PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

Small Business CyberSecurity Questionnaire

Organization Name:_____ Date:

Primary contact for data security matters: _____

Number of computer systems in your organization: _____ Number of locations/offices: _____

Does your organization have a central server(s) for storing and managing data? ____Yes _____No

Please answer the questions below to the best of your ability, so that we can better understand your level of computer security and data protection. This information will assist with the process of developing an improved security posture for your organization and help to insure business continuity in the event of a cyber attack or data breach. All answers should represent the company as an entity, and not any one specific individual member of the organization. If you are uncertain about the answer to any of the questions, please make your best estimate, as an unanswered question will count as zero points toward the organization's overall security score for evaluation purposes. Any information provided on this form will be kept strictly confidential and used only for evaluation purposes.

Please choose only one answer for each question by placing an "X" next to the closest correct response.

1. On a scale from 1 to 10, with 10 being the highest rating, how important is cybersecurity, data protection, data recovery (backups) and employee cybersecurity awareness within your organization?

   ___(1) ___(2) ___(3) ___(4) ___(5) ___(6) ___(7) ___(8) ___(9) ___(10)

2. What level of password secrecy is being enforced at your organization?

____ No passwords are being used to protect data stored on computer systems (0)

____ Everyone uses the same login name and password (1)

____ All user accounts (login names) are unique, but they all use the same password (2)

____ User accounts and passwords are unique for each user, but users know each other's passwords (3)

____ User accounts and passwords are unique for each user and kept private (4)

____ User accounts and passwords are unique and complex* for each user, and kept private (5)

*Combination of upper and lower case letters, numbers and symbols (at least 3 of these 4 types)

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

3.) What level of password complexity is being enforced at your organization?

____ Anything can be used for a password, regardless of length or complexity (0)

____ Passwords must be at least 8 characters long, but there are no other requirements (1)

____ Passwords must be at least 8 characters long and cannot be names or dictionary words (2)

____ Passwords must be at least 12 characters long and use complexity* (3)

____ Passwords must be at least 16 characters long and use complexity* (4)

____ Passwords must be at least 16 characters long and are randomly generated (5)

*Combination of upper and lower case letters, numbers and symbols (at least 3 of these 4 types)

4.) What level of security has been implemented within your organization to separate different kinds of information (financial, legal, medical, HR, etc.) and access to it?

____ No security or organization. Everyone can access all company data (0)

____ Data is organized by type, but no specific permissions have been set (1)

____ Data is organized by type, and staff is allowed access based on user need for each type (4)

____ Data is organized by type, access is assigned based on user need; access is monitored and logged (5)

5.) What level and/or type of Internet/web filtering is being used by your business?

____ None. Web browsing is not restricted, monitored or filtered in any way (0)

____ Minimal. Employees are told what websites are acceptable and expected to comply (1)

____ Light. Antivirus software on the computer systems block users from infected websites (2)

____ Medium. Software on each workstation blocks websites by category and reputation (3)

____ Heavy. A gateway Unified Threat Management (UTM*) appliance provides web filtering (4)

____ Maximum. A UTM* appliance only allows users to visit approved web sites; all others are blocked (5)

*UTM devices inspect Internet traffic for viruses, spam and website requests and filter malicious content

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

6.) What kind of computer antivirus solution does your organization use?

____ Random antivirus software installed on each system, some may not be protected at all (0)

____ The same free, unmanaged/unmonitored antivirus software is used on all systems (1)

____ Systems are all running a paid-for version of standalone antivirus, unmanaged and unmonitored (2)

____ Systems are all running a monitored antivirus solution that is managed from a central console (3)

____ Systems are all running a monitored antivirus solution that is managed by an IT service provider (4)

____ Systems are all running managed/monitored antivirus and there is a gateway UTM* solution (5)

*UTM devices inspect Internet traffic for viruses, spam and website requests and filter malicious content

7.) What kind of backup solution does your organization use?

____ None (0)

____ Critical data gets backed up to a thumb/external drive sporadically (1)

____ Critical data gets backed up to a thumb/external drive sporadically and taken off site (2)

____ Full server/system local backups are performed daily and physically taken off site (3)

____ Full server/system backups are performed daily and replicated to cloud storage on the Internet (4)

____ Full server/system backups are performed hourly and replicated to cloud storage daily (5)

8.) How often does your organization perform a test data recovery from backups to verify integrity?

____ Never (0)

____ Annually (1)

____ Twice each year (2)

____ Quarterly (3)

____ Monthly (4)

____ Weekly (5)

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

9.) How many people in your organization know the master/administrator password with full computer system control and access to all data on the network?

____ Everyone, or don't know (0)

____ Most of the members on the staff (2)

____ Only senior members on the staff (3)

____ Three or fewer senior staff members, on a need to know basis (4)

____ Only the person/company entrusted with managing user accounts and data security (5)

10.) What kind of e-mail antivirus and spam filtering solution does your organization use?

____ None, or don't know (0)

____ Local antivirus scans incoming messages for viruses when they are opened (2)

____ Local antivirus scans incoming messages for viruses prior to opening them (3)

____ All incoming messages are scanned for viruses before they arrive into a user's mailbox (4)

____ All messages pass through an outside spam/virus filter or UTM*; local antivirus scans it, too (5)

*UTM devices inspect Internet traffic for viruses, spam and website requests and filter malicious content

11.) Is User Access Control (UAC) turned on for the computers/workstations within your organization? (UAC is the notification that pops up whenever you install software or make changes to your computer system, asking you to confirm your actions.)

____ Not turned on for any computer system, or don't know (0)

____ Turned on for a few systems, but not all of them (1)

____ Turned on for most computer systems (2)

____ Turned on for all computer systems on the network, but users can click past it (3)

____ Turned on for all computer systems, and it requires an Administrator to approve changes (5)

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

12.) What kind of Internet firewall does your organization use for protecting your network?

____ Don't know (1)

____ The modem/router provided by our Internet Service Provider (2)

____ A wireless home/personal router/firewall (Netgear, Linksys, TP-Link, D-Link, etc.) (3)

____ A business-class router/firewall installed by an IT professional or qualified employee (4)

____ A business class firewall/router with Unified Threat Management features* turned on (5)

*Gateway Antivirus, Web Filtering, Stateful Packet inspection, Intrusion Prevention, Bad Website Blocking

13.) Who is allowed to connect their personal devices to your wireless network connection? (Cellphones, laptops, tablets, etc.)

____ Anyone; it requires no passcode to connect to it (0)

____ Only people who we give the encryption passcode to (1)

____ Only to a dedicated Guest Access wireless connection, without a passcode (2)

____ Only to a dedicated Guest Access wireless connection, with a guest passcode (4)

____ No one is allowed to connect personal devices to our wireless network (5)

14.) Who is allowed to connect flash drives (also called thumb drives) to their computer at the office?

____ Anyone. We have no policy regarding the use of flash drives (0)

____ Anyone, as long as it is work related (1)

____ Anyone, work related, after their antivirus performs a mandatory virus scan (3)

____ Any staff member, but only drives provided by the company, after a virus scan runs (4)

____ Only authorized members of the staff using a company-owned flash drive on certain computers (5)

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

15.) How is financial, medical and/or PII* (Personally Identifiable Information) stored on your computers, and what kind of security is in place to protect it?

____ It might be found on any computer, with no protection or security in place to protect it (0)

____ All data of this type is consolidated and stored on one computer/server, with minimal protection (1)

____ All data of this type is consolidated and only available to specific staff members with passwords (3)

____ Data of this type is consolidated and encrypted with passwords, with limited staff access (4)

____ All data of this type is consolidated and kept on an encrypted hard drive, in a secure location (5)

*PII refers to the following types of information that can be used to identify an individual, and to potentially compromise their identity or security: Names, addresses, phone numbers, driver's license numbers, social security numbers, date of birth

16.) What software-based firewall (Windows or third-party) is running on your computers to protect against the internal spread of a worm virus or hostile attack from another computer on your network?

____ None; it has been turned off on all computers to avoid software issues (0)

____ Unknown, but not intentionally turned off (default state in Windows is On) (2)

____ Windows/other firewall is turned on for most systems, turned off on the others (3)

____ Windows/other firewall is turned on for all computer systems (4)

____ Windows/other firewall is turned on and monitored for all systems on the network (5)

17.) How are Microsoft Windows Updates managed and installed on your organization's computer systems?

____ Unknown (0)

____ Windows installs automatic updates, but we never verify that they are current (1)

____ Windows installs automatic updates, which we verify manually on a random basis (3)

____ Windows installs automatic updates, which we verify manually on a regular basis (4)

____ Windows and Microsoft Updates are managed and monitored network-wide from a console (either in-house or by a professional IT support provider) (5)

PJ Networks
Computer Services
Network Support ~ Security and Compliance ~ Managed Services

18.) How are third-party software updates (Adobe, Java, iTunes, etc.) managed and installed on your organization's computer systems?

____ Unknown (0)

____ We install software updates when prompted by the software programs (2)

____ We use software (AV or other package) to check for updates and prompt us to install them (4)

____ Third-party software updates are managed and monitored network-wide from a console (either in-house or by a professional IT support provider) (5)

19.) What ongoing training and data security awareness does your organization provide to your employees in order to insure that they are knowledgeable, aware and diligent in their data security practices?

____ None/Unknown (0)

____ We hold annual data security meetings and training sessions (2)

____ Each employee is provided with a training manual upon joining our organization (3)

____ We provide cybersecurity training manuals to new employee and hold quarterly meetings (4)

____ We provide access to online training courses, test employee security awareness and knowledge with quizzes and tests, and we have monthly meetings to discuss data security and best practices (5)

Thank you for completing this small business cybersecurity questionnaire.

Each answer has a number in parentheses that counts toward your organization's total self-assessment score, with a possible total score of 1 to 100 points. A higher score indicates that your organization has an advanced awareness of security, it employs the highest security standards and practices, and that it proactively works on maintaining its overall security posture on an ongoing basis. A lower score would indicate that there are areas of improvement that need to be addresses.

Please let us know if you are interested in cybersecurity training materials, or a professional consultation to review your organization's security policies, procedures and practices.

The BIG Question:

Can you handle everything on our own, or do you need professional IT support..?

Get a little training, educate your employees, be diligent and you can handle most of it on your own!

Managed Services can take care of many of a small business's needs when it comes to following best cybersecurity practices. These include:

- Operating system patches
- Third-party software updates (Adobe, java, etc.)
- Automated backups (local and cloud)
- Vulnerability Scans
- Antivirus updates and definitions
- E-mail spam/virus filtering
- Bad website blocking
- Realtime system alerts
- System firewall monitoring
- Suspicious/unusual computer activity
- System health alerts

You can bring in **professional assistance** to:

- Install/configure a business-class firewall
- Secure your network environment
- Educate your employees
- Establish best security practices
- Create company computer and Internet usage policies
- Secure wireless network connections
- Provide ongoing training

But <u>you</u> will still need to:

- Enforce company security policies
- Provide new employees with training
- Practice best security practices (lock your screen!)
- Keep cybersecurity alive as an active topic
- Correct each other when necessary
- Report serious/repeat offenses to management (sorry)