Data and Network Security Checklist

Get to know your company's cybersecurity maturity

Complete the checklist below...

When it comes to your data, you can never be too careful. Data loss or theft has both short-term and long-term repercussions for your business operations. Taking a proactive approach and securing your network and data can go a long way to preventing a catastrophic incident.

Do you know everyone who has access to your company data? You're trusting them with the personal information that your clients have entrusted you with. This checklist is comprised of questions you should ask an IT manager or network administrator whenever and wherever you're storing data.

1 Basic Network Security

- [ ] Who is in charge of your network security? Do they have IT-related experience?
- [ ] What is your process to review, test and implement new technology solutions?

2 Documentation

- [ ] Are your IT systems and administrative passwords well documented and up-to-date?
- [ ] Do multiple trusted people have access and is this access level documented?
- [ ] Is the information secure in a reputable Password Manager, not a browser?

3 User Access

- [ ] Are there measures in place that control who is able to access your data?
- [ ] Is there an administrator who manages access control?
- [ ] Is there a record of who can access the data and a log to track the user?
- [ ] Is there anyone outside of your internal staff that will have access to client data?

4 Email

- [ ] Are you using spam and malicious file scanning?
- [ ] Have you confirmed your MX Records, SPF Records and Server Identity are set up properly?
- [ ] Are you scanning for malicious links and attachments inside your email system?
- [ ] Do you have a written policy for transmission of sensitive data?
- [ ] Are you leveraging encrypted email to communicate outside of your organization?

5 Bring Your Own Device (BYOD)

- [ ] Do you have a mobile device manager to manage data accessed on mobile devices?
- [ ] Is there a policy to remove firm data if an employee's device is lost or the employee is terminated?

6 Networking

- [ ] Do you have a hardware firewall and is it under support by the manufacturer?
- [ ] Is the firewall configuration clean and operating system up to date?
- [ ] Do you have a monitored Intrusion Detection System in place?
- [ ] Are you using strong encryption on your wireless networks?
- [ ] Are firewall logs being monitored to understand who is gaining access to the environment?

7 Physical Security

- [ ] Are your servers and data in a physically locked or restricted area?
- [ ] If so, who has access and how?
- [ ] Are laptops loaded with disk encryption and/or tracking software in the event they are lost or stolen?
- [ ] Are the doors to your offices secure at night and on the weekends?
- [ ] Are devices left open and unattended allowing prying eyes to view information

8 Data/Files

- [ ] Where are your backups and how do they get where they are going?
- [ ] Are backups retained offsite and secure from a ransomware attack?
- [ ] Are your files and folder permissions on your servers/SharePoint or other Cloud repository secure and setup properly?
- [ ] How do you store and transfer sensitive information with your clients?

9 Websites

- [ ] Where is your website hosted?
- [ ] Are you using SSL certificates for your website to ensure encrypted communication?
- [ ] Are you leveraging additional security to block attacks that can disrupt your business?

10 Operating Systems and Applications

- [ ] Are you enforcing the use of strong passwords? Are regular password changes enforced?
- [ ] Are your computers running supported versions of their operating systems?
- [ ] How often are your systems patched and how do you know it is working?
- [ ] Do you patch all of your applications or just Microsoft Products?
- [ ] Are you running up-to-date network-wide MDR software?
- [ ] Are MDR alerts addressed 24x7?

11 Data Loss/Theft

- [ ] Do you have a data theft plan?
- [ ] Do you have a policy for notifying your clients of a data breach/loss situation?

12 Dark Web Scan

- [ ] Have you had a dark web scan performed on your email domain to determine if any accounts are compromised?

13 Password Vaults

- [ ] Do all employees have access to and use a password management solution to prevent simple passwords?

14 MFA (Multi-Factor Authentication)

- [ ] Multi-Factor Authentication enabled on all applications and services that allow it?

15 Endpoint Security

- [ ] Do you have more than just standard MDR? Content filtering, 3rd party application patching, and malware defense?

16 Event Tracking (SIEM)

- [ ] Is there a security monitoring solution in place for event log tracking and analysis?

Security Awareness Training

17

- [ ] Do you have a training program in place to train your employees about cyber security best practices?
- [ ] Is training setup at least annually?
- [ ] Are you testing your employees on their knowledge of email phishing?

So, how did you do?

If you were unable to check many of the boxes, you may be exposing your company to major risk. If you need help with any of these items, consider talking with the cybersecurity experts at IronEdge Group. We have the tools and personnel to substantially reduce the cybersecurity risks to your business so you can worry less and focus on success.

Ready to take the next step in securing your business?

Let's discuss how IronEdge's **Cybersecurity Services** can protect your business from evolving threats.

Request Cybersecurity Scan

IRONEDGE