Mid America Cooperative Council

MACC VOICE

February 2016 Newsletter

Mid America Cooperative Council
6302 Rucker Road, Suite H Indianapolis, IN 46220
Phone: (317) 726-6910 Fax: (317) 726-2630
E-mail: knowledge@macc.coop Web: http://www.macc.coop

IT Security Policies for Cooperatives

While high profile breaches at Target, Home Depot, and Sony dominate the headlines, **breaches at small businesses fly under the radar**. Yet these disruptions are often more devastating, to the point of business failure.

Churches and other organizations that never considered themselves targets are becoming victims of credit card fraud, automatic clearing house (ACH) fraud, and wire fraud. These crimes are often perpetrated from outside the country by attacking the online cash management features that banks provide their customers. You can take steps to protect your entity, but before taking action, you must first understand and acknowledge this growing threat. **The attacks fall into three main categories:**

- Theft of personal financial information
- Online banking malware (so-called corporate account take-over)
- Ransomware attacks (the most common being CryptoLocker)

Theft of personal financial information

Organized crime groups (primarily in Russia, Eastern Europe, and China) have created a high demand for personal financial information, including name, address, social security number, driver's license number, bank account number, and credit card details. Hackers steal this information then sell it to criminals who use it to commit various forms of identity theft. The more complete and associated to an individual, the more valuable the information is on a "wholesale" basis. Payroll databases, customer sales records, and supplier/accounts payable records are common targets for this type of attack. Indeed, as the price being paid to hackers escalates, smaller businesses are being targeted.

Online banking malware

Zeus, Citadel, Spyeye, and Gozi are just a few examples of the new breed of sophisticated online banking malware. Once a network is infected with this type of malware the online banking credentials (user ID, password, challenge questions) are harvested by the attacker, who then logs into the online banking server and executes fraudulent wires or ACH transactions. More sophisticated malware can bypass multifactor authentication tokens (often called corporate account takeover).

Malware code is often delivered via email, either by a file attached directly to the message, or more commonly, by use of a link to a rogue web page. In the latter case, the malware returns with the web page and installs itself on the victim's computer. This type of attack has been dubbed "spear phishing" since often only one email is sent to the victim organization. Spear phishing emails have improved significantly in their sophistication and effectiveness, and can be very difficult for users to identify as fraudulent. They often use carefully crafted scripts to entice the user to click the link. In some cases, the emails are even "spoofed," that is, they are crafted to appear to come from someone inside the victim organization (e.g., the company president). In other cases, the emails are designed so they appear to come from a legitimate business or organization, such as UPS, American Express, PayPal, or the IRS.

Ransomware

Ransomware is a malware that encrypts virtually all data and files that it can find, both on the local machine and on every network device to which it can connect. This renders the data unusable by the victim organization. Typically, the hacker requests payment (the ransom) in exchange for decrypting the affected data. This is how the hacker hopes to make his money. Having working backups that are regularly tested allows victims to wipe the affected machines clean and reinstall both systems and data.

CryptoLocker is by far the most common ransomware deployed. CryptoLocker attacks are increasing rapidly because they are easy and effective. Such attacks rose from 7,000 in April 2014, to more than 15,000 in May. Kovter is a ransomware variant with an especially malicious tactic. It dumps a payload of child pornography, in addition to the encryption, to put more pressure on the victim to comply with the ransom demand.

Protecting your business

Preventing these attacks is no small task. It requires a multilayered approach.

- Keep current on technical defensive measures such as firewalls, intrusion detection systems and spam filters.
- Keep up-to-date on the anti-virus software on each device, and complete regular scans to keep them clean.
- Keep all network servers and PC workstations current with the latest security updates and patches.
- Limit the number of PCs used to conduct online cash management. If possible, isolate them from the rest of the company network.
- Encrypt sensitive data, such as intellectual property and personal financial information.
- Utilize bank security tools for online cash management.
- Make regular backups of key data and systems and store them in a secure, off-site location.
- Monitor activity and balance online accounts, daily.
- Perform periodic vulnerability or penetration assessments to validate that controls are functioning as intended.

(excerpts from "Protecting Your Organization From Online Hackers", by Mark Eich)

IT Security Policies for Cooperatives (continued)

Premier Companies' CFO/Controller Mike Lafferty says, "As far as IT security, we take what I would say is a three step approach starting with addressing this risk, and what is and is not allowed in our employee manual. Then, all installations of hardware and software are coordinated and performed by our IT manager.

We do not allow employees to purchase and self-install anything that will be connected to our network. Finally, and this is key, we have hired an outside service (TLS.net) to monitor our network and update the security on all machines 24/7. This was expensive to set up as it required a major upgrade to our firewall, and dedicated VPN tunnels for all branch communications. However, based on the operational and reputational risk and what the cost of that might be, I think it was money well spent. Are we now bullet-proof? Absolutely not. You still have employees that don't lock their machines when they leave their desk. You also have the ever present social engineering threat as most hacks probably come from people talking their way in, but we do try to make our employees aware of this."

Cybersecurity for Small Business

This self-paced training exercise provides an introduction to securing information in a small business. Topics include: Defining cybersecurity; Explaining the importance of securing information through best cybersecurity practices; Identifying types of information that should be secured; Identifying the types of cyber threats; Defining risk management; and Listing best practices for guarding against cyber threats. Duration: 00:30:00
Please visit this link to begin the course: **https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses,** or for a text version of the course, please visit **https://www.sba.gov/sites/default/files/cybersecurity_transcript.pdf**

(this course is available through the U.S. Small Business Administration)

"LIKE US" ON FACEBOOK: https://www.facebook.com/pages/Mid-America-Cooperative-Council/115596228461591

"FOLLOW US" ON LINKEDIN: https://www.linkedin.com/company/mid-america-cooperative-council?trk=top_nav_home

"FOLLOW US" ON TWITTER: https://twitter.com/MACCcoop

Rod's Thoughts

Open communications and trust are the most important values in your board room. They are, also, important in strengthening your cooperative business and culture. What value do you place on open communications and the trust that what is said in your board room is held in confidence? Perhaps this is a beginning place for your co-op's brand image.

Each of our cooperative members and directors live in a competitive world, one where information has value and trust of securing that information is a game changer. The brand image of our co-op is of great value, and identity preservation is a primary concern of all.

I personally felt betrayed with the TARGET security breach. It was the second time that a business that stored my critical information was hacked. Have you had a similar experience? We trust those with whom we conduct business to secure our valuable information, and we feel violated when that trust is lost.

MACC is grateful that Mark Eich has presented to our financial conferences, in both 2014 and 2015. He stunned the audience in 2014 when he told us that "More money leaves the United States through cyber fraud from Russia than all the drug trade combined." He went on to explain the kind of industry that supports this activity.

The second big surprise we learned from Mark was that most of our risk could be managed with relatively simple steps, that are outlined in this newsletter. Just like the trust of confidentiality in our co-op board room, managing that risk is relatively simple through policies. However, it is very challenging to implement because people must decide how to implement the policies.

Our co-op's brand image is dependent on clear communications and understanding of our risk management policies. When we establish procedures and policies for minimizing IT risk, we communicate these procedures to everyone. Then, we go through training to make certain everyone understands, because it is how these policies are interpreted that create the cracks in our system.

Just because we are a cooperative, which is owned by and working for the mutual benefit of all our members, does not mean that all information is transparent. We are still a business, competing in the marketplace for the trust of our member/owners and a respected brand image. Elected directors must also be clear about how the boards' policies are interpreted. Regular training and conversations about what can be communicated to their fellow member/owners is appropriate. This is also a source of IT risk.

The best co-op boards spend time at each meeting building that trust in a variety of ways. Some hold regular "executive meetings," others bring in outside speakers to offer a different perspective, and others combine their annual planning meeting with a specific event to build deeper relations among directors. **Whatever the culture of your co-op, your brand image and IT risk is dependent on this trust built in your boardroom and your cooperative by reinforcing your established policies. Revisiting and clarifying these policies will have an impact on your cooperative business**.