**CYBERSECURITY IN BANKING**

Ever increasing use of online and mobile banking services requires banks to remain vigilant against the threat of cyberattacks. Vigilance requires not only understanding the threat in its current form, but also appreciating the evolving nature of the threat and the constant need to test and update procedures and safeguards.

There are several cybersecurity resources available to banks. For example, the Federal Financial Institutions Examination Council on E-Banking has published extensive recommendations regarding security procedures and other loss prevention measures.[[1]](#endnote-1) The FFIEC materials describe e-banking risks in the areas of transaction/operations risks, compliance/legal risks, strategic risk and reputation risk, as well as useful e-banking risk management activities, including board and management oversight, managing outsourcing relationships, information security programs and administrative controls. They also provide a lengthy reference list of laws, regulations and guidance applicable to bank cybersecurity issues.

The Conference of State Bank Supervisors has its own *Resource Guide for Bank Executives*[[2]](#endnote-2) that describes four common categories of cyberattacks against banks:

* Distributed Denial of Service – attackers overwhelm a banks’ website with traffic in order to disrupt online service, causing reputational harm and potentially distracting the bank from some other fraud.
* Corporate Account Takeover – attackers impersonate a bank’s business customer and request unauthorized wire and ACH transfers to accounts controlled by the attackers.
* ATM Cash Out – attackers gain access to and alter the setting on ATM web-based control panels, causing large-dollar losses.
* CryptoLocker – attackers send phishing emails to bank employees that contain malware to infect the bank’s computers and encrypt its data. The attackers then demand a ransom payment in order for the bank to recover access to its files.

Obviously, large investments in technology and training are required to mitigate against each of these risks. However, the second category of risk—the corporate account takeover—requires the customer’s cooperation and vigilance.

Fortunately, the Uniform Commercial Code helps banks avoid the risk of loss on commercial accounts through account agreements that provide for robust security procedures, such as “dual control,” to verify the authenticity of payment orders. Account agreements should require that customers follow and maintain the confidentiality of the specified security procedures. They should also require that customers prevent unauthorized access to accounts and immediately notify the bank of any unauthorized access to or disclosure of confidential information to unauthorized persons.

Banks who use third-party vendors should also review their vendor contracts and confirm that the vendor is required to implement commercially reasonable security procedures and to provide immediate notification of suspicious activity.

Finally, banks should discuss cybersecurity insurance with their professional liability insurance agent to understand what cybersecurity coverages are available, as well as what exclusions, caps and deductibles might apply. This is a new and evolving insurance product and significant differences exist from policy to policy.

For more information about cybersecurity legal and regulatory considerations contact Mel Tull, VBA General Counsel, at [mtull@vabankers.org](mailto:mtull@vabankers.org) or (804) 819-4710.

*This article has been prepared for informational purposes only and is not legal advice.*

1. <http://ithandbook.ffiec.gov/it-booklets/e-banking> [↑](#endnote-ref-1)
2. <https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf> [↑](#endnote-ref-2)