March 8, 2018

Passphrases and Other Password Protection Strategies

FINANCIAL SERVICES, RISK ADVISORY/INTERNAL AUDIT
BY SCHNEIDER DOWNS PROFESSIONAL

Building a reputation for sound data privacy and robust security is challenging for many organizations in this digital age, especially those in the financial services industry. Below are a few statistics to help illustrate the reasons why this challenge exists for so many financial services organizations:

- In 2017, the financial services industry was the most-attacked industry. In particular, 24% of the total breaches that occurred last year affected financial organizations. The second-highest percentage (15%) of breaches involved healthcare organizations. (Source: 2017 Verizon Data Breach Investigations Report (DBIR))
- 81% of the hacking-related breaches of 2017 leveraged either stolen or weak passwords (Source: 2017 Data breach Investigations report)

Enabled by the alarming use of weak or insecure passwords, not only are employees an organization's first line of defense against cyberattacks, employees are also potential threats to these attacks. The defensive strategy against these attacks is simple—improve protection of vulnerable passwords by creating and using passwords that are easy to remember, but difficult to be compromised. With our comprehensive expertise and experience helping clients improve their cybersecurity strategies, Schneider Downs recommends any number of the following procedures to help your organization effectively develop its own defensive strategy to prevent falling victim to a crippling data breach or other attack:

1. Encourage use of unique passphrases (minimum length of 8 up to 64 characters) and not passwords[1].
2. Enable multi-factor authentication (MFA), where possible.
3. Implement and adopt security policies and procedures, and enforce them through security awareness training and education.
4. Implement periodic auditing to detect password policy violations and maintain compliance with policy and/or regulatory requirements.
5. Leverage use of free, popular password managers to reduce the risk of losing or forgetting passwords or passphrases.

While no security measure is full proof, proper password management is an essential security measure in safeguarding organizations from cyber threats. At Schneider Downs, we assist companies in assessing their risk exposures to cyberattacks. For more information on Schneider Downs' cybersecurity offerings, check out the Cybersecurity Services page. If you find that your question has not been addressed, please do not hesitate to contact us.

[1] Passphrases are commonly described as a sequence of words or other text used to authenticate one's identity. In June of 2017, the National Institute of Science and Technology (NIST) released new password security guidelines. In short, these new guidelines recommended using long passphrases instead of complex passwords that were created from the use of special characters, numerals and capitalization.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.