CYBERSECURITY WORKBOOK

LIGHTHOUSE
TECHNOLOGY SERVICES

ABOUT LIGHTHOUSE

Lighthouse Technology Services connects companies in need of technology talent with the right technologists for their businesses, and we've been at it since 2004.

Headquartered in beautiful Buffalo, NY, on the shores of the Great Lakes, and in the midst of Niagara Falls, we serve as a guide to companies looking for technology help, and as a beacon to talented professionals looking for a partner on their technology work journey.

CONTENTS

TECHNOLOGY INVENTORY & ASSET MAP

1. Do you have an accurate, up to date inventory of all your company technology?

2. Do you know how many laptops and desktops you have, and know which are assigned to what employees?

3. Do you have a map document of where all your technology is, and how it's connected within your building(s)?

4. Do you have inventory of all employee devices being used by company employees for work purposes and which are accessing your network?

5. Do you have access to technology tools to help you construct a technology inventory and map, or do you/would you have to build these manually?

6. If you do have a technology inventory and map, how frequently is it updated?

IT RISK ASSESSMENT

1. Have you performed an IT Risk Assessment?

2. If you have, when was the last IT Risk Assessment conducted?

3. What risks have been identified that need to be mitigated?

4. What is your strategy for future cyber risk assessments? How regularly do you plan to conduct additional assessments?

5. How are you identifying cyber risks in your current technology and network setup? With your current company processes and protocols?

6. Are you firmly aware of and in compliance with all current cyber regulations your company needs to follow (PCI, HIPAA, SOC2, etc.)?

7. What assets and entry points does the company have that need protection?

8. How is the company securing its technology?

9. How is the company detecting problems?

10. What is the company doing to create a healthy cybersecurity culture?

NETWORKS

1. List the brand, date of installation, and date of last update for each:

- Firewall

- Anti-Virus

- Malware Protection

2. How have you tested the security of your network?

3. How often do you rotate your WiFi password?

4. Do you have a separate guest network setup for your company WiFi?

5. Hardware/Software Policy

6. Describe your policy and procedures for updating hardware and software.

7. How often do you patch?

8. How do you ensure all employee accessible software and hardware is patched?

9. How do you ensure BYOD devices used to access company software or the company network are patched and updated with the latest security patches?

10. How do you track the age of company used hardware?

11. What is the company's policy on refreshing technology?

12. What is the company's technology on recycling, destroying, or decommissioning old technology that's no longer in use?

PASSWORD PROTOCOLS

1. What is the company's current policy on establishing, using, and changing passwords?

2. Do you use a password generator?

3. Do you use an encrypted password manager?

4. How often do you require password changes?

5. How is your team notified that it is time for them to make required password changes?

6. Are employees required to create unique passwords each time they update?

7. What is your process for access if an employee is locked out or can't remember their password?

8. Can you verify all company and employee passwords are strong? How?

9. Do you have documented protocols and policies pertaining to expected password behavior?

10. Do you have the ability to identify any company usernames or passwords that may be available on the dark web?

11. Do you use a password manager application?

12. Do you use password encryption software?

13. In what ways have you limited access to password restricted systems?

EMAIL SECURITY

1. What spam and phishing protection tools have been put in place?

2. How have you educated employees on how to identify a malicious email?

SOFTWARE ACCESS

1. List all company software currently in use:

2. Describe protocols for limiting access to company software for existing users.

CYBER INSURANCE

1. Do you have cyber insurance?

2. Do you have a copy of your cyber insurance policy?

3. What exclusion clauses are listed in your cyber insurance policy?

4. Are you using encryption software?

5. What software do you use for Multi-Factor Authentication (MFA)?

6. What software do you use for Virtual Private Network (VPN)?

7. What software do you use for data backups?

8. Do you have documented processes for cyber incident response?

9. Do you require Certificates of Insurance (COI) from vendors and suppliers, as well as their cyber incident response plans?

CONFIGURATION THREATS & VULNERABILITY SCANS

1. When was the last date a vulnerability scan was performed to inventory company and employee device configuration settings?

2. What insecurities were identified in company systems and software?

FIREWALLS

1. List all brands of firewalls currently being used and the date(s) in which each was installed and last updated.

2. What filtering settings or filtering setting policies are in place for your firewall(s)?

3. What web activity are you looking to prevent employees from accessing on company devices?

4. Are your firewall settings adjusted to ensure this type of activity is prevented?

5. Do employees complain about any restrictions of web activity/not able to access the web in ways they'd like to?

6. Do employees complain of web activity or emails getting through to their devices that would like to prevent from getting through?

7. List the number of people who have administrative control over, and ability to change, the company's firewall settings.

8. Does the company have any sensitive data that needs to be accessed that might be better accessed through a VPN and not open to standard web access?

MULTI-FACTOR AUTHENTICATION (MFA)

1. Is Multi-Factor Authentication in place at the company?

2. From the list in the Software Access section, list which of those programs have MFA enabled.

3. How often are employees asked to verify or update their contact methods for MFA?

4. Is there software that the company uses which holds sensitive company, client, or employee data that does not have MFA activated on it?

5. Are you concerned some employees have weak passwords as login access to company software?

PROTECTING THE SUPPLY CHAIN

1. What is your current policy on cybersecurity requirements of your vendors and suppliers?

2. Do any vendors or suppliers have access to/or do you share any company used software, hardware, or systems?

3. Do you require a Certificate of Insurance (COI) from your vendors with proof of cyber liability insurance?

4. If so, how often do you request an updated COI?

5. What process is in place for vetting vendors' and suppliers' cybersecurity hygiene?

6. What requirements does your company have for cybersecurity hygiene of vendors and suppliers?

7. What steps are taken for limiting access to company software and applications for vendors, suppliers, and third parties?

8. When was the last IT audit performed to identify outdated IT systems and protocols that could be removed or replaced to reduce cyber-attack risk?

9. When was the last IT audit performed to identify unapproved apps or technology that operate outside company policies, protocols, and standard operating procedures?

10. Does the company have patch management and software update processes in place to stay current on security updates for all company hardware and software?

11. Who at the company is responsible for staying current with cybersecurity news and trends so as to be proactive in what to cyber concerns watch out for?

ANTIVIRUS & DETECTION RESPONSE

1. List the brand name of the antivirus tool(s) the company current has in place and their date of installation and last update:

2. Do you have endpoint detection and response (EDR) software in place?

3. Do you have a managed detection and response software in place?

4. If so, list the brand name of the EDR tool(s) the company current has in place and their date of installation and last update.

BUSINESS CONTINUITY & DISASTER RECOVERY

1. Do you have a documented business continuity plan (BCP)?

2. When was the last time the BCP was updated?

3. When was the last time the BCP was tested?

4. What are the most probable concerns that would cause the company to use the BCP?

5. Do you have a documented disaster recovery plan (DRP)?

6. When was the last time the DRP was updated?

7. When was the last time the DRP was tested?

8. Which company stakeholders were involved in the creation and approval of these plans?

9. When was the last time the plans were updated? How frequently do you plan to review them?

10. What are the main concerns that are the most probable that cause the company would have to use the DRP?

11. How have you tested your existing plans for assurance?

12. Do you feel adequately protected for such a disaster or disruption?

DATA BACKUPS

1. List the name of the backup solution you currently have in place, the amount of data that can be backed up, and the date the solution was implemented:

2. Do you have a multi-backup solution in place?

3. Are your backup solutions on premise, offsite, in the cloud, or a combination of these?

4. Are automated backups being used?

5. Who is responsible for monitoring automated backups?

6. What is the scheduling and process for backing up data?

7. Describe your process and frequency for checking the integrity of your automated backup solution.

8. When was the last time you checked the integrity of your backup solution?

9. What redundancies are in place in the case one backup fails?

10. When was the last time your backup solution was tested or audited? How often do you test these?

11. When was the last time your backup solution settings were updated, configured, or adjusted to match any backup requirement changes for company data?

TRAINING & EDUCATION

1. Describe the company’s existing cybersecurity training policy.

2. How do you safely test your employee’s application of cyber security trainings and good cybersecurity hygiene?

3. What training tools and practices do you currently use to help employees learn best cybersecurity practices and good behavior?

OUR CORE VALUES

In our cybersecurity work, and in all that we do, the Lighthouse team is guided by three core values.

The first core value is to **Follow the Golden Rule,** and treat others the way you would want to be treated.

The level of service we provide is the same we would hope for in return. We invest the time that's necessary to help our partners find the best solution. Our team is also generous with their time and their networks, making connections and sharing expertise however we can.

Second, you'll hear our team say **"Be a Lighthouse"** often.

Because to us, that phrase guides the work we do. It's all about helping people. We tell the stories of our company in the hopes they inspire others, and we share our light with the communities we serve to uplift and support everyone we touch.

And lastly, our third core value is **Light Up Those Around You.**

We want to bring positivity and joy to every interaction, however we can. We build trusting and friendly relationships. And we have the proof to back it up, with satisfied clients across Western New York and beyond, and more than 150 five-star reviews online for the world to see.

We're serious when we say our goal is to be the most inspiring technology partner in the communities we serve.

And we hope this conversation about cybersecurity has inspired new conversations that can benefit you and your business.

LHTservices.com

Seneca One Tower
1 Seneca Street, Suite 2820
Buffalo, New York 14203
(716) 634-0509