Cybersecurity Tips for Data Privacy, Data Protection and Data Security for Businesses, Firms, and Organizations

by

Brian K. Harte, Ph.D., COO

American Board of Forensic Accounting

Introduction

Cybersecurity breaches and cybercrime continue to be areas of great concern for accountants, auditors, other professionals, and the businesses they serve. The expanded use of networked computers, the internet, and cloud computing have created new opportunities for hackers, scammers, and fraudsters to commit cybercrimes and infiltrate businesses. Moreover, the need to safeguard personal and business data has promulgated the importance of business entities adopting a strong posture of cybersecurity awareness to prevent occurrences of and damages caused by cyberattacks. In addition to attacks on businesses themselves, cybercriminals may use unlawful computer access techniques or network intrusion tactics "to gain access to customer credit card records and bank accounts, supplier networks and employee financial and personal data" (Small Business Administration-SBIR/STTR, 2017, p. 2). Unauthorized network intrusions and social engineering attacks remain a persistent problem faced by not only large business entities but also small and medium-sized businesses. Based on a recent Small Business Administration (2023) survey, "88% of small business owners felt their business was vulnerable to a cyber-attack" (Madrid, 2021, p. 1).

According to Dr. Jaine LeClair, Chief Operating Officer of the National Cybersecurity Institute (2015) at Excelsior College, "fifty percent of small to medium-sized businesses (SMB) have been the victim of cyber attacks" (p. 1). The financial and reputational costs of these attacks on affected businesses may prove to be extremely high. This article will examine recommended action steps to protect personal and private data within businesses, privacy concerns regarding these data, and types of data breaches that businesses often experience. The intention of this work is to raise awareness of persistent cybersecurity threats to businesses as well as accounting and auditing firms. Additionally, this article will provide

recommended action steps that may be taken to respond to and recover from unlawful data breaches and to mitigate additional damage that may be caused by cyber attacks.

Cybersecurity Tips for Businesses, Firms and Organizations

According to information presented in IBM's latest Data Breach Report, "83% of organizations experienced more than one data breach in 2022"(Huang, et. al., 2023, p. 1). In the year 2018 alone, "the U.S. was the country most severely affected by cybercrime in terms of financial damage: industry experts estimated that the U.S. Government faced costs of over 13.7 billion U.S. dollars as a result of cyberattacks" (Petrosynan, 2022, p. 1). In 2020, "there were over 700 thousand attacks against small businesses, with damages totaling 2.8 billion dollars and the numbers continue to rise every year" (Madrid, 2021, p. 1). To combat cybersecurity threats, the Federal Communications Commission (2023) offers cybersecurity tips to assist businesses to develop a cybersecurity strategy "to protect their business, their customers, and their data from growing cybersecurity threats (including the following recommendations):

1. *Train employees in security principles* – establish practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violations of company cybersecurity policies;
2. *Protect information, computers and networks from cyber attacks* – keep clean machines; having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats – use antivirus software to scan updates;
3. *Provide firewall security for your Internet connection* – make sure the operating system's firewall is enabled to install free firewall software available online – ensure employee home systems are protected by the use of firewalls;
4. *Create a mobile device action plan* – require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while on public networks;
5. *Make backup copies of important business data and information* – regularly backup critical data on computers, including electronic documents, spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files – back up data automatically (at least weekly) if possible – store copies offsite or in a cloud environment;
6. *Control physical access to your computer and create user accounts for each employee* – prevent access from unauthorized users – store computers in locked areas – create separate user accounts for each employee – only grant administrative privileges to IT staff and key personnel;
7. *Secure your Wi-Fi networks* – ensure they are encrypted and hidden – do not broadcast network name and password protect access to router(s);
8. *Employ best practices on payment cards* – ensure banks used by the business to ensure trusted and validated tools and anti-fraud services are used – isolate payment systems from other less secure programs – do not use the same computer to process payments and surf the internet;
9. *Limit employee access to data and information; limit authority to install software* – employees should only be given access to the specific data systems that they need for their jobs – they should not be able to install software without permission;
10. *Passwords and authentication* – employees should use unique passwords and change passwords every three months – deploy multi-factor authentication that requires additional information beyond a password" (p. 1).

Common Cyber Security Threats for Businesses, Firms and Organizations

The SBA (2023) identified several common cyber attack threats that impact businesses, firms, and organizations including, but not limited to: malware attacks, viruses, ransomware attacks, spyware, and phishing. These threats can be defined as follows:

- Malware – malicious software used to damage a computer server or network
- Viruses – harmful programs used to infect computers connected to other devices
- Ransomware – malware used to infect and restrict access to a computer – perpetrator often demands money in return for restoring the data
- Spyware – malware used to gather information and use without consent
- Phishing – uses email or malicious website – infects computers or systems to collect sensitive information (p. 1).

In addition to the aforementioned threats, businesses may also fall victim to: distributed denial-of-service (DDOS) attacks, artificial intelligence (AI) and machine learning enabled cyber attacks, cryptocurrency and blockchain attacks, and attacks through the use of penetration of third-party software and applications.

Business owners and their stakeholders should be aware that the aforementioned cyber security threats continue to be a persistent problem that could have significant reputational risks as well as exorbitant financial costs to their businesses.

The Use of Case Studies to Prepare for Potential Cyber Security Attacks

Accountants and auditors—as well as the businesses, firms and organizations they serve—may be susceptible to a possible cyber attack at any time. Thus, the use of case studies developed by the National Cyber Security Alliance through a grant from the National Institute of Standards and Technology (NIST) (2003) may provide a series of potential cybersecurity threats that may be used to actively prepare for common threats including, but not limited to, the following types of cybersecurity attacks: keylogging attacks, malware and bank fraud; encryption and business security protocols; social engineering and phishing attacks; and data breaches.

The Small Business Cybersecurity Cases Study Series is available at the following website: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series.

Data Privacy and Security

Protecting sensitive customer and business data through proactive measures is essential to foster a posture of data security. The National Cybersecurity Center of Excellence (NIST) (2023) defines data security as "the process of maintaining the confidentiality, integrity, and availability of an organization's data in a manner consistent with the organization's risk strategy" (p. 1). The National Cybersecurity Center of Excellence (NCCoE), a part of the NIST, provides a "collaborate hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges" (Cawthra, et. al., 2019, p.2).

The National Cybersecurity Alliance (2023) offers several tips for keeping personal data safe. The following tips, offered by the National Cybersecurity Alliance (2023) are equally important for businesses, employees, and firms that aim to prevent a possible cyber attack:

- *Encrypt your data with a Virtual Private Network (VPN)* – a service that enables you to select a server location
- *Don't save passwords to your browser* – disable automatic password storing and delete passwords you have saved
- *Avoid using public Wi-FI networks* – most public WI-FI networks are unsecure
- *Update all tools, applications, and operating systems* – software requires regular updates to ensure their security
- *Don't open unfamiliar attachments and links* – opening phishing links can infect your computer with malware
- *Don't share personal information with anyone* – you are the first line of defense in protecting personal data
- *Use cybersecurity products* – industry recognized cybersecurity products can assist to monitor, detect and clean your device from malware and viruses
- *Don't use personal devices at work* – your personal data can pass through the network managed by the company
- *Back up your data* – consider using cloud storage solutions to back up your data in the cloud (p. 1).

Data Breaches

The Federal Trade Commission (FTC) (2023) offers guidance for businesses that have experienced a data breach involving personal, customer, or other proprietary or corporate information. In your remediation of the breach you should quickly move to secure your operations, fix vulnerabilities, and notify appropriate parties (Federal Trade Commission, 2023). The FTC (2023) recommends the following action steps for securing operations "if you experience such a breach:

1. Move quickly to secure your systems and fix vulnerabilities that may have caused the breach, including securing physical areas related to the breech,
2. Mobilize your breach response team right away to prevent additional data loss,
3. Assemble a team of experts to conduct a comprehensive breach response - including identifying a data forensic team and consulting with legal counsel,
4. Stop additional data loss – do not turn machines off and place clean machines online in place of affected ones – update credentials and passwords of authorized users,
5. Remove improperly posted information from the web,
6. Interview people who discovered the breach,
7. Do not destroy any of the forensic evidence – this may be crucial for investigative and remediation purposes" (p.1)

To fix vulnerabilities that may have led to the breech, the FTC (2023) recommends that affected businesses:

1. Determine who is involved and decide if access privileges need to be changed,
2. Check your network segmentation – ensure the breach is contained,
3. Work with forensic experts to analyze encryption is enabled and that the backup date was preserved – determine what data was compromised,
4. Create a comprehensive plan to communicate what happened to all audiences and stakeholders,

5. Anticipate questions that may be asked – continue good communication to alleviate concerns and frustration (p.1).

As a last action, the FTC (2023) recommends that business entities notify appropriate parties. In doing so, the FTC recommends the following:

1. Determine your legal requirements – these may vary by state
2. Notify law enforcement – call local police immediately – report your situation and the potential risk for identify theft
3. If the breech involved electronic personal health records ensure that you are covered by the Health Breach Notification Rule, 45 CFR §§ 164.400-414 – includes notification obligations and rules (p. 1)

Health breach resources pertinent to answer various notification requirement questions that individual business entities may have can be found at the following websites:

HIPPA Breach Notification Rule:

hhs.gov/hipaa/for-professionals/breach-notification

HHS HIPPA Breach Notification Form:

hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting

Complying with the FTC's Health Breach Notification Rule

ftc.gov/healthbreachnotificationrule

A free copy of the FTC's (2019) Data Breach Response Guide may be obtained from the following website: https://www.bulkorder.ftc.gov/publications/data-breach-response-guide-business

The aforementioned resources and guides may prove valuable in informing you of recommended action steps when your business is faced with a data breach. It should be noted, however, that some of these steps may vary from case to case.

Conclusion

The awareness of practical steps to identify, prevent, respond to, mitigate, and recover from damages caused by a cyberattack or cybersecurity breach are crucial for any business. "Small businesses are especially attractive targets because they have information that cybercriminals (bad actors, foreign governments, etc.) want, and that typically lack the security infrastructure of larger businesses to adequately protect their digital systems for storing, accessing, and disseminating data and information" (Small Business Administration, 2023, p. 1). Accountants, auditors, and other business professionals should strive to adopt behaviors that assist to mitigate the risks of cybersecurity incidents through continual training and increased awareness. Additionally, developing and enforcing policies that promote and encourage sound cyber security behaviors can foster a strong cyber security posture that may lead to less cybersecurity breaches and minimize intended disruptions and damages from network intrusions and social engineering attacks.

Training Opportunities with the American Board of Forensic Accounting

Learn more about the latest forensic accounting techniques through the American Board of Forensic Accounting (ABFA). Visit the ABFA's website at abfa.us. The ABFA offers a variety of career development and certification opportunities in the areas of cybersecurity, forensic accounting, forensic investigation, forensic bookkeeping, forensic intelligence, and forensic auditing.

This article is presented for educational and research purposes only and does not express the opinions of the ABFA or its members. The content is available through the public domain and is intended to be informative in nature.

References

American Board of Forensic Accounting. (2023). ABFA. https://abfa.us/

Cawthra, J., Ekstrom, M. Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2019). Data confidentiality: Detect, respond to, and recover from data breaches. *National Cybersecurity Center of Excellence/National Institute of Standards and Technology*. https://www.nccoe.nist.gov/sites/default/files/legacy-files/dc-drr-project-description-final.pdf

Federal Communications Commissions. (2023). Cybersecurity for small business. https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). The devastating business impacts of cyber breach. *Harvard Business Review.* https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

IBM. (2022). Cost of a data breach report 2023. https://www.ibm.com/reports/data-breach

Madrid, M. (2021). Protect your small business from cybersecurity attacks. https://www.sba.gov/blog/protect-your-small-business-cybersecurity-attacks

National Cybersecurity Alliance. (2023). 10 must-know tips for keeping your personal data safe. https://staysafeonline.org/resources/10-must-know-tips-for-keeping-your-personal-data-safe/

National Security Institute/Excelsior College. (2015). Small business big threat: Protecting small businesses from cyber attacks. Statement for the Record: Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College Before the United States House of Representatives Committee on Small Business, 4/22/15.

Petrosynan, A. (2022). U.S. government and cyber crime – statistics & facts. *Statista.* https://www.statista.com/topics/3387/us-government-and-cyber-crime/

U.S. Department of Health and Human Services. (2023). Breach notification rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

U.S. Small Business Administration. (2017). The impact of cybersecurity on small business. Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) program. https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf

U.S. Small Business Administration. (2023). Strengthen your cybersecurity. https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity#id-best-practices-for-preventing-cyberattacks