PUBLICATION

Coronavirus: Privacy and Cybersecurity Considerations for Financial Institutions

Authors: Alexander Frank Koskey, III
March 18, 2020

Financial institutions are continuing to address the immense business impact of coronavirus (COVID-19). The Federal Financial Institutions Examinations Counsel (FFIEC) has issued its updated guidance on pandemic planning and regulators have encouraged financial institutions to work with customers affected by COVID-19. However, special attention must be paid to privacy and cybersecurity implications as financial institutions refine business continuity plans. The following is a brief overview of some of the key privacy and cybersecurity issues financial institutions should be considering in managing the increased risk created by COVID-19.

- **Teleworking**: Many financial institutions are allowing employees to telework to minimize the potential effects of COVID-19 and the disruptions to services and operations. However, the shift to a fully remote workforce places significant stress on information technology systems and infrastructure. Between March 9 and March 15, VPN usage in the U.S. grew an estimated 53% and some experts estimate it could increase to more than 150% by the end of the month. Financial institutions should ensure that they have the infrastructure in place to support a large-scale teleworking arrangement to maintain operational continuity. This includes having alternative plans if standard Internet service providers do not have capacity to support your workforce working from home.

- **Network Vulnerabilities and Security Concerns**: The rush to create a virtual workforce and solve operational problems with COVID-19 can also result in not doing due diligence on potential network vulnerabilities and security concerns. As employees migrate out of the office and begin teleworking, they may be using unmonitored and unsecured networks which are susceptible to unauthorized third-party access. Employees should be educated on the security implications of working from home. Financial institutions should ensure that all devices have mobile device management (MDM) software to maintain consistent security standards, can be updated or patched appropriately, and can be wiped clean in the event that a device is lost or stolen. If possible, it is also recommended that multi-factor authentication (MFA) be added as an additional layer of security. Bring your own device (BYOD) agreements and telecommuting policies should be clearly documented and communicated.

- **Cybersecurity Risks**: Cybercriminals are leveraging COVID-19 to deploy phishing attacks, spread malware, steal login credentials, and engage in financial fraud. Such attacks include emails claiming to be from representatives of the World Health Organization which contain attachments that, when opened, infect the victim's device with malware. Customers of financial institutions are also receiving emails from threat actors trying to coerce customers into sharing login credentials. Financial institutions should remind all employees to not click on links or open attachments contained in unsolicited emails and to not respond to solicitations for personal or financial information. It is also imperative that financial institutions maintain good communication both internally and externally to promote fraud management and be vigilant about maintaining cybersecurity standards.

- **Incident Response**: With increased cybersecurity risk comes the need for increased security operations to handle potential alerts. Financial institutions should review their incident response plans to ensure that security incidents can be addressed and responded to with a remote workforce.

Incident response plans should be maintained in paper with contact information (cell phone numbers) included so the IR plan can be implemented if necessary. If possible, companies should consider conducting a tabletop exercise to simulate an incident when multiple members of the incident response team are unavailable or working remotely.

- **Potential Data Loss**: Although discouraged, employees may be using personal devices to work from home which lack the same security features as company-issued devices. Additionally, for ease of accessibility during teleworking, employees may also forward sensitive business or client information to personal accounts. Financial institutions should review policies regarding the acceptable use of personal devices and align them with business continuity capabilities. This also includes clearly indicating whether company data is allowed on personal devices. Further, all employees should always be reminded of responsibilities and obligations to safeguard company and client information.

As financial institutions continue to manage risks in response to COVID-19, it is imperative that companies practice good cybersecurity hygiene. The increased reliance on a remote workforce reinforces the need to review privacy and security protocols and educate employees on their responsibilities to safeguard information. Such practices will help reduce risk and promote business continuity in these uncertain times.

Baker Donelson continues to monitor the impact of the coronavirus on the financial services industry. If you have any questions regarding these issues or how your financial institution can improve its privacy and security protocols in response to the coronavirus, please contact Alex Koskey or any member of Baker Donelson's Financial Services Team. Also, please visit the Coronavirus (COVID-19): What You Need to Know information page on our website.