Banking Update

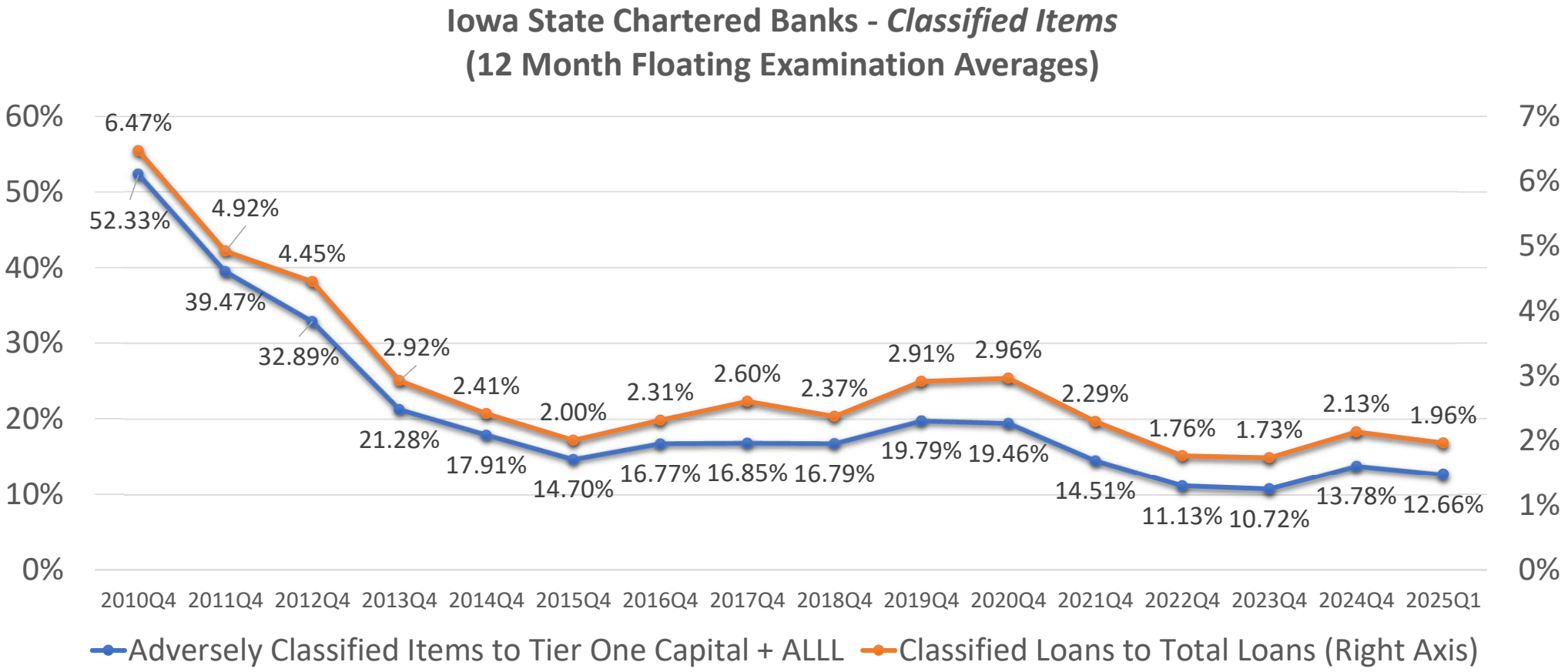
James Johnson

Superintendent of Banking

IOWA | Division of Banking

Iowa Community Banks Matter!

Classifications remain relatively low, but we are starting to see signs of stress.



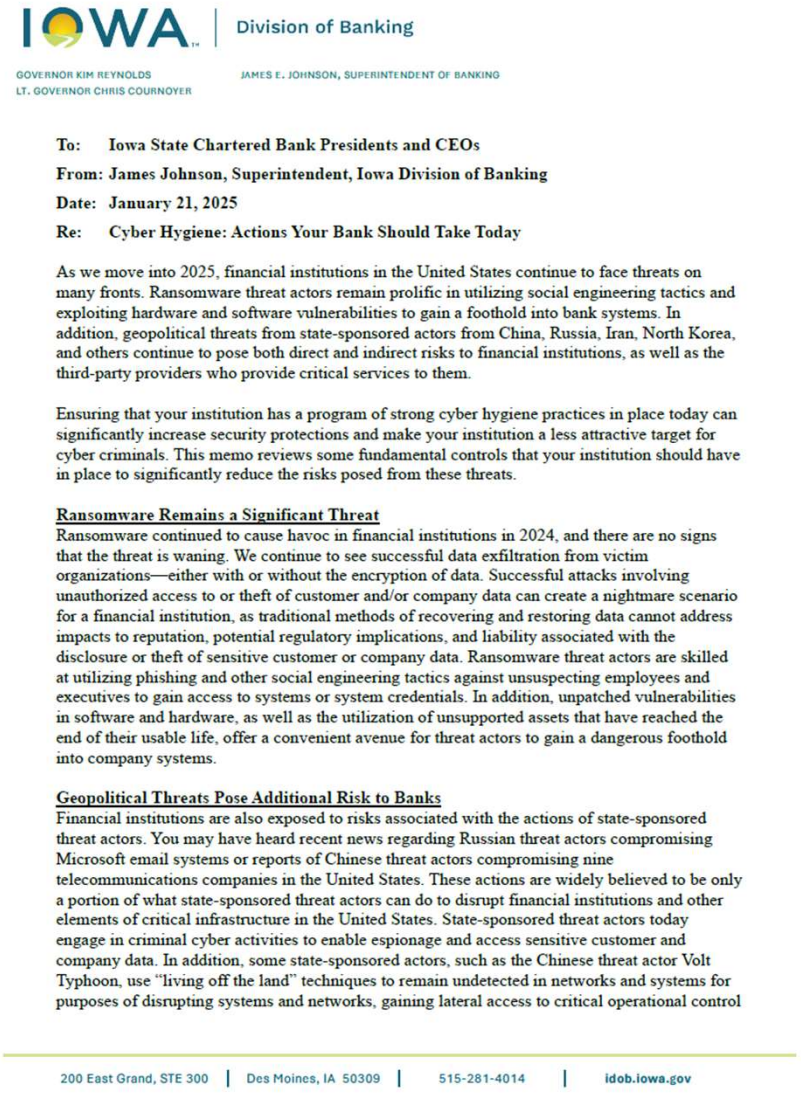
Observations from Recent Examinations

- Earnings challenges
- Tighter liquidity
- Leadership/staff turnover
- Information Technology weaknesses

CYBER HYGIENE INDUSTRY AWARENESS EMAIL

From the Superintendent of Banking on January 21, 2025
To Iowa State Chartered Bank President and CEO's

Please help make sure this document gets in the hands of senior management and IT officers.



IOWA | Division of Banking

GOVERNOR KIM REYNOLDS
LT. GOVERNOR CHRIS COURNOYER

JAMES E. JOHNSON, SUPERINTENDENT OF BANKING

To: Iowa State Chartered Bank Presidents and CEOs

From: James Johnson, Superintendent, Iowa Division of Banking

Date: January 21, 2025

Re: Cyber Hygiene: Actions Your Bank Should Take Today

As we move into 2025, financial institutions in the United States continue to face threats on many fronts. Ransomware threat actors remain prolific in utilizing social engineering tactics and exploiting hardware and software vulnerabilities to gain a foothold into bank systems. In addition, geopolitical threats from state-sponsored actors from China, Russia, Iran, North Korea, and others continue to pose both direct and indirect risks to financial institutions, as well as the third-party providers who provide critical services to them.

Ensuring that your institution has a program of strong cyber hygiene practices in place today can significantly increase security protections and make your institution a less attractive target for cyber criminals. This memo reviews some fundamental controls that your institution should have in place to significantly reduce the risks posed from these threats.

Ransomware Remains a Significant Threat

Ransomware continued to cause havoc in financial institutions in 2024, and there are no signs that the threat is waning. We continue to see successful data exfiltration from victim organizations—either with or without the encryption of data. Successful attacks involving unauthorized access to or theft of customer and/or company data can create a nightmare scenario for a financial institution, as traditional methods of recovering and restoring data cannot address impacts to reputation, potential regulatory implications, and liability associated with the disclosure or theft of sensitive customer or company data. Ransomware threat actors are skilled at utilizing phishing and other social engineering tactics against unsuspecting employees and executives to gain access to systems or system credentials. In addition, unpatched vulnerabilities in software and hardware, as well as the utilization of unsupported assets that have reached the end of their usable life, offer a convenient avenue for threat actors to gain a dangerous foothold into company systems.

Geopolitical Threats Pose Additional Risk to Banks

Financial institutions are also exposed to risks associated with the actions of state-sponsored threat actors. You may have heard recent news regarding Russian threat actors compromising Microsoft email systems or reports of Chinese threat actors compromising nine telecommunications companies in the United States. These actions are widely believed to be only a portion of what state-sponsored threat actors can do to disrupt financial institutions and other elements of critical infrastructure in the United States. State-sponsored threat actors today engage in criminal cyber activities to enable espionage and access sensitive customer and company data. In addition, some state-sponsored actors, such as the Chinese threat actor Volt Typhoon, use "living off the land" techniques to remain undetected in networks and systems for purposes of disrupting systems and networks, gaining lateral access to critical operational control

200 East Grand, STE 300 | Des Moines, IA 50309 | 515-281-4014 | idob.iowa.gov