

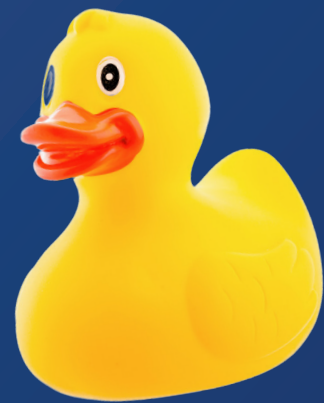


**Commonwealth Sentinel**  
**CYBER SECURITY**

**2024**

**Baseline Risk Assessment:  
How Secure Is Your Data?**

*Find out if you are  
a sitting duck in  
12 short questions!*



**CommonwealthSentinel.com**

June 1, 2024



**Commonwealth  
Sentinel**  
CYBER SECURITY

Dear Friend,

The first step in effective cyber security is risk assessment. How can you keep your organization safe from cyber criminals if you don't know all the potential pitfalls?

If you think your organization is too small to be a target, think again. Over 40% of cyber attacks go after small organizations. On average, that kind of attack will cost you \$25,000.

Be proactive and start your cyber security planning by taking this short risk assessment. Anyone in your organization should be able to answer these questions. If they can't, you know there is a problem.

I've spent twenty years working for the U.S. Navy in security and intelligence. These days I use my expertise to help local governments, small businesses, and non-profits because I firmly believe that every organization, regardless of size, deserves good cyber security!

**It is easier and less expensive to protect your organization than it is to recover from a cyber attack!**

I hope you will find this information useful. If you have any questions, please don't hesitate to contact me!

Best,

Sheri Donahue  
CEO/ Cyber Security Evangelist

**P.S.** Feel free to reach me by cell at (502) 649-3102

**Commonwealth Sentinel**  
CYBER SECURITY

1230 US Hwy 127 South  
Suite #5  
Frankfort KY 40601  
Phone: (502) 320-9885

Info@CommonwealthSentinel.com  
CommonwealthSentinel.com



@cwealthsentinel



# Commonwealth Sentinel's Baseline Risk Assessment: How Secure Is Your Data?

---

The following baseline assessment allows you to quickly evaluate your organization's cyber security risk.

**Anyone within an organization should be able to answer these basic questions.** These questions will help you to understand your risk profile and assess the security controls in place.

1. Are backups maintained on three different storage types, kept in at least 2 different locations and 1 kept off-premises?

- Yes
- No
- I don't know

2. The modern office has changed significantly over the past few years. Many employees are working at home. Do you have different protocols for protecting remote workers than those working in the office?

- Yes
- No
- I don't know

3. As the number of remote workers increased, so did cloud storage and tools. Today over 70% of organizations use cloud storage. Do you store data in the cloud (GoogleDrive, Box, Dropbox, or OneDrive)?

- Yes
- No
- I don't know

## Simple Risk Assessment Continued:

4. As cloud storage and tools increased, hackers began attacking remote systems more and more. The easiest way in? Passwords. Do you use multifactor authentication when accessing email?

- Yes
- No
- I don't know

5. Another way hackers access cloud systems is by phishing their way onto people's computers and then using their access to get to the data in the cloud. Do you receive simulated phishing training?

- Yes
- No
- I don't know

6. Because users became the easy way into the network, many organizations implemented special cyber security training. Have you received cyber security training in the last 90 days?

- Yes
- No
- I don't know

7. Sometimes hackers get into people's e-mail. This allows them to look through all of the messages for personal information. Do you prohibit sending personal information by e-mail (Social Security Number, Date of Birth, or Credit Card Information)?

- Yes
- No
- I don't know

8. Users often store passwords in locations that hackers can easily access. These locations make it easy for the user AND the hacker. Do you prohibit storing passwords in Word, Excel, Outlook, and in your Smart Phone?

- Yes
- No
- I don't know

9. Do you use passwords longer than 8 characters that include uppercase, lowercase, numbers, and punctuation?

- Yes
- No
- I don't know

10. People often reuse passwords. Shocking, right? Well, hackers understand this, and they've created tools to guess simple passwords. Does every user have unique usernames and passwords for their devices and programs?

- Yes
- No
- I don't know

11. Are employees given "least privilege access"? That is, do they have access to only those programs, networks, and data that they need to do their jobs?

- Yes
- No
- I don't know

12. Are employees/visitors prohibited from accessing the organization's network with their personal devices (e.g., iPhones, Laptops, Apple Watch)?

- Yes
- No
- I don't know

**Go to page 5 for the Answer Key ⇨**

## **ASSESSMENT ANSWER KEY:**

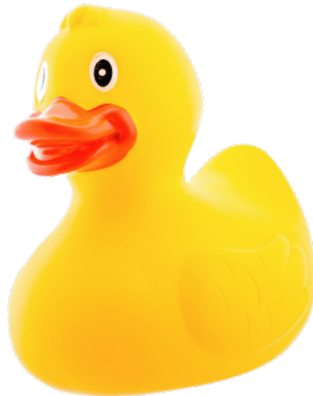
If you answer **Yes** to 0 of 12 ⇒ You are a cyber security Dead Duck

If you answer **Yes** to 3 of 12 ⇒ You are a cyber security Sitting Duck

If you answer **Yes** to 6 of 12 ⇒ You are a cyber security Ugly Duckling

If you answer **Yes** to 9 of 12 ⇒ You are a cyber security Duck And Cover

If you answer **Yes** to 12 of 12 ⇒ You are a cyber security Eagle



Okay, all joking aside, unless everyone at your organization is 12 for 12 **everyday**, you are at risk. If you are interested in a more in-depth assessment, use code **GOODDUCK24** and receive Level 2 Cyber Security Assessment\* for \$1,500, regularly priced at \$2,000.

Call Commonwealth Sentinel at (502) 320-9885 to get started today!

\***Level 2 Cyber Security Assessment** will provide an overview of your strengths and vulnerabilities, a dark web scan, and a road map of how to achieve cyber security maturity.