Addressing Insider Threats, Cyber Attacks & Data Security

Insider threats are not new; these have been imminent since the very first banks opened their doors. However, the difference between then and now is that many of these once 'traditional' and simplistic threats are becoming more sophisticated and complex. Therefore, banks need to take additional precautions in detecting, preventing, and mitigating these insider risks posed by their internal staff, vendors, contractors, and any other individuals who may have access to secure systems and private information. Here is a list of best practices to help manage insider threats:

Enforce dual controls/segregation of duties. This is a key loss prevention measure to help keep everyone inside the bank, at a vendor, or contractor honest.

Perform internal audits of the various functions within the bank to help keep staff in check.

Invest in culture enhancement programs like Integrity Solutions® to help keep staff from creating dishonest acts.

In 2016, there will primarily be two different types of cyberattacks: (1) external cyberattacks involving merchant data breaches that steal customers' payment information and (2) internal cyberattack involving a breach from within the bank. The following are the measures banks can take to implement more trusted layers of security and get ahead of these cyberattack:

Educate employees and customers about risk prevention measures they should take.

Utilize designated computer(s) for storing secure information, and put protective measures in place to ensure these computers are never used for emailing or web browsing.

Implement dynamic payment card security measures, such as end-to end encryption, tokenization, chip technology, or biometrics.

Educate yourself about trending risks through networking with peers and utilizing public risk education resources like free webinars and industry publications.

Also, don't forget about the need to perform the file security and help protect critical data:

Secure all perimeters wherever any secure files or data resides – ensure this is done on site, as well as with your vendors and/or contractors.

Implement protection solutions to guard inbound and outbound data loss – such as the risk protection services and tools offered by Allied Solutions.

Centralize management technology.

Finally, consider implementing the following proven risk mitigation strategies to help optimize security layers and get ready for the threats and challenges to come in 2016:

Utilize a financial intelligence unit (FIU) to find the source of fraud and criminal activity and help optimize data security.

Adopt an enterprise risk management (ERM) strategy to align risk prevention initiatives with corporate initiatives.

Banks need to continue to be diligent in managing these areas of risk and ensure we never let our guard down! That's why it is essential we make strides toward becoming more sophisticated with how we manage risk exposures and aligning these goals and tactics with our overall business strategies.

Ann D. Davidson
Vice President
Risk Consulting

ALLIED SOLUTIONS

Contact Info
www.alliedsolutions.net
800.826.9384

Ann D. Davidson is the Vice President of Risk Consulting in the Bond Division at Allied Solutions, LLC and an active member of the International Association of Financial Crimes Investigators and the Wisconsin Automated Clearing House Association. Davidson has over forty years of diverse experience in the financial industry, including positions in claims, pensions, underwriting, and loss prevention and has grown to be considered one of the nation's premier authorities on risk management products. As a well-known expert in risk control and risk management products, Ann has developed an impressive list of achievements and accreditations in the financial industry. She has made notable contributions to numerous articles in accredited financial publications and has been a key-note speaker at hundreds of conferences and training seminars nationwide on a wide variety of timely risk management topics.