Ensuring Bank Cybersecurity Beyond Technology – Education
by Konrad Martin

When considering the banking industry, it seems almost automatic that banks would have some of the latest technological strategies and software in place when it comes to protecting their organizations from cyberattacks. In fact, all banks are subject to some form of personal data breach laws as well as FINRA (Financial Industry Regulatory Authority) oversight, which is a not-for-profit organization directed by Congress to protect investors by, in part, "writing and enforcing rules governing the activities of 3,700 broker-dealers with 630,000 brokers" and "examining firms for compliance with those rules." On its own, FINRA oversees up to 75 billion market transactions daily, and has implemented innovative technology including cloud computing combined with cutting-edge applications, programs and hardware to help identify and protect against cyberattacks. Combine the power of FINRA with each bank's own cybersecurity efforts, and these financial institutions would seem to be impenetrable fortresses that could defend the most cunning hacker's attack.

Yet given the scope of these institutions (i.e., money, lots of it and in various forms and currencies) and the potential payout if successful, banks continue to be the target of hackers' efforts. Extra security efforts are imperative to keep not only the coffers safe, but to protect against client doubt that they can trust a particular institution with, sometimes literally, their life's savings. Technology safeguards are important for sure, but there is another oft-overlooked strategy to protect against would-be hackers: education. Banks need to ensure they are providing their employees with the needed training to identify and thwart hacking efforts.

In fact, education is the easiest and best way for any organization to defend itself from cybercrime. Even for organizations that have transitioned to cloud-based computing, which offers the most cyberprotection, this high-level technology still needs education and training to ward off hackers. These days, most hackers have evolved in sophistication; rather than depending on the brute force of a nefariously devised program to break through a firewall, a hacker understands that he or she will have much more success targeting individuals, luring them to click on some kind of link that, unknowingly to the user, allows the hacker access to the whole network.

Sadly, the weakest part of any financial institution's security is the people. To fight this reality, employees should be educated on how to use the network and what attachments are okay to click on (and what attachments are not). This may sound easy; so easy, in fact, that many organizations skip this step and instead simply instruct their employees they can only open emails that come from people they know. Unfortunately, hackers have come to expect this – and they can easily use personal information about an employee which they've gleaned from social media to create imposter accounts. (In addition, there is no way of knowing whether the person you know has been hacked, and therefore the user would be responding to a hacked email.)

Frequently, this is known as "spear phishing." In these situations, a hacker can break into the email account of an administrator, by convincing the individual to click on something that seems harmless but allows the hacker to either implant keylogger software to record when the user types their login name and password, or sometimes connect directly into the email server. Then, when someone emails that administrator about a financial transaction, the hacker can respond as that administrator and offer alternative directions – wiring a deposit to a specific bank account instead, for example. This is all done without the original intended's knowledge of the matter – hackers can send emails and then delete the record of them right away or move emails to a mailbox the intended user doesn't see or can't access. Typically, by the time the true reality of these situations is realized, it's too late to ask the bank to reverse the transaction, and the money is gone for good.

Email, internet, social media – all of these are luxuries that must be treated responsibly. It's incredibly easy for a hacker to collect expansive information about an individual – including their address, names and ages of spouse and children, job, pets, and educational background – simply by spending a few minutes on Facebook (which, in addition to its issues with sharing user data, also experiences on average 600,000 hacks a day!). Policies and procedures must be put in place so that employees know how to appropriately manage both their personal and professional technology – for the benefit of everyone.

Given that banks are at higher risk for cyberattacks because they have what thieves are looking for, it only makes sense that these institutions fortify their technical security with the type of training and education necessary to be best-positioned for long, trusted client relationships.

Konrad Martin is co-founder and principal of Tech Advisors (www.tech-adv.com), a leading technology solution provider for small to mid-size businesses. He can be reached at konradm@tech-adv.com or 508-359-4028.