BankOnITUSA
Originator of the Bankers Private Cloud
Securely Expanding Your Capabilities

Strategic Technology Update

June 6th, 2014

QUALITY ENDORSEMENTS
CBSC SERVICES

BankOnIT is a a CBSC Preferred Provider of the Bankers Private Cloud; providing a secure and reliable network for your bank, with the flexibility and infinite scalability to meet your strategic and operational goals.

For more information about BankOnIT and The Bankers Private Cloud Please Contact:

Cherlyn Lee
Senior Vice President
clee@bankonitusa.com
618.407.5770

Bankers
PRIVATE CLOUD

CEOs Are Being Held Accountable for Information Security

When Gregg Steinhafel rose to the ranks as CEO of Target, he likely banked on his rich retail experience that began as a youngster in the family furniture store to catapult him and his company to further success. Retail was his business.

But after a data breach left forty million Target customers with stolen credit- and debit-card numbers last December, Steinhafel learned what is becoming a reality for CEOs: knowing how to protect your customers through computer security is as important as company strategy or growing profits.

The data breach and how Target handled it – the company was slow to contact customers and has been accused of not responding to security alerts that may have prevented the attack – were factors in Steinhafel's resignation in early May. Though Target isn't the only retailer to have been hacked recently, Steinhafel is the first CEO to lose his job after such an incident.

Retail executives aren't alone in this new reality. Bank CEOs typically have substantial banking experience and understand the risks involved in lending, investments and even traditional bank operations risks. But these same CEO backgrounds that have made them successful bankers may not have prepared them to strategically manage information technology risks. Ultimately it's the board and the CEO who are responsible for ensuring their customers' data – and money – is protected.

The Federal Financial Institutions Examination Council (FFIEC) emphasized the importance of executive leadership having knowledge of information technology risks and mitigating those risks in a recent webinar for nearly 5,000 community bank CEOs and senior managers.

In the webinar, the FFIEC stated that bank CEOs and boards must set the tone from the top in building a security culture. Steinhafel's resignation underscores this point further. While it was once acceptable to delegate all things IT-related to lower-level personnel, bank regulators and boards now recognize that information technology and computer security need oversight from the top.

The potential problems and risks facing information technology are changing as quickly as new technology is evolving. Because those risks are becoming more complex and frequent, the burden can no longer fall to IT personnel. Managing information security risks is a strategic issue that banks must factor into the institution's overall operations.

But when a bank CEO's background is in lending and investments, making the leap to becoming an IT expert can be overwhelming. Utilizing outside experts is a good way to bridge this gap. Many financial institutions are moving toward cloud-based services to improve efficiency, reliability and information security while minimizing risk -- including regulatory and strategic risks – that are present in today's rapidly changing technology environment.

While technical capabilities and efficiencies can be gained by using an experienced vendor, the bank must properly manage the vendor relationship.

The FFIEC recommended in its recent webinar that bank CEOs create a governance plan that ensures ongoing awareness and accountability with IT service providers. CEOs are to specifically provide senior management with timely reports and meaningful information including addressing the bank's vulnerability to cyber threats.

Comptroller of the Currency Thomas Curry underscored these points in a speech in April and noted that it is critical that banks monitor compliance of third-party vendors.

“We expect the board and management to ensure that appropriate risk management practices are in place, that clear accountability for day-to-day management of these relationships is established, and that independent reviews of these relationships will be conducted periodically,” Curry said.

Regulatory knowledge, technical capability, internal controls and reporting are all elements needed for a successful vendor relationship. Cloud computing vendors that are regulated, that in turn do not outsource and provide the bank the necessary reporting, can help banks operate more efficiently, be better prepared for future cyber threats and help meet regulatory compliance demands.

About the author
Robert Mendez is a former banker and joined BankOnIT in 2007 as Executive Vice President. He has over 30 years experience in the banking industry including as a banker, banking software company founder, teaching and writing about banking and technology. He received a BBA in Finance, obtained his MBA from Oklahoma City University and is a graduate of the Graduate School of Banking of the South at Louisiana State University.

QUALITY ENDORSEMENTS
CBSC SERVICES

BankOnIT is a a CBSC Preferred Provider of the Bankers Private Cloud; providing a secure and reliable network for your bank, with the flexibility and infinite scalability to meet your strategic and operational goals.

For more information about BankOnIT and The Bankers Private Cloud Please Contact:

Cherlyn Lee
Senior Vice President
clee@bankonitusa.com
618.407.5770

Bankers
PRIVATE CLOUD