A Key Trait of a High-Performing Bank - a Culture of Awareness

BY JASON CORDER

We regret that an error appeared in this article in the Summer issue. We are re-printing the article with corrections. We apologize for any confusion this may have caused and have taken steps to ensure that such errors do not occur in future publications. Thank you for your understanding. ACB

If you ever read automobile reviews in websites or magazines like *Car and Driver* or *Motor Trend,* you probably know that there are different factors that make a sports car an "outstanding car."

Some of these things are obvious and measurable, such as horsepower, torque, acceleration times, and stopping performance. There are other traits that are not as obvious on paper and can be harder to measure. Things such as how a car handles, the optimal level of driver feedback, and the comfort of a car are difficult to measure but are very important to what makes a car an outstanding car. In the same way, most high-performing banks have several identifiable traits that are easy to recognize by looking at performance ratios and measurements. These traits, shown on a report like the *Uniform Bank Performance Report* (UBPR), include a strong Net Interest Margin, indicating that a bank's interest incomes and interest expenses are effectively managed. Another indicator typically present at a high-performing bank is a low "Net Losses to Average Total Loans and Leases" ratio which, along with low past due ratios, speaks to management's effectiveness in overseeing credit risk. Another trait one sees in a high-performing bank is a lower-than-peer Efficiency Ratio, which shows that management has established a good balance between net interest income and noninterest income against overhead expenses.

There are other traits present in a high-performing bank that are not as straightforward. These traits are more subjective, a little more "touchy-feely." Traits such as providing an excellent customer experience and engaging in beneficial community involvement can lead to strong financial performance, but these traits have more to do with a bank's culture rather than financial data. In our firm, which works with over 150 banks in thirty states, we've noted that high-performing banks nearly always have a "culture of awareness." Awareness is defined as "knowledge and understanding that something is happening or exists." This concept of awareness can be applied at every level of a bank, whether it is knowing which customers are the most profitable and least profitable and responding appropriately, awareness of changes in the local market that might impact a bank's customer base, or an understanding of trends in bank technology that may require a bank to make strategic shifts to accommodate those changes. Establishing a culture of awareness is especially important in the areas of security and risk identification/risk management. Each of these areas are interrelated, and security awareness can be considered a component of risk management. Developing an enterprise-wide culture of awareness in these areas can result in an engaged Board of Directors, knowledgeable bank personnel, and connected customers.

Jason Corder is a Senior Vice President with Sawyers & Jacobs LLC, a consulting firm focused on serving financial institutions. Sawyers & Jacobs is an ACB Associate Member. Jason may be reached at 901-828-1942 or jcorder@sawyersjacobs.com.

Security awareness has been necessary since the dawn of banking. However, security risks are constantly changing, and the prolific and evolving threats from cybersecurity should continue to be a primary focus of bank management. The Federal Deposit Insurance Corporation (FDIC) noted in its *2022 Risk Review* that the operational risk from cyber threats and illicit activities is a "key risk to banks." The FDIC stated that "Operational risk in banking is one of the most critical risks to banks. Cyber attacks continue to evolve, become more sophisticated, and multiply as bad actors discover creative ways to exploit technological and operational vulnerabilities." Having a culture of awareness is a vital step in addressing information security and cybersecurity risks. Bank networks, systems, and levels of access should be configured in such a way that cybersecurity-related risks are minimized. Having a robust security awareness program works in a complementary way with technical controls and can supercharge a bank's ability to effectively prevent and respond to information security and cybersecurity threats.

A robust security awareness program typically has a few defining characteristics. The most important aspect of a security awareness program is a top-down emphasis from the Board of Directors and senior management. This means that management understands and prioritizes security. This results in adequate resources and training for those directly responsible for a bank's security and for bank personnel as a whole. Bank personnel will see that ongoing training and testing programs are prioritized activities rather than simply "check the box" activities. Outside expertise will be engaged as needed to conduct training and testing. Those occasions when employees' awareness is lacking (i.e., failing phishing tests or not shredding sensitive customer information) will be seen as opportunities for effective education rather than "name and shame" events. Employees can then be a part of the bank's frontline defenses in the same way that they are for customer service. Additionally, employees that are knowledgeable about security can be more effective in training a bank's customers on how to use bank products safely and securely.

At a broader level, having a culture of awareness concerning risk

Continued on Page 20

MAKING BANKS BETTER.

INNOVATION. RISK MANAGEMENT. CYBERSECURITY. TECHNOLOGY.

IT Audits • Cybersecurity Assessments • Core Evaluations
Strategic Technology Plans • Vendor Management • Risk Assessments
Information Security Officer (ISO) Coaching • Cybersecurity Incident
Response Testing • Penetration Testing • Cybersecurity Board Education
Business Continuity Plans • GLBA Compliance • Digital Services Strategy

sawyersjacobs.com

901.853.1000 • info@sawyersjacobs.com

ACB Associate Member

Follow Us on Social

management is essential in a high-performing financial institution. Our firm facilitates risk assessments for enterprise risk, information security, cybersecurity, business continuity, digital banking, vendor management, and several other areas, and the purpose of these risk assessments is **awareness.** What assets (e.g., systems, information) does the bank have? What are the threats to those assets? What is the likelihood of those threats occurring? What is the magnitude of impact should threats occur? What are the mitigating controls to reduce the risk from those threats? What is the residual, or remaining, risk after considering the bank's controls?

Lastly, what is the bank's risk response? Knowing the answers to these questions and verifying that measured risk levels align with the Board of Directors' **clearly defined** and **clearly communicated** risk appetite results in an awareness of what actions need to be taken to maintain acceptable levels of risk. Such risks might be threats such as ransomware attacks or unauthorized access to bank systems, but it could also be risk to the Bank's reputation because the bank's online banking system is clunky or experiences frequent downtime. A culture of awareness results in the correct people being **promptly informed** when a risk is elevated and in **corrective action** to bring the risk back to acceptable levels.

One final thought: if you have a high-performing (and expensive) sports car, you will want a competent mechanic who specializes in keeping your make and model of car at a level of optimum performance. In the same way, having the right partner to provide expertise in reviewing the quality of the bank's oversight for the bank's systems, security, risk management, and awareness is incredibly important for maintaining the bank's level of high performance. As you work to identify that important strategic partner, consider factors other than price. For example, the vendor providing your IT audit should be someone you rely on to assess the state of your bank and make recommendations that help to make the bank better. While reasonable pricing is important, like engaging your bank's legal counsel this is not an area where it's wise to simply put the work out for bid and choose the low-cost provider; instead, bank-specific expertise, firm reputation, and experience should weigh heavily in your decision. And, ultimately, this helps the bank to have a stronger culture of awareness, which can lead to a higher-performing bank and a smoother ride across an increasingly competitive and uncertain landscape!

_____

1 https://www.merriam-webster.com/dictionary/awareness

2 https://www.fdic.gov/analysis/risk-review/2022-risk-review/2022-risk-review-section-3.pdf

ACB

SAWYERS & JACOBS