Commercial Financial Services Brief: Responding to the Heartbleed SSL Vulnerability

April 14, 2014

The FFIEC issued guidance to banks on April 10, 2014, in connection with the recently discovered Heartbleed flaw in the internet security protocol known as OpenSSL. OPENSSL is an open source internet encryption protocol used by many websites for conducting secure online transactions. The flaw potentially leaves otherwise secure transactions subject to theft of authentication credentials (e.g., passwords, etc.) and other information stored in the computer's memory.

Heartbleed has been characterized as one of the most significant threats to secure internet transactions ever found. This is a major security flaw that potentially puts the confidentiality of user authentication credentials at risk, including the authentication credentials of your employees when signing into insecure web based online services.

As part of your data security and vendor management programs, you are required to monitor threat developments and take appropriate remedial actions. In the guidance the FFIEC reminded financial institutions of their obligations in this regard. In particular, the FFIEC stated that:

Financial institutions should monitor the status of their third-party service providers and vendors' efforts to implement patches on software that uses OpenSSL and to take the following steps, as appropriate:

- *Ensure that third-party vendors that use OpenSSL on their systems are aware of the vulnerability and take appropriate risk mitigation steps.*
- *Monitor the status of the vendors' efforts.*
- *Identify and upgrade vulnerable internal systems and services.*
- *Follow appropriate patch management practices and test to ensure a secure configuration.*

Given the severity of this risk, the following enhanced steps should be considered:

1. Review your software and technology vendors to identity those programs, products or services that your financial institution uses that may use the OpenSSL protocol. This may require directly contacting your vendors to inquire regarding OpenSSL and Heartbleed.

2. Identify what steps are required in order to remediate the threat and the timeline that the vendor proposes for taking such remedial actions. For critical, high risk systems, you may want the vendor to certify that it is either not affected by Heartbleed or has implemented remedial measures.

3. Document the steps you have taken and the responses received from vendors.

4. Consider whether it makes sense to provide additional education to your customers about the risks presented by Heartbleed as part of your customer service efforts.

If you have questions regarding how to address this situation, please contact George Meinz at 320.252.4414 or george.meinz@lathropgpm.com.