Katten Muchin Rosenman LLP CORPORATE & FINANCIAL WEEKLY DIGEST

Corporate & Financial Weekly Digest

Posted at 12:06 PM on May 13, 2011 by Jeffrey M. Werthan

Comptroller of the Currency Issues Incident Prevention and Information Security Alert to National Banks

On April 18, the Office of the Comptroller of the Currency (OCC) issued an alert to CEOs of National Banks and other regulated entities. The alert highlights the need for national banks and their technology service providers (TSPs) to take steps to ensure their enterprise risk management is sufficiently robust to protect and secure the bank's own and their customers' information. The OCC explained that several recent security breaches have highlighted the need for national banks and their TSPs to perform periodic risk assessments of their information security programs with respect to the prevention and detection of security incidents. Most security-related incidents occur because of the lack or failures of basic controls that allow attackers to gain entry into a target environment through phishing, spear-phishing, drive-by malware injection and other techniques. Once attackers have entered an environment, they typically use sophisticated tools and techniques to gain access to sensitive data or systems. Successful attacks often compromise sensitive customer information or create fraud. The increasing sophistication of the tools and techniques attackers use often includes stealth or other means that make their detection more difficult.

The OCC stated that it expects national banks and their TSPs to review carefully the National Security Agency's (NSA's) Information Assurance Advisory (March 28) and the United States Computer Emergency Readiness Team's (US-CERT) Early Warning and Indicator Notice (EWIN) 11-077-01A Update, both associated with one of the recent events. The NSA advisory provides detailed recommendations consistent with previously issued OCC and Federal Financial Institution Examination Council guidance. Access to sensitive information, systems and control components should be highly restricted and carefully monitored. National banks should ensure that their information security program or that of their TSP includes the evaluation and appropriate disposition of the above-mentioned recommendations based upon their environment and risk profile. The US-CERT EWIN contains a list of domains associated with malicious activity. National banks and their TSPs should prohibit network traffic, inbound and outbound, within those domains.

Click here and here to read more.