BAC
BAC Community Bank

# Cash Management Online Banking

## Customer Information Security Self Risk Assessment & Controls Evaluation

Industry wide, businesses are becoming increasingly susceptible to computer breaches. The attackers use malicious software to steal User ID and Password information for the company Cash Management Online Banking system and/or break into other software systems at the company to change data before it is sent to the Bank. The attackers then are able to attempt large ACH or Wire transfers from the business account, usually very quickly before the company has time to notice a problem.

This questionnaire is a tool for businesses to use in performing an Information Security Self-Assessment and Controls Evaluation. Upon completion, businesses should address any questions answered with “no”, as these would be considered a security deficiency. Businesses must remember that they are responsible for the security of their environment and any transactions that occur using their Cash Management Online Banking credentials. **This form does not need to be returned to BAC Community Bank, it is for your own business controls evaluation.**

| **Question** | **Yes** | **No** |
|---|---|---|
| 1. Has an employee been appointed to manage the protection of sensitive information? | | |
| Has this person received training in information security? | | |
| Has the organization allocated budget and resources for information security? | | |
| 2. Have information security policies and standards been developed and implemented? | | |
| Do employees receive training on information security policies and standards initially upon hire and regularly thereafter? | | |
| Are information security policies and standards periodically updated to contain controls to combat the latest attack techniques? | | |
| 3. Have response procedures been established should a breach, virus infection, or other information security event occur? | | |
| 4. Are servers and workstations backed up at least on a weekly basis? | | |
| Are backup files stored offsite? | | |
| Are backup files encrypted and password protected? | | |
| Are backup files tested on a periodic basis to ensure that data can be restored? | | |
| 5. Are third parties such as contractors and vendors who connect to your systems required to comply with your information security policies and standards? | | |
| 6. Have anti-malware (anti-virus) controls been implemented on all systems? | | |
| Do all systems have both anti-virus and anti-spyware software installed? | | |
| Does your organization’s email server have anti-malware software installed specifically for email? | | |
| Are anti-malware signature files updated at least once every day? | | |
| Are periodic audits performed to ensure that anti-malware software is being updated as intended? | | |
| Are appropriate IT/security personnel notified immediately if an infection is detected on any system? | | |

| | | |
|---|---|---|
| 7. Does the organization protect its perimeter network with a firewall? | | |
| Has the firewall been configured to restrict outbound traffic (minimum necessary services) as well as inbound traffic? | | |
| Are firewall logs and server logs regularly monitored for intrusion attempts? | | |
| Are appropriate personnel notified in real-time if a high-risk threat is detected? | | |
| Does the firewall (or other system) block malicious web traffic? | | |
| Is web browsing restricted by policy or technical constraint to only business appropriate sites? | | |

| | | |
|---|---|---|
| 8. Does the organization have a patch management program in place to ensure that critical security patches are applied to all systems within 7-10 days of release? | | |
| Does the patch management program address patches with 3rd party applications such as Adobe Acrobat Reader and Flash, Backup Exec, and Symantec Anti-virus? | | |
| Does the patch management program address updates to other systems such as networking devices (routers and switches)? | | |

| | | |
|---|---|---|
| 9. Does the organization control remote access and wireless technology? | | |
| Is remote access to sensitive information encrypted? | | |
| Is remote connectivity (through the organization's VPN) encrypted? | | |
| Are wireless connections protected with WPA2 encryption? | | |
| Are WPA2 passwords changed at least quarterly? | | |

| | | |
|---|---|---|
| 10. Does the organization protect laptop computers? | | |
| Are laptop hard drives encrypted? | | |
| Are policies in place specifically addressing the unique security requirements of laptop computers such as risk of theft and the use of public wireless hotspots? | | |
| Are wireless network adapters automatically disabled when portable computers are connected to the wired network? | | |

| | | |
|---|---|---|
| 11. Does the organization maintain a password policy which requires? | | |
| A minimum of 8 characters? | | |
| The use of upper and lower case letters, numbers, and special characters? | | |
| Passwords to be changed at least every 90 days? | | |
| That passwords not by cyclical, reused, or in any way related to the user? | | |

| | | |
|---|---|---|
| 12. Has the organization had an independent security assessment performed to validate controls are effective? | | |