Tech Time: Preventing Potential Hacks

February 2015 – Vol: 38 No. 2
by Jim Deitch

It takes more than just your IT staff to make it happen

Feb. 25, 2015

The Sony, Home Depot, Target and other recent cyberhacks have credit union executives asking, “What can we do to prevent similar hacks to our systems?”

And it’s a good question.

Notably, most hackers don’t enter the security perimeter through traditional IT security systems. The “headline hacks” almost always begin with an employee or vendor inadvertently providing access. Lesser known financial services hacks have resulted in significant losses:

- A financial institution employee at work clicked on a link from an email that was supposedly from the president of that institution. The link inserted malware, which a hacker used to obtain complete network compromise, customer data, and a gateway into other systems in a federally insured financial institution.
- An employee clicked on a “spoofed” Wi-Fi connection that was thought to be secure. Logon information was stolen, and systems were compromised through insertion of malware into the initial compromised laptop.
- An assistant branch manager permitted an individual posing as a service technician from the financial institution’s third-party vendor access to a server, where malware was inserted and customer information was exfiltrated.

- An individual posing as a building maintenance vendor gained access to a branch, inserted a malware device onto the premises, and exfiltrated confidential data through that device.

To prevent hacks, consider the "safeguards" rule of the **Gramm-Leach-Bliley Act**, which calls for credit unions to use the best security approach that is both readily available and cost effective. Credit union CIOs and IT managers rightfully suggest they have deployed perimeter defense technologies to mitigate the chance of external penetration by hackers. That's good. Continuing in this vein, here are several guidelines credit unions can follow:

First, credit unions need to have different people in charge of testing and verification. A CEO would not permit a CFO to audit his or her own financial statements. Similarly, the CIO or IT executive should not test the IT security systems he or she has put in place. Discussions with senior federal regulators suggest security testing be completely independent of the IT day to day operating functions.

An IT-independent security risk management assessment should be conducted from a hacker/attacker's point of view to determine the credit union's current security posture and risk profile. This is *not* a "penetration test" performed on the credit union's IT hardware. Instead, this assessment should consider the types of physical, cultural, operational, system and internal control breaches that innovative hackers and employees could perpetrate. From it, a credit union should develop a security roadmap and implement security best practices to improve the organization's security maturity level. It's vitally important to assess and test physical, cultural and technology controls in

tandem.

In addition, credit unions need to ensure appropriate levels of physical security are in place to limit access to sensitive data storage, data centers, network infrastructure, and host systems. Train credit union employees at every location to challenge physical access to any facility, and to require verification from headquarters before granting any unknown person physical access.

If a credit union uses outsourced IT service providers, these vendors should provide a **SSAE 16** independent assessment of their systems inspection. It is critical that the "complementary controls" identified in the SSAE 16 be tested by credit union internal auditors or other independent assessment, and implemented by the credit union.

Network security usually has appropriate firewalls, routing and switching equipment. However, ensure appropriate security features, such as access control lists for sensitive network segments, are employed. There should be proactive detection and monitoring of network anomalies and intrusions. A Security Information and Event Management device should be installed and tuned properly to detect attacks and malware in real-time. A variety of SIEM devices and outsourced services are available that can fit within a credit union's budget. A formal incident response plan should be developed and exercised regularly.

Each credit union application should allow for the establishment of roles, rights and access views for defined parties. A detailed audit log should be provided that shows all access (by username and timestamp) to information and system configuration changes.

Effective security requires careful and frequent risk assessment followed by well-designed testing that is independent from the IT security function. The system compromises described above were not "brute force" attacks on an IT system or network; rather, the breaches occurred by employees circumventing established controls, or hackers that exploited common weaknesses in the overall system of controls.

James M. Deitch *is CEO and co-founder of Teraverde. Deitch is a thought leader in community and mortgage banking, having served as CEO of four community banks, including two de novo banks. He has served on the Mortgage Bankers Association of America Board of Governors for three terms, representing a community bank lender. He is a Certified Mortgage Banker, and has extensive secondary marketing experience as well as extensive regulatory experience with OCC, FDIC and state regulators, especially in the residential lending and community banking areas.*