NSP | Nonprofit Support Program
HARTFORD FOUNDATION FOR PUBLIC GIVING

Assess Yourself Against the Stable & Secure Benchmarks

For each Stable & Secure Benchmark, review and discuss the questions below to help you identify opportunities for improvement that can be addressed in your tech plan. If this document raises questions for you and/or if there are some question you do not understand, make a note of them to discuss with your planning consultant or another IT resource.

1. Computer Life Cycle
2. Operating Systems for Computers and Servers
3. Appropriate Network Environment
4. Reliable Internet Connection
5. Firewall Protection
6. Secure Wireless Networks
7. Backup & Recovery Process
8. Malware Protection
9. Secure Internet Browsing
10. Data Security
11. Documentation
12. Technology Support
13. Physical Security
14. Power and Surge Protection

1. Computer Life Cycle
Nothing lasts forever, and computers (and other electronic equipment) are no exception. It's important to keep track of which equipment is nearing the end of its usefulness, to manage a regular transition from older equipment to newer, and to plan for these expenses in your budget.

Q1. Do you keep an equipment inventory up to date and do you have a plan for replacing computers as they become less useful?

Q2. Do you have any backup computers that could operate as a spare in case an "everyday" computer crashes? Does the backup have the software installed necessary to actually take the place of another in the office?

Q3. Do you have a regular expense in your budget to smooth out the costs of replacing computers, or do you plan for a "big bang" upgrade every several years?

2. Operating Systems for Computers and Servers
The operating system (OS) is the basic environment on which all your other applications run. There are many operating systems, with Windows, OSX (Apple), and Linux the most popular.

Q4. Do you have a strategy for approaching operating system decisions? For example, standardization on a single OS vs. allowing people to choose their own workstation and OS or bring their own devices (BYOD) to work? Does your strategy take into account the maintenance implications of your chosen approach?

Q5. Is there someone within your organization (or a vendor) who is responsible for making sure security patches are applied to your computers' OS and monitoring when patches will no longer be produced for each OS in use?

3. Appropriate Network Environment
Computer networks are an increasingly important part of any IT infrastructure, and it's important to have a reliable and fast network for efficient collaboration.

Q6. Do you have a network in place at your office(s)? If the network operates via cables in a building, are those cables in good condition?

Q7. Is there someone responsible (internally or a vendor) for designing the network and keeping it up and who you could call in an emergency to restore it? Are there frequent emergencies that interrupt the daily operations of your organization?

4. Reliable Internet Connection
Internet services, including email and various web applications, have become an integral part of daily work. Having a fast and reliable Internet connection can help to promote everything else in your office going more smoothly, especially if you already have or intend to move some of your critical software to cloud-based services.

Q8. Is your office network connected to the Internet, or are individual computers able to connect to the Internet directly via a hub or router? What is the speed of the connection? Do you find that you ever saturate *the connection (when everything slows down because everyone is doing heavy internet-based work at the same time)?*

Q9. Are there frequent Internet outages that interrupt the daily operations of your organization? How long does it typically take for service to be restored? Are there other options for Internet access at your location(s) if and when this happens?

5. Firewall Protection
It's very easy for ill-intended people to launch automated attacks over the Internet, so it's important to filter the raw Internet traffic from getting directly to the computers on your network. That's what a firewall does – protects your computers from being accessed via your network from the outside in.

Q10. Are computers on your internal network, or individual computers, connected to the Internet?

Q11. If yes, is there a device that sits in your network between the Internet and your computers to filter traffic coming into the network? This is usually called a firewall but can also be combined with a router (with the combo device typically just called a router).

Q12. Do you have any internal servers that are designed to be Internet-facing? Is there someone responsible (internally or a vendor) for the security of those systems?

6. Secure Wireless Networks
Wireless networks can be very convenient for untethering ourselves from a particular working space, but they must be properly maintained and can also present security risks.

Q13. Do you have a wireless network at your office? If yes, is there some level of security required for connecting to the network?

Q14. Is there someone responsible (either internally or a vendor) for monitoring the wireless network and working to bring it back up when it goes down?

Q15. Are there frequent wireless outages that interrupt your normal operations? How long do these outages usually last?

7. Backup and Recovery Process
Backups are easily overlooked until you need them (and then it's usually too late!). Make sure you have operational and technical processes in place to ensure your critical organizational files are copied to a secure location on a regular basis, and make sure you occasionally test your ability to recover from your backups.

Q16. Is there a process by which everyone's individual computers are backed-up, or a portion of them where people are instructed to keep important files, on a regular basis? Is the backup process automated or manual?

Q17. If you are maintaining any servers (or vendors are maintaining servers for you), are they backed up on a regular basis?

Q18. If you are using any web applications for core processes, do you take backups or full extracts of that data on a regular basis? For example, for a cloud-based CRM tool?

Q19. Are all your back-ups in one physical location, or does your process ensure that some are in another location ("off-site," although it could really just be another one of your sites)?

Q19. Do you have a plan to make sure each of your backup and restore processes will work properly in an emergency (i.e. have you actually every tested the process to restore and recover data)? Do you run through your plan at least once a year?

8. Malware Protection
Some software is malicious; serving unwanted ads, stealing your data or processing power, or worse. Prevention is the best approach to staying malware-free, but it's also important to have a plan for when a computer becomes infected.

Q20. Do you have anti-virus software installed on all your computers? If not, do you have a good reason why it's not installed?

Q21. Are staff savvy enough not to click strange links in emails? Are they familiar with the basic ways that they can be fooled into infecting their own computer (phishing emails/scams, Trojan horse programs, infected media, unpatched OS, etc.) so they can be better able to avoid them?

Q22. When a computer is discovered to contain malware, do you have a process for resetting the computer and restoring the data files (but not the malware!) from backups?

9. Secure Internet Browsing

The internet is one common avenue for information to be stolen and for malware to be installed. It's important to understand the basics of Internet security to avoid making the organization vulnerable.

Q23. Are staff familiar with HTTPS, the secure version of HTTP which is used on sites that deal with online banking, health data, or other secure information? Do they know to check that a site connection is secure prior to entering any secure information?

Q24. If there is anti-virus software installed, is it configured to protect against malicious websites?

10. Data Security

Many organizations are increasingly paperless, and that has translated into an abundance of data. Some data may have protection requirements written into the law (medical data, payroll data, credit card data, etc.); it's important to know how to protect all your data with the appropriate level of security.

Q25. Do you keep any data that is particularly sensitive and perhaps regulated? If so, is there an appropriate infrastructure for securing that data in-transit and while "at rest"?

Q26. Is all secure data on all devices secured by a password? Do you have a strong password policy? Do staff know never to share their password with anyone*?*

11. Documentation

It's important to document your systems and processes for consistency and so that you can transition duties from one person to another if necessary. Documentation can also be an excellent way to look at whether your current processes can be improved or optimized, and for cross-training staff.

Q27. Are your core processes documented so that if a key staff person was no longer available to work, others would be able to keep things going by following the documentation?

Q28. Are your plans documented so that you can quickly execute them when necessary? For example, you might have plans for what to do if the internet goes down, or if a computer crashes, or if someone gets a computer virus, etc.

12. Technology Support
Good IT support can be provided internally or by a vendor; the most important thing is that they can promptly provide both proactive and reactive support and be a partner with the organization they are supporting.

Q29. Do you have an internal person or a team or a vendor that is primarily responsible for day-to-day tech support? Are technology crises frequent? When they happen, are they solved quickly? After they happen, is there a post-crisis analysis to put structural solutions in place to reduce the likelihood of future crises?

13. Physical Safety
One of the most important kinds of technology security is physical security. You can have all the protection software in the world on your server but if someone can just pop open a door and walk out with your server, then that's a much bigger risk.

Q30. Are devices with secure or mission-critical data kept behind locked doors? Are there other elements of physical security in place, like an alarm company or security cameras, that would discourage a potential thief?

Q31. For paper files that contain secure or mission-critical information, are they kept in a locked room or in a locked file cabinet? Is there any redundancy or protection for those files in the event of a fire?

14. Power and Surge Protection
All computer devices need electricity to function, and there are accessories that can prevent too much power or too little from getting to them. These are especially important if you live in a place that experiences big storms that could cause surges in power.

Q32. Are all electronic devices plugged into surge protectors which are themselves plugged directly into the outlet? A surge protector will prevent a power surge from making it all the way to your device (and frying it).

Q33. Do you have Uninterrupted Power Supply (UPS) units connected to any particularly critical devices, computers, or servers? A UPS will provide steady power for an additional period of time in the event of a power outage. It probably won't be enough time to run your whole infrastructure while the power's out (unless it's only out for a few minutes), but it should give you enough time to shut things down in an orderly way and avoid data loss that can be associated with suddenly cutting the power.