January 28, 2019

Part One in a Series: Managing Risks of Technologies Emerging as Business Opportunities - Websites and Mobile Applications

DIGITAL & TECHNOLOGY, RISK ADVISORY/INTERNAL AUDIT
BY SCHNEIDER DOWNS PROFESSIONAL

Websites and mobile applications are an important medium for businesses to interact with customers, obtain information, and conduct business transactions. According to a 2018 survey of 351 small businesses performed by Clutch.co, 42% of small businesses currently have a mobile app and 30% plan to build one in the future (Panko). Internal Audit as a profession must identify and mitigate the emerging risks associated with these websites and mobile applications.

The use of websites and mobile applications, particularly by small businesses, opens up an array of potential security issues. According to the Verizon Data Breach Investigation Report, 21% of data breaches in 2017 were through web applications. This is a higher percentage than any other type of breach, with the next closest type of breach being miscellaneous errors at 16% of breaches reported.

Like most risks, the risks associated with websites and mobile applications can be mitigated. Let's first identify what they are. Websites and mobile applications can be vulnerable due to:

- A lack of technical security assessments being performed

- Noncompliance with legal and regulatory requirements (e.g., data privacy)

- Inappropriate system configurations

- Unencrypted data stored in static areas of the application or website

- Security procedures are nonexistent for end users using mobile applications and websites

The possible issues that can result from a successful attack on a website or mobile application are numerous and severe. With websites and mobile applications being a key medium for a company to generate sales, the lost revenue due to a successful attack can be very detrimental. Another issue that may be even more troublesome is the loss of sensitive data. With online sales being so critical, the possibility of losing customer information is a risk that must be addressed. With the General Data Protection Regulation (GDPR) - see our most recent article on the subject here - lost customer information can be extremely costly to your company.

So how does this impact Internal Audit? This series is focused on identifying the risks related to the next generation of Internal Audit. We as professionals already know that websites and mobile applications are an integral and essential part of our

everyday lives. As internal auditors look at risk in its entirety and not just financial statement risk, we must consider the possibility that security flaws can exist in websites and mobile applications. Considering these possibilities when performing risk assessments and helping the client identify potential weaknesses or vulnerabilities are two crucial ways that Internal Audit can bring value to the client.

If you have additional questions or concerns about the risks and possible mitigation techniques related to websites and mobile applications, we welcome the opportunity to discuss your concerns and become a trusted advisor. Please visit our Risk Advisory Services page.

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.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.