than technology or good procedure. Stopping data breaches **before** they occur requires building a "Breach-Free Culture" within your organization. Properly training employees across all areas of data protection is a necessary component to breach-proof environment.
Although cyber-criminals may get the headlines and media attention, the fact is that that most breaches are caused by human error and process failures, not advanced hackers.

TBGSolutionsInc.com
888-533-9123
Info@TBGSolutionsInc.com

Technology can't always stop someone from making mistakes, but training them in a way that changes thinking and behavior can bring about a "Breach-Proof Culture" where employees across all departments share a heightened awareness, understanding, and commitment to eliminating risk.

The Chinese expression, *zhuan ji*, can mean opportunity or threat. Social media sites such as Facebook, LinkedIn, and Twitter present both an opportunity and a threat to employees individually as well as the organization. Employees **must** take precautions to protect their digital identity and their reputation online! Social media platforms are an identity thief's playground.

Organizations that proactively educate their employees regarding data security and identity theft drastically reduce their chances of a costly breach. TBG Solutions' training impacts the way you think! When you change the way someone thinks, it results in a change of behavior, reducing the risk of a data breach. Common sense is not common knowledge.

The following items have been specifically designed by our company to facilitate a culture shift for your organization as you seek to address these issues.

TBG Solutions Inc. will provide:

- **Training/Staff Development**
  - Statistics (% of social media users, online identity theft, data breaches, etc.)
  - What is identity theft? - 7 most common types...
  - Real world examples of social media posts that created liability.
  - Discussion on key information to remove from Facebook in order to prevent identity theft.
  - Steps to keeping your staff safe and managing the risk of a liability.

- **Optional Mitigation Program Recommended** - We also recommend implementing a comprehensive Identity Theft Monitoring and Restoration service as an optional employee program.

- **Optional - Proactive: Cyber - Powered by Threat Advice**
  - Cybersecurity continued-education through a cutting-edge learning management system.
  - Cyber risk profile for each employee and organization-wide risk reports.
  - Prize incentives for employee progress.
  - Phishing simulations and network exposure scans.
  - Real-time threat intelligence and alerts for your industry and business.
  - Policies and procedures library to help you set a standard for your employees.

Implementation

Training lasts approximately 90-120 minutes. It is vitally important that training be held as "mandatory" to ensure all employees understand the complexity of Data Security, Identity Theft, and Social Media Risk as well as ID Theft program coverage. To accommodate your organization's needs, several presentations of various numbers of employees can be scheduled. Additionally, new employee training and refresher courses are recommended.

TBGSolutionsInc.com
888-533-9123
Info@TBGSolutionsInc.com