Complete Update

On April 8, 2025, the Office of the Comptroller of the Currency (OCC) notified Congress that it had identified a major incident resulting from a breach of the OCC's email system. The breach occurred when an unauthorized user accessed a number of OCC user accounts, including emails and attachments, via a service account with administrative-level privileges.

The OCC regulates and supervises all national banks and thrift institutions in the United States, and its breach announcement offers the following key takeaways for the banks and thrifts it examines so that they don't wind up making breach announcements of their own.

- Prioritize configuring and hardening Microsoft 365 environments, as well as providing timely alerts and reporting when changes are made. Also, ensure proper conditional access policies are in place and multi-factor authentication (MFA) is mandatory for all users.
- Invest in security information and event management (SIEM) and ensure real-time alerts are generated and read by the proper personnel.
- Use the principle of least privilege security. Be sure to restrict user access rights to the minimum necessary to perform job functions.
- Provide information security awareness training to your users to allow them to spot suspicious behavior.
- Conduct regular incident response roundtables so that staff members are equipped to deal with events like these.
- Update incident response playbooks to include Microsoft 365 breach scenarios.

You can read more on the breach **here.**

If you are interested in learning more about the information contained in this update or would like help with implementation, please reach out to us via inquiries@completecompli.com.

Dave McPhillips, CBCM, CBSM
Information Technology Consultant