HODGSON
CONSULTING & SOLUTIONS

Security Risk Assessment

FREQUENTLY ASKED QUESTIONS

1. How exactly does this Cyber Security Assessment work?

The assessment has 4 parts.

The first part consists of a remote session where we conduct a brief and easy survey to complete. The first survey is for you, the CEO, office manager, or other executive, to complete. Don't worry, it's mostly "Yes/No" or multiple-choice answers that won't take very long to complete. It's also NON-technical, so you should be able to complete it easily.

The second survey is for the person who manages your IT. We will send the survey for completion by the person who manages your IT. If you don't have someone who manages your IT, or if you don't want them to get involved or know about this assessment, we can help you through it.

The third part is a NIST Assessment and technical audit conducted by Hodgson Consulting & Solution's technician. This assessment and audit is done using a well-known network and cyber security assessment software that will scan your network for vulnerabilities, poor configuration, slow performance, and other hidden problems that would affect security and performance. We'll also do a Dark Web scan to reveal if any of your login credentials, e-mail addresses, and passwords are being sold via cybercrime rings, so you can change those passwords and be hyper-vigilant for phishing scams. When done, this scan will give you a Risk Score and Management Plan to reveal where your network is exposed and what needs to be patched, protected, or updated to better secure your systems. We will need to work with someone on your team to get the diagnostic software set up on your systems. There will be NO disruption to your network, NO slowness, NO tracking, and NO changes. Once this diagnostic tool runs, it will close and exit without leaving any trace.

The fourth step is to meet with you and your executive team to go over the Report Of Findings and Action Plan. This is NOT e-mailed due to the confidentiality of the information shared. During this meeting, we'll show you what we discovered and deliver all the reports generated. We will also make recommendations and discuss options for how we might help you remedy any problems discovered. You are under NO OBLIGATION to do or buy anything.

2. How much time will this take to complete?

The time for each assessment and audit will vary based on the size of the organization, the number of locations, and the complexity of your network.

3. Are you going to be accessing, viewing, or copying our files and data?

Absolutely NOT! No information will be taken, copied, or viewed by anyone. This is STRICTLY confidential, and we will provide you with a signed confidentiality agreement before doing the assessment to alleviate any concerns you may have.

4. I KNOW things are screwed up, and I'm embarrassed to have someone review us. Is this truly confidential?

Let us assure you that **no one** gets a "perfect" score, and every assessment we've done has uncovered problems, security shortfalls, and a host of things that need to be addressed. Let me personally assure you that WE WILL NEVER BLAME YOU OR MAKE YOU FEEL EMBARRASSED. It's absolutely NOT your fault that cybercriminals have become as sophisticated and aggressive as they have been. You shouldn't have to do this – but the reality is if you don't, you will get compromised. At that point, employees, clients, competitors, and the federal government will be on the warpath to blame you. By doing this assessment and then addressing any security issues found, you are demonstrating a "good faith" effort in attempting to protect their data.

Further, if you are trusting an outsourced IT company, you shouldn't feel bad or embarrassed to have their work checked. Fresh eyes always see things we cannot for being too close. And finally, everything we discover and discuss is completely confidential. Our goal is to protect hardworking business owners like you from cyberscum robbing unsuspecting businesses blind or severely crippling, or harming them.

5. Should I have my current IT person/company involved? What if I DON'T want them to know you're doing this?

It's entirely up to you whether or not we work with your current IT person or company. We are here to work for YOU and sit on YOUR side of the desk, so we can work with them or keep this process confidential.

However, keep in mind that some IT companies (outsourced) or people (employees) may feel threatened and retaliate. They might try to cover up their mistakes or do things to prevent the assessment from being completed, such as refusing to give you your network password, refusing to complete the surveys, or falsifying information (saying they have it covered, invalidating the reports, etc.).

To that end, if you DO want us to work with them, we need your full support and the ability to alert you to anything that is blocking us or preventing us from honestly and candidly conducting the assessment. Again, we are sitting on your side of the desk to shine a spotlight on where you're being underserved or where you are exposed to threats that can have a significant, negative impact on your organization.

Some people want us to conduct this assessment without their IT person or company knowing. In some cases, they are outsourcing their support, and are not happy with the

service they are getting, and feel there are things NOT being done that should be done. In that case, we can conduct this completely under the radar.

6. What if I don't know the answer to a question on the survey?

It's perfectly normal and okay not to know all the answers. Most people don't. That's why all questions have an ***Unsure*** option and a ***Notes*** field for you to add any information to help make the answer clearer.

7. Why do you need to scan my network?

Any thorough Cybersecurity Assessment requires a technical scan to identify any vulnerabilities that may exist in your environment, which is why you want this assessment done. This scan is non-invasive and uses an industry-standard tool. Nothing is installed, and nothing is left behind after the scan is complete.

8. How long after you finish the assessment will we get the results?

Once we have completed the survey and scan, we'll need 4-5 days to evaluate the results and produce the report. We'll schedule a meeting to go over our Report Of Findings and deliver a Recommended Action Plan. This is always done via a private one-on-one meeting and never e-mailed. We can do this via a Zoom or Microsoft Teams meeting, or in person.

9. If you find problems, how will we know what to do about them?

Our report will include recommendations on what you can do to mitigate any problems we've uncovered. In most cases, we can assist you with remediation; however, you are not obligated to hire us or buy anything. If you choose, you can take what you find back to your current IT person or company to resolve.

10. I don't have a server in my office; is this assessment still worth doing?

ABSOLUTELY! In fact, organizations without a server are at a higher risk of becoming a victim of a cyberattack, particularly if the phones, laptops, and tablets are used by remote employees who might also use those devices for personal use.

11. Most of our "stuff is in the cloud. Do I need to worry about doing this type of assessment?

Yes, cloud applications are just as insecure as those installed in your office. In fact, because you have more control over the security of your office, they may be less secure. Further, the DEVICES connected to your cloud applications must be scanned for vulnerabilities, particularly if the people using them may also use them for personal e-mails, web surfing, etc.

12. Will you fix any security issues you find as part of this assessment?

We can resolve the problems we find, but they are not included with the assessment. The assessment is used to identify any vulnerabilities or inadequacies in your security that may lead to a cyberattack. If you need help implementing the recommendations, we'll be happy to discuss how we can help when we deliver the Report Of Findings.

13. Do we have any obligation to use your firm to implement your recommendations?

No. The assessment and its recommendations are yours to keep and do with as you feel would be in the best interests of your organization. We certainly can help implement them, but you are under no obligation to hire us or buy anything.

14. Is the assessment industry-specific and/or aligned with any specific compliance requirements?

The NIST Cybersecurity Framework is for any private sector or critical infrastructure business. Adhering to the NIST CSF can help you meet some of the requirements of other Regulatory Compliance, such as PCI DSS, GDRP, HIPAA, NYDFS, and ISO.

15. Will you alert me to anything critical that you find?

ABSOLUTELY! If at any point in the assessment or audit we come across findings that we feel present an immediate security risk to your organization, we will communicate it to you immediately.

HODGSON
CONSULTING & SOLUTIONS

1110 W. Lake Cook Rd, Suite 235, Buffalo Grove, IL 60089
(847) 906-5005 | www.hodgsonconsulting.com