BankOnITUSA®

THE CEO UPDATE

Q4 2024

A JOURNAL OF THE BANKONIT CEO FORUM

The CEO Update is the quarterly publication of BankOnIT's annual CEO Forum. It is developed to serve the BankOnIT community with thought-leading content from our team and vetted partners.

Donald Rumsfeld, Secretary of Defense of the United States of America, 1975-1977 and 2001-2006, is famous for saying, "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."

The same concept can be applied to technology decisions.

China outnumbers the USA 50 to 1 is a known known. Last month at the BankOnIT CEO forum, an FBI agent shared that state-sponsored Chinese hackers outnumber the FBI personnel dedicated to cyber defense by over 50:1. This is an example of a Known Known.

IT Firms Hiring North Korean Spies was an Unknown Unknown[1]. "When cybersecurity company KnowBe4 was filling a remote IT job in July, it hired a highly skilled applicant who gave his name as Kyle and spoke accented English. He asked the company to ship his company laptop to an address in Washington state. Kyle was actually in North Korea." This is an example of an Uknown Uknown. Read more of this article from *The Wall Street Journal* at this link North Korean Spies Are Infiltrating U.S. Companies Through IT Jobs - WSJ.

There's a fourth category - Unknown Known. MOVEit was an Unknown Known[2]. It's a file transfer system used by various entities to move files. While it was known that files were being transferred, it was not known (by many at least) how those files were being moved or that the MOVEit application was in use, or what impact unauthorized access to the application by cyber attackers would have.

CrowdStrike was a Known Unknown[3]. Companies that were using CrowdStrike knew they were using it; they likely did not know the level of access CrowdStrike had to the Microsoft operating system and the resulting business impact an errant update could cause on business operations. This is an example of known unknown.

The following matrix may help determine areas of technology where your institution is taking risks you are unaware of and, as a result, not accounting for your institution's risk management strategies.

Awareness-understanding matrix

	Aware	Not Aware
Understand	Known Knowns: Things we are aware of and understand	Unknown Knowns: Things we understand but are not aware of
Don't Understand	Known Unknowns: Things we are aware of but don't understand	Unknown Unknowns: Things we are neither aware of nor understand

According to a recent survey of community banks by BNY[4], respondents cited cybersecurity risk as their top challenge.

Cyber risks pose significant financial sector and broader U.S. economy threats, according to the Spring 2024 Semiannual Risk Profile released by the OCC[5]. Cyberattacks continue to evolve and become more sophisticated and pervasive throughout the financial sector. The OCC report further states threat actors continue to exploit publicly known software vulnerabilities and weak authentication controls

at targeted organizations, including banks and financial service providers.

The OCC recently released their Bank Supervision plan for 2025[6] and provided the following areas of focus:

- Examiners will continue to focus on the adequacy of banks' preventative controls, incident response, data recovery, and operational resilience.
- Examinations will emphasize incident response, backup, and operational resilience capabilities to withstand or recover from cyberattacks, especially for critical operations.
- Examiners will also consider cyber intelligence gathering, sharing, and analysis; threat and vulnerability detection; and strong authentication and access controls, including the use of multi-factor authentication, to include third-party access management, network management, and data management.

OCC banks must maintain heightened threat monitoring and effective controls to safeguard against disruptive financial sector attacks. The FDIC, Federal Reserve and state departments are likely to quickly follow suit.

A recent *Wall Street Journal* article discussed how the Justice Department is fighting Cybercrime[7]. The Assistant Attorney General for National Security was interviewed for the article. This quote was particularly enlightening:

"Nation-state-sponsored cyber threats are increasing in sophistication, increasing capability, and persistence with the intent to use cyber-enabled means to carry out a range of threats. We're most concerned about China, Russia, Iran, and North Korea. The range of threats extends from traditional espionage—classified information on government systems—to seeking to obtain trade secrets from some of our leading technology companies. Probably the most concerning are the threats to our critical infrastructure." (As a reminder, banking is considered a part of our critical infrastructure).

The new password manager app from Apple is Free and is available with the latest iPhone, iPad, and Mac software[8]. It suggests unique, unguessable passwords when you sign up for new accounts and fill them in whenever needed.

According to Gene Ludwig, former Comptroller of the currency, quoted in a recent American Banker article[9], "Despite the significant progress made in addressing cyber threats, it is surprising that technology risk is not yet treated as a major risk vector in all financial institutions, on par with credit risk, compliance risk, fraud, and cyber risk. This is not solely a matter of government regulation but a fundamental issue of good banking practice. It is essential to consider everyday operational and tail risks associated with technology. For too many banks, governance in this area remains weak, and CEOs may not have a full understanding of the risks being faced or the measures being taken to mitigate them."

Are you a bank CEO or board member with questions about technology at your institution? Contact us at solutions@bankonitusa.com or 405-653-1920.

[1] North Korean Spies Are Infiltrating U.S. Companies Through IT Jobs - WSJ
[2] Latest MOVEit Data Breach Victim Tally: 455 Organizations – BankInfo Security
[3] Massive Global Tech Outage: CrowdStrike Update Slams Banks, Airlines And More - Forbes
[4] BNY Survey
[5] OCC Report Highlights Key Risks in the Federal Banking System
[6] OCC Bank Supervision Operating Plan
[7] How the Justice Department is Changing Its Tactics on Cybercrime - WSJ
[8] Apple's New Password Manager is Free - WSJ
[9] Banks must get serious about measuring and mitigating AI-related risk – American Banker