IRONEDGE GROUP

Technology In Your Corner

Data and Network Security Checklist

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.

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?

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 or locked away?

User Access

- ❑ Are there measures in place that controls 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?
- ❑ Does your firm offer training on cyber security to its employees?
- ❑ Is there anyone outside of your internal staff that will have access to client data?

Email

- ❑ Are you using external Spam and Virus Filtering?
- ❑ Have you confirmed your MX Records, SPF Records and Server Identity are setup properly?
- ❑ Are you scanning for viruses inside your mail server database?
- ❑ Do you have a written policy for transmission of client data?
- ❑ Are you leveraging encrypted email to communicate outside of your organization?

Bring Your Own Device (BYOD)

- ❑ Do you have a policy or software to manage use of mobile devices?
- ❑ Is there a policy in place to remove firm data if an employee owned device is lost or the employee is terminated?

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 a strong encryption on your wireless networks?

About IronEdge

Founded in July of 2005, IronEdge Group provides businesses in and around Houston and San Antonio with a multitude of enterprise IT solutions. For more than a decade, IronEdge Group has worked with businesses of all sizes and industries to design and deliver technology solutions that meet the needs of their customers and exceed their expectations. Specializing in assisting organizations streamline daily operations,

IronEdge Group focuses on taking proactive measures to ensure the security and integrity of their clients technology. Among many other awards, IronEdge Group has recently landed a coveted position on the CRN's 2016 Managed Service Provider 500 list, along with being voted one of the "Best Places to Work" by the Houston Business Journal for the third consecutive year.

IronEdge Group
3000 Wilcrest Drive, Suite 300
Houston, Texas 77042

(713) 574-5555
sales@ironedgegroup.com
www.IronEdgeGroup.com

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?

Data/Files

- ❑ Where are your backups and how do they get where they are going?
- ❑ Are your files and folder permissions on your servers secure and setup properly?
- ❑ How do you store and transfer sensitive information with your clients?

Websites

- ❑ Where is your website hosted?
- ❑ Are you using SSL certificates for your website to ensure encrypted communication?

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 network wide anti-virus and anti-malware software and is it up to date with a valid subscription?

Data Loss/Theft

- ❑ What is your data theft plan?
- ❑ What is your policy for notifying your clients of a data breach/loss situation?

Common Policies to Protect and Control Data

Acceptable Use Policy
A set of rules and guidelines created by the owner of a network, website, and application to control a users' actions to prevent risks associated with the abuse of technology.

Remote Access Policy
A documented outline of acceptable methods of remotely connecting to the internal network.

(Bring Your Own Device) BYOD Policy
Because of the popularity of using personal mobile devices (such as smart phones and tablets) to perform tasks while at work, businesses should implement a BYOD policy and software solution to control the devices access to their data and network.

Encryption Policy
Defines which methods of data encryption can be used in an organization, as well as the recommended encryption method(s). This type of policy is critical when it comes to compliances, to ensure data safety standards are clearly understood and met by everyone on the network.

Privacy Policy
Details how information collected will be used, disclosed, stored and managed by the company receiving the information.

Email and Communications Policy
Outlines acceptable behavior and uses of a business' email along with other business communications. They often define the acceptable and unacceptable uses for that communication, i.e.: phones, fax machines, VoIP, etc.