Community Banks Are Left Unprotected as **Cybersecurity Risks Increase**

Cybersecurity attacks are the biggest threat to the U.S. financial system as international, national, regional and community banks are all under attack. Even though Banks with less than $1 billion in assets were the victims of nearly half (47%) of all bank-related cyber-crimes, regional and community bank CEOs and board members leave it up to IT and annual exams to protect their financial organization and their customers. This executive brief shows why the whole financial organization needs to take responsibility for reducing information security risk and how CEOs and board members can protect the bank from brand damage, customer disloyalty and financial implications.

In his 2019 letter to shareholders, JPMorgan Chase's CEO Jamie Dimon wrote: "The threat of cybersecurity may very well be the biggest threat to the U.S. financial system." It impacts banks across the spectrum: international, national, regional, and community. In fact, in a Forbes article titled "5 Cybersecurity Myths Banks Should Stop Believing," I learned that a study from Nationwide showed:

Banks with less than $1 billion in assets were the victims of nearly half (47%) of all bank-related cyber-crimes between 2012 and 2017.

Financial institutions with less than $35 million in revenue accounted for 81% of hacking and malware breaches in 2016--a jump from 54% the previous year.

Amid an accelerating rate of attacks and incidents, many community bank CEOs and board members leave it up to their IT department and annual exams to protect them. But, security is not just an IT issue. It is a business risk issue that can cause brand damage and customer disloyalty. It can reduce your bank's competitive edge over larger, national banks. It can result in financial implications and affect the future of the bank.

Why is cybersecurity such a threat when banks must undergo annual regulatory exams of their IT systems and processes?"

The threat of cybersecurity may very well be the biggest threat to the U.S. financial system.

JAMIE DIMON
CEO, JPMorgan Chase

I understand that these exams are just checks and balances. The regulators are checking if banks have systems and processes in place for "what if" scenarios. There is no "stress test" to confirm if those systems and processes are effective. Because auditors are checking off items without any real confirmation of its effectiveness, I call the standard testing a rubber-stamped approach that focuses on prevention. This may be useful in protecting against untargeted attacks, but it is insufficient to secure financial organizations from determined assailants. The uncomfortable reality is that attackers are gaining entry with relative ease and are usually able to sit undetected in bank systems for an average of 200 days. It's why FinCEN recently warned banks about business email compromise scams.

Getting confirmation is vital because many banks (primarily regional and community banks) lack a culture in which the institution as a whole takes responsibility for reducing information security risk. Often information security is the sole responsibility of the CISO, and there is insufficient leadership, awareness, and expertise at the board level. Banks commonly fail to provide their staff training, tools, or incentives. Employee negligence and malicious acts account for two-thirds of cyber breaches. Less than 20% are directly driven by an external threat, according to a 2017 analysis by advisory firm Willis Towers Watson.

Getting a high score on the annual exam does not mean banks are protected.

Getting a 1 or 2 on the annual exam means a financial institution is doing what a regulator thinks it needs to be doing. But who says regulators are up to date on emerging trends within banking as consumers go mobile.

A 2018 study from Accenture reported on the cybersecurity of 30 major banking applications. All 30 apps had at least one known security risk identified, and 25% of them included at least one "high-risk security flaw." And it's not just mobile where banks are seeing problems with the software. Their web-based banking applications have also shown to lack security, with one report calling the financial sector the "most vulnerable to attack" of all the industries tested.

What about 3rd party networks and IoT?

Banks do not just have to worry about the security of their own systems. They have to worry about their customers' systems as they are another cyber vulnerability. Hackers are using online accounts to gain entry into the bank's networks. The risks multiply as banks pile update upon update on already creaking computer systems.

Shared banking systems and third-party networks are also a risk concern. As financial organizations become increasingly reliant on third-party vendors for their day-to-day operations, banks need to assess these vendors for cybersecurity vulnerabilities.

Lack of awareness in regards to third-party security could cost banks millions in 2019 and coming years, especially as payment functionality gets embedded on more "connected" devices.

While the Internet of Things promises exciting opportunities, banks face challenges adapting to its infrastructure and keeping systems and customers secure. This is why banks need to rethink cybersecurity and go beyond the standard, rubber stamping approach, as shown in the chart below:

Standard Rubber Stamped IT Approach	Aligned Business Technology Approach
Risk prevention	Risk Protection, Detection and Response
Checks if processes are in place for what if scenarios	Confirms processes are effective and can be executed through stress tests
Focuses on known threats and exploits	Uncovers current threats and yet to be published threats with early warning security systems
Checks if banks have tech & systems in place	Confirms that tech & systems are secure & effective
Attackers sit undetected for 200 days on average	Risk removal
What regulators think bank needs	Compliance + alignment of tech with business objectives and future trends and initiatives

CEOs, are you ready to protect your business?

next steps

Connect with me at JasonOnLinkedIn.com

SecuringYourTomorrow

1.800.549.3312

jfsmith@isgtech.com

K·Coe ISG