our vision

Special Edition
October 2015

Sharing clear solutions on topics affecting our clients and their investors through innovative insights, sophisticated technology, and a solid tradition.

Alternative Investment Solutions Cybersecurity Overview

Death, Taxes & Data Breaches

2014 and 2015 proved to be turbulent years in the world of cybersecurity as high profile data breaches reached an unprecedented level. According to the Assistant Director of the FBI's Cyber Division, "The threat has reached the point that given enough time, motivation and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet." [1]

A data breach at any organization can have far-reaching consequences regardless of whether it is a government institution, retail department store, bank, investment advisor or any other institution that maintains confidential information. Beyond the initial loss of crucial data such as customer information and intellectual property, there is the possibility of federal and state penalties, civil suits, depressed market value, and reputational harm.

Implementing cybersecurity standards has never been more crucial. Although there's no one-size-fits-all approach to cybersecurity, and no 100% guarantee against cyber-theft, the National Institute of Standards and Technology suggests following its five-part framework (commonly referred to as the "NIST Framework") to reduce vulnerability:

Identify. Identify at risk data (i.e., what your company needs to protect) and assess existing vulnerabilities.

Protect. Limit access to only authorized users and devices and educate users on cybersecurity awareness and risk management.

Detect. Perform network monitoring to detect threats in a timely manner.

Respond. Contain and mitigate breaches, coordinate with stakeholders to execute a response plan and notify the appropriate authorities.

Recover. Execute recovery plans to restore systems and data, resume business activities and manage public relations. [2]

Of note, the NIST Framework should encompass not only internal systems, but also those of external vendors.

[1] *https://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism*
[2] *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*

usbancorp Fund Services, LLC

In connection with the NIST Framework, the Securities Industry and Financial Markets Association ("SIFMA") has published a list of cybersecurity action items for small firms. In it, SIFMA recommends the following safeguards:

1. Strictly enforcing username and password security requirements.
2. Restricting administrative and privileged access to systems and data through preventative and detective controls, following the "need-to-know" principle.
3. Allowing only trusted software on operating systems and preventing all other software through application whitelists.
4. Updating anti-virus software.
5. Training employees on how to recognize suspicious emails and attachments.
6. Using trusted and up-to-date operating systems.
7. Enabling automatic software updates to reduce risks associated with out-of-date versions.
8. Backing up data with secure cloud solutions or physical external hard drives.
9. Ensuring mobile devices are secure with passwords and the data is encrypted (at rest and in motion) in the event of a loss.

For additional guidance, SIFMA suggests the SANS Institute's Top Twenty Critical Security Controls list or the NIST Small Business Information Security guide.

At U.S. Bank, we take cybersecurity very seriously – our reputation and livelihood depend on it. And as a financial institution regulated by the Federal Reserve, the OCC and others, U.S. Bank not only has an ethical, but a legal responsibility to protect our clients' data. Robust information security policies on topics ranging from third party risk management to network security, combined with internal and external compliance oversight, ensure U.S. Bank remains committed to data security at every level of the organization. And our top-down commitment is evident. In February, U.S. Bank's CEO, Richard Davis, attended the White House Summit on Cybersecurity and Consumer Protection, along with President Obama and other industry leaders. Touching on U.S. Bank's commitment to data protection, Mr. Davis said, "We believe in both being a strong individual player and a strong team player. Individually, we invest in robust systems and technologies to prevent cybercrimes and as a team player, we seek to collaborate, coordinate and share information with other companies and government to help us stay a step ahead of cyber criminals and keep us on the forefront of this very important issue."

Contact

For more information on how U.S. Bancorp Fund Services, and our entire organization, are working diligently to maintain the integrity and confidentiality of your data, please contact your primary administrator.

Additional Resources

FCC Cybersecurity for Small Businesses
FCC Cybersecurity Planner
FINRA Cybersecurity Targeted Examination Letter
FFIEC Cybersecurity Resource Center
NIST Cybersecurity Framework
PWC Cybersecurity: The new business priority
US Chamber of Commerce Internet Security Essentials for Small Business

usbfs.com
800.300.3863

usbancorp Fund Services, LLC