THE SHOW-ME BANKER

THE VOICE FOR MISSOURI'S INDEPENDENT BANKERS

November 2017

MIBA
Missouri Independent Bankers Association

Security Conference
(see photos on page 24)

2 CYBERSECURITY CHECKLISTS:

1 for Your Bank and 1 for Your Bank Employees

By Todd Nielsen, JMARK Business Solutions, Inc.

In order to remain in business, stay competitive, and keep yourself and your bank safe from a data loss disaster, here is a fairly standardized checklist that should be followed if you expect to survive the oft-treacherous contemporary conditions of business computing and web connectivity. Here are 10 things you should have on your data network disaster survival checklist:

- ☑ 1. Implement a solid business continuity plan. This is perhaps the sine qua non in the world of IT support and protection. It allows a given entity to continue doing business through any cyber threat, data breach or natural disaster, such as fire, flood or earthquake that destroys part or all of a physical IT framework. Effective business continuity can occur because of cloud-based or offsite backup, which allows remote access to data via cloud servers.
- ☑ 2. Have a firm disaster recovery policy in place. As a subset (and very necessary) part of business continuity, disaster recovery, or DR, is essential to keeping a healthy IT network and a future in doing business in a web-based or cybernetic manner. It involves the employment of a set of procedures or policies that ensure the recovery of data, which is vital to business operations and continuation, generally through cloud-based means.
- ☑ 3. Utilize employee cyber safety training and policies in the workplace. Employee cyber safety training and strict policies will cut down significantly on the risk of incurring a serious data breach and any subsequent data loss, downtime or threat to the company's future operations.
- ☑ 4. Use antivirus protections on all computers on the network. Using effective antivirus software on all the computer terminals on your IT network will ensure the filtering out of spam, email phishing, malware and other exploits.
- ☑ 5. Don't ignore the suggested software updates. They may be annoying to most of us, but studies show that it's a bad idea to ignore the pop-ups from Microsoft and other tech or software platforms. Don't leave it to your staff to do. Have an IT support team like JMARK, which can force updates and upgrades, to eliminate the missing of these important updates.
- ☑ 6. Use cloud computing to cut down on overhead cost and data liability. Being able to use cloud computing services to collaborate on projects saves cost and liability in many ways.
- ☑ 7. Perform a regular network system check. This should be done by an IT professional or support team, and will analyze and report on any deficiencies in your IT network's infrastructure.
- ☑ 8. Perform regular PC maintenance. Performing regular PC maintenance has a built-in checklist of its own, which includes:
  - Daily data backup;
  - Weekly scans for malware;
  - Monthly disk defrags; and
  - Monthly scanning of your hard drive for errors.
- ☑ 9. Do semi-regular server maintenance checks. A server maintenance checklist, as part of healthy server management, should include such steps as backup verification, updating of your OS and control panel, changing passwords, and the checking of remote management tools, server utilization and system security.
- ☑ 10. Have the most proactive data loss prevention measures in place. This can include cybersecurity, intrusion detection and prevention, firewalls, antivirus software, cloud-based storage and software services, and can come as a "turnkey solution" with the an IT company like JMARK, and performance-assurance systems on the job.

Your Bank Employees

Hackers pose a critical threat to your bank cybersecurity, and incidents are increasing. Why? Because most employees don't know how to identify phishing scams and other cyber threats that can lead to a network infection or intrusion.

When your staff is properly trained, they're your first line of defense — and this training should not only include things like strict passwords and policies but extend to their workspace and behaviors. Here are a few tips to start off your training.

1. Always keep your system, software and web browsers up-to-date. If you don't, you're leaving your system exposed to viruses, malware and intrusions.
2. Lock down your computer. Never leave your laptop or desktop computer on when you step away from your desk. Make sure they are set to lock within a very short period of time.
3. Be cautious when online. Don't open websites that appear suspicious, and never open a link or advertisement from an email unless you know who it's from. Do the same on social media sites like Facebook, LinkedIn or Twitter. These links and ads could contain malicious viruses.
4. Watch out for phishing scams on email. Phishing attacks are increasingly sophisticated and becoming more difficult to spot. You must be vigilant:
    - Hover over links to see the actual email address of the sender. Don't open attachments unless you're 100 percent sure of where they came from.
    - Beware of banner ads, especially those offering gifts that are too good to be true.
    - Never share personal information from a link clicked in an email. Stick to the phone or a website that you proactively navigated to over a secure connection.
    - Be cautious when receiving a non-personalized email from an individual you only know slightly, and that asks you to open an attachment or share information.
    - If you have the slightest question about whether activity is suspicious or not, report it to your IT service provider or technical team.
    - Bump up spam filters to their max settings. Yes, you will likely miss a few emails from friendly sources, but you're more likely to block criminal activity with tighter security settings.
5. Use strong passwords and user names. The difference between a good password, and a weak one is the major determining factor in protecting your online information. The best practice in terms of password security is to NOT use words that can be found in the dictionary. Use long codes with 10 distinct characters or more, that also contain symbols and other special characters to increase complexity. The same goes for usernames — avoid common ones such as "User1." Consider using a password manager like LastPass or DashLane.
6. Always use a PIN or password to open your computer devices including your phone and tablet. It's important to password protect these devices to keep others from accessing your data if they're lost or stolen. Employing mobile device management software is one way to secure confidential bank information on mobile devices.

For a printable and downloadable cybersecurity checklist that you can give to your employees, go to www.jmark.com/MIBACyberSecurity; and, as always, please reach out to me at tnielsen@jmark.com if I can answer any questions about technology in banking. ■

Todd Nielsen is an executive, writer, & speaker. He currently leads strategy execution initiatives as Chief Strategy Officer of JMARK Business Solutions, Inc. His almost 20 years of diverse experience - dealing with rapidly changing markets and technologies has made him a strong leader and business advisor.