



The Seven Deadly Cyber Threats

by [Steve Brown](#)

Did you know that research finds 85% of successful data breaches target the top 10 known vulnerabilities? That isn't the news here though. What is news is that all of those breaches could have been prevented because patches were available. The companies impacted had not updated their patches. Now you know why regulators are focused on something as mundane as asking about patch updates during IT exams.

Educating employees and customers about the myriad common cybersecurity threats that community banks increasingly face is critical. According to Chicago Fed research, there are 7 cyber threats or cyber-related risks that are the most common in community banks. We cover all but third-party vendor risk, which we recently discussed on Mar 16th.

Malware: This one is perhaps the best known and most widely discussed. It represents any software that is used to disrupt computers or networks, gather information or access private systems. As you likely know, malware typically works by breaching a bank's network through vulnerabilities or weak points of attack, and can infect storage media like USB sticks, mobile phones or tablets. These are often connected to computers, and through malware, hackers deliver computer viruses, ransomware, spyware and botnets. Since malware is often distributed via drive-by downloads, email attachments, file sharing or phishing, it is the most common cyber risk. Prevention is about educating your employees and doing regular IT updates.

DDoS: Distributed denial of service attacks have been on the rise over the past 5Ys as a main attack type on US banks. Here, cybercriminals utilize millions of computers to send simultaneous requests to a single bank computer or website. This floods the system so the bank's network is shut down or disrupted. While IT teams are distracted dealing with this issue, cyber criminals attack elsewhere and try to slip through defenses. Prevention here includes limiting router flows, adding filters, layering defenses, timing out open connections and increasing network scale.

Takeover: Corporate account takeover happens when cybercriminals essentially steal the identity of a business. They take control of a business customer's bank account, steal legitimate online banking credentials and then use those to process a money transfer to an offshore account. Prevention here includes setting more safeguards and closely monitoring suspicious activity (business), as well as following proper procedures to the letter and alerting clients of oddities (banks).

Leakage: Data leakage is the unauthorized transfer of confidential data without permission from the bank. This can happen either electronically or through storage devices such as USB drives. These incidents can also be intentional or unintentional, and, according to SANS Institute, nearly 75% of data leakage incidents involve customer data. Prevention includes disabling thumb drives and installing software that tracks, quarantines, notifies and blocks such attempts.

Vulnerabilities: Mobile and web application vulnerabilities are essentially flaws within the applications that sit on smart phones or at a bank's website. These flaws are discovered by hackers

and exploited to gain access to your mobile or online platform. Once inside, hackers steal data, take over customer accounts or even take control of a bank's internal network. Unfortunately, the more mobile banking continues to grow, the greater this risk. Prevention includes improving server controls, improving authentications/authorizations and adding encryption.

Changes: Weaknesses in project or change management commonly occur as a result of poor documentation and risk analysis. These can expose a bank's systems and important data. Since banks use project management to manage changes in their IT infrastructure, support new business processes or integrate new technologies and products, vulnerabilities in these processes can be exploited by cybercriminals to gain access. The best thing to do here is to review your change management processes and beef them up as needed to ensure a quality structure.

Recall that regulators view cyber risk as a national security issue that goes well beyond banking, so take proactive, strong and continual steps to protect yourself and your data.

BANK NEWS

Printing Buildings

Deloitte research finds 3D printing technologies used in engineering and construction reduces the time it takes to build a building by 50% to 70%, cuts labor costs by 50% to 80%, increases efficiency and enhances quality. More and more buildings are expected to be built using 3D printing in the coming years.

M&A Activity

1) Inland Northwest Bank (\$636mm, WA) will acquire CenterPointe Community Bank (\$131mm, WA) for consideration of approximately \$12.85 per share if electing cash (40%) or 1.0280 shares of common stock if electing stock (60%).

Real Estate

Research by the Urban Land Institute (ULI) projects commercial real estate markets will continue to soften over the next few years.

Confidence

A survey by JPMorgan finds 80% of middle market business executives and 62% of small business executives say they are confident about the economy. Both are up sharply and almost double the level seen last year.

Bank Lending

Bank Director research finds US lending activity totals \$15T of which banking represents about 44% of the market.

Copyright 2018 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.