Cybersecurity Risk Assessment

As a business, it is very important to have strong processes and controls in place for monitoring and managing access to your computer network, workstations, and online account services. This Risk Assessment can help you understand what controls you have in place and which controls you should consider strengthening to improve security.

To determine your Risk Rating, answer each question below. It is important to answer each question by selecting the answer that best matches your organizations current business practice.

At the end of the Risk Assessment, we can evaluate your organization's Risk Rating. This will help to determine what controls should be strengthened.

Personnel Security:

1) Do you have an Acceptable Use Policy and are employees required to sign this policy?

a) **Yes, and employees sign it annually or as needed (1)**
b) **Yes, but only at hire (2)**
c) **No (5)**

2) Does each employee using a workstation with access to sensitive data 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) Is the Anti-Virus software up-to-date on the network and each workstation?

a) **Yes, all systems (1)**
b) **Yes, but only critical systems (3)**
c) **No (5)**

5) Do you use only manufacturer supported hardware and software AND are there procedures in place for software updates and patches?

a) **Yes, yes there is a formal process where updates/patches are applied at least monthly (1)**
b) **Yes, no updates/patches are informally applied 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" 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) Do you use email SPAM filtering?

a) **Yes (1)**
b) **No (5)**

11) Do users manually lock their workstations when the workstation is unattended?

a) **Yes, and inactivity timers will lock systems after a period of inactivity (1)**
b) **Yes, but it is only manually (2)**
c) **No (5)**

12) Do you use any wireless technology in the office for business purposes?

a) **No (1)**
b) **Yes, but wireless traffic uses industry standard encryption (Wi-Fi Protected Access (WPA)) (1)**
c) **Yes, but wireless traffic uses Wired Equivalent Privacy (WEP) encryption (3)**
d) **Yes, and wireless traffic is not encrypted (15)**

Physical Security:

13) Are critical systems 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?

a) **Passwords are never shared or stored written down (1)**
b) **Passwords are never shared and are securely stored in a password protected file (3)**
c) **Passwords are shared, but never written down (10)**
d) **Passwords are written on paper or sticky notes and placed by the computer (15)**

15) Do you keep a log of vendors/visitors that access restricted areas?

a) **Yes (1)**
b) **No (3)**

16) Is the network (or computers) routinely backed-up?

a) **Yes (1)**
b) **No (5)**

Determining your Risk Rating:

Once all questions have been answered, add up the numbers next to each answer. Using the total, note where the total falls on the chart below:

Risk Rating Scoring

0 – 17	**Low**
17 – 27	**Medium**
28 – 37	**High**

38 or above represents Extreme Risk

If the score is **"Low"**, then things are already being done to protect your company, employees, and customers. Even with a **"Low"** score, it's important to be diligent and maintain your security program, please see **"What everyone should do on an annual basis"** in the Best Practices section below.

A **"Medium"** score indicates some of the recommended things are being done to protect your company, employees, and customers, but with a little effort it would be simple to strengthen the controls and lower the risk score. When time permits, go back and review the questions and answers. Find those questions with high point value answers and review the **"Best Practices & Tips"** sections for some ideas on how control may be improved.

If the score is "**High"** or "**Extreme Risk",** action is required to ensure you network, workstations, and sensitive data is protected. It is critical that improvements are made in a timely manner. Start by identifying those questions with the highest point value answers, reviewing some of the **"Best Practices & Tips"**, and putting together a game plan on strengthening the weak areas.

Best Practices & Tips:

What everyone should do on an Annual Basis: Technology changes quickly, unfortunately so do the threats associated with quick changing technology. This is why it is important to make sure security controls are evaluated annually to ensure the controls are still relevant. It is also important to stay educated on security awareness, regularly provide employee training, annually review insurance policies to ensure proper coverage, and keep hardware, software, and anti-virus protection up-to-date.

Personnel Security:

1) **An Acceptable Use Policy** will detail what acceptable and approved activities are permitted in the workplace and what the consequences are for noncompliance. For example, "employees may access the internet for work related purposes only", may be something included in an **Acceptable Use Policy**. Other elements to include could be definition of devices that could be used to access the network, business purpose of network activity, clean desk policy, password policy, attempting to circumvent controls, and the consequences for noncompliance.

2) **Security Awareness Training** should be provided to all employees at time of hire and on an annual basis. As technology changes, so do the threats associated with the changing technology. Training should include acceptable passwords, clean desk (locking computers and not leaving unattended sensitive data lying out on a desk), Social Engineering, and a review of the **Acceptable Use Policy**.

3) At a minimum, background checks should be performed on any employee that has access to sensitive data. The more access an employee has, the further the background check should progress. Also, it is wise to remain alert to changes in employees' circumstances that could increase the likelihood for fraud or abuse.

Computer Security:

4) For full protection **Anti-Virus** must be running and up-to-date. Most **Anti-Virus** software relies on a dictionary of the latest viruses. If the **Anti-Virus** software is not frequently updated, the latest virus threats will not be included in the dictionary.
    a) Anti-Virus updates should be performed monthly OR as recommended by the manufacturer.
    b) Anti-Virus scans should be run:
        i) Regularly
        ii) Immediately if a virus is suspected.

5) Only use manufacturer supported hardware/software and ensure everything is up-to-date. Manufacturers frequently release updates, sometimes referred to as "patches", that are intended to fix an unanticipated problem. These updates should be reviewed, and if necessary, immediately installed to ensure you are protected.

6) Administrative Privileges should be limited whenever possible.

7) After **Employee Education,** Firewalls are the next best line of defense. Firewalls, if configured correctly, can block unwanted traffic to and from your network.

8) Intrusion Detection System/Intrusion Prevention System (IDS/IPS) are used to monitor network/internet traffic and may report and/or respond to potential attacks.

9) Consider filtering web traffic to restrict harmful or unwanted internet site access, especially on computers used to perform "High Risk" transactions.

10) SPAM Filters may help eliminate potentially harmful or unwanted emails from making it to an end users' email inbox. This is especially important to aide in combating Social Engineering Scams such as Phishing.

11) To prevent unauthorized access by both internal and external threats, all systems should be locked when not in use. Users should lock systems when they are away from their desk AND inactivity timers should be in place to ensure systems are locked down if the user forgets to lock the system down.

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) Critical systems should be restricted to authorized employees with a "business need" for access. If an employee does not need access to critical systems, their level of access should be set appropriately to restrict them.

14) Passwords are one of your best lines of defenses; they **MUST be secured and NEVER shared**. Here are a number of tips to consider with regards to passwords and password strength:
    - Use strong passwords and change passwords frequently, especially if you believe someone else may know your password.
    - DO NOT share passwords.
    - Make your password unique.
    - DO NOT write down passwords.
    - Use a combination of UPPER CASE and lower case letters with numbers (1234567890) and, if possible, special characters (!@#$%^&*).
    - Avoid "high profile" passwords like date of birth, spouse's name, pet's name, favorite movie, etc..
    - Make it something you can remember.

15) It is important to keep a record of who has accessed restricted areas and/or critical systems.

16) One of the most important steps you can take is to prepare well in advance of a problem by periodically backing up computers/network. Unfortunately, far too often the only option available on a compromised computer is wiping the system hard drive and reinstalling the operating system or purchasing a new computer. Either way, a viable backup is needed to recover data.