Corporate Account Takeover (CATO) Risk Assessment

As a business, you want to be sure you have a strong process in place for monitoring and managing who has access to your Business Resource Manager services and how the information is handled. Use this Risk Assessment to make sure you have the necessary controls in place.

For each question below, select the answer that best represents your environment. You'll see a number after each possible answer. These numbers will be used in the section called Risk Rating.

At the end of the Risk Assessment you'll find a section called "CATO Vulnerability-Best Answers & Tips". Use this to evaluate your current environment and to make to make any necessary changes, so your Business Resource Manager process remains safe, secure and effective.

Date Risk Assessment Conducted: _____

Risk Assessment Completed By: _____

Please fax or email the completed document to Prevail Bank at 715-748-2679 or brm@prevail.bank.

Personnel Security

1) Are employees required to sign and Acceptable Use Policy (AUP)?
   a. Yes, at least annually or more frequently as needed (1)
   b. Yes, but only at hire (2)
   c. No (5)

2) Does each employee using Business Resource Manager go through security awareness training?
   a. Yes, at least annually or more frequently as needed (1)
   b. Yes, but only at hire (2)
   c. No (5)

3) Do you run background checks on employees prior to hire?
   a. Yes, for all employees (1)
   b. Yes, but only based on position (2)
   c. No (5)

Computer System Security

4) Do your computer systems have up-to-date antivirus software?
   a. Yes, all systems (1)
   b. Yes, but only critical systems (3)
   c. No (5)

5) Is there a process in place to ensure software updates and patches are applied (i.e., Microsoft, Web Browser, Adobe Products, etc.)?
   a. Yes, a formal process where updates are applied at least monthly (1)
   b. Yes, not informally as needed (3)
   c. No (5)

6) Do users run as local administrators on their computer systems?
   a. No (1)
   b. Only those that require it (3)
   c. Yes (5)

7) Is a firewall in place to protect the network?
   a. Yes (1)
   b. No (15)

8) Do you have an Intrusion Detection/Prevention System (IDS/IPS) in place to monitor and protect the network?
   a. Yes (1)
   b. No (3)

9) Is internet content filtering being used?
   a. Yes, internet traffic on the system used for "high risk" internet banking activities is completely restricted to only sites specifically needed for business functions (1)
   b. Yes, we have internet content filtering (2)
   c. No (5)

10) Is email SPAM filtering being used?
   a. Yes (1)
   b. No (5)

11) Are users of Business Resource Manager trained to manually lock their workstations when they leave them?
   a. Yes, and the system are set to auto-lock after a period of inactivity (1)
   b. Yes, but it is only manually (2)
   c. No (5)

12) Is wireless technology used on the network with Business Resource Manager?

a. No (1)
b. Yes, but wireless traffic uses industry approved encryption (i.e., WPA, etc.) (1)
c. Yes, but wireless uses WEP encryption (2)
d. Yes, and wireless traffic is not encrypted (15)

Physical Security

13) Are critical systems (including systems used to access Business Resource Manager) located in a secure area?

a. Yes, behind a locked door (1)
b. Yes, in a restricted area (2)
c. No, in a public area (5)

14) How are passwords protected?

d. Passwords are securely stored (i.e., Excel file) (1)
e. Passwords are written on paper or sticky notes and placed by the computer (15)

15) Do you control unauthorized physical access to protect your computers?

f. Yes (1)
g. No (3)

16) Do you create back-up copies of information?

h. Yes (1)
i. No (3)

Risk Rating

Once you have completed the questionnaire, add up the numbers next to each answer you have selected. Using your total, note where you fall on the chart below:

Overall Risk Rating

0-17	Low
18-27	Medium
28-37	High
Over 38	Extreme

CATO Vulnerability – Best Answers & Tips:

Compare your answers to the Business Resource Manager Risk Assessment to the "Best Answers" listed below. Tips are also provided to help you protect your systems and information.

Personnel Security

1. An Acceptable Use Policy (AUP) details the permitted user activities and consequences of noncompliance. Examples of elements included in an AUP are: purpose and scope of network activity; devices that can be used to access the network, bans on attempts to break into accounts, crack passwords, circumvent controls or distrust services; expected user behavior; and consequences of noncompliance.
2. Security Awareness Training (SAT) for Business Resource Manager users, at a minimum, should include a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc. Watch our Identity Theft tutorial on our website for further detail.
3. Companies should have plans in place to verify job application information on all new employees. The sensitivity of a particular position or job function may warrant additional background and credit checks. After employment, companies should remain alert to changes in employees' circumstances that could increase incentives for abuse or fraud.

Computer System Security

4. Companies should active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.
5. Update your software frequently to ensure you have the latest security patches. This includes a computer's operating system and other installed software (i.e., Web Browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.). In many cases, it is best to automate software updates when the software supports it.
6. Limit local Administrator privileges on computer systems where possible.
7. Use firewalls on your local network to add another layer of protection for all the devices that connect through the firewall (i.e., PCs, Smart Phones, and Tablets).
8. Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.

9. Business Resource Manager activities are completely restricted to only sites specifically needed for business functions. Filter web traffic to restrict potentially harmful or unwanted internet sites from being accessed by computer systems. For "high risk" systems, it is best to limit internet sites to only those business sites that are required.
10. Implementing email SPAM filtering will help eliminate potentially harmful or unwanted emails from making it to end users' inboxes.
11. Systems should be locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.
12. Wireless networks are considered public networks because they use radio waves to communicate. Radio waves are not confined to specific areas and are easily intercepted by unauthorized individuals. Therefore, if wireless is used, security controls such as encryption authentication, and segregation are necessary to ensure confidentiality and integrity.

Physical Security

13. Physically secure critical systems to only allow access to approved employees.
14. Passwords should never be left out for unauthorized individuals to gain access.
15. Identify and challenge all third parties entering the organization's sensitive areas, lock all secondary entrances, and consider both the placement of paper documents and position of computer monitors to protect information.
16. Back up all critical information at least once a week, test backups monthly for successful recoverability, and rotate backups to an off-site location.