Protecting your Business with Cybersecurity in 2020 and Beyond

By Josiah Dykstra, Ph.D.

Every modern audiology practice relies on computers and Internet to function. Whether it's scheduling, chart reports, or social media, technology can make or break a business. The cost of downtime—from equipment failure, hackers, disgruntled employees, or accidents—disrupts essential business functions that could cost you hundreds or thousands of dollars an hour. Hackers target everyone's accounts, machines, and data. Some hackers want to steal personal information that they can sell (identity theft), some want to extort money (ransomware), and others want to use your computer to send spam (botnets). Now is a perfect time to review how you can best protect yourself in the new year and new decade.

In some cases, security is more than a good idea to protect essential business functions, it is also the law. As a healthcare provider, you are subject to laws and requirements to safeguard protected health information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires implementation of administrative, physical, and technical safeguards for electronic PHI. Compliance with HIPAA is mandatory and carries financial penalties for noncompliance. If you accept credit card payments like most businesses, other security standards—such as Payment Card Industry Data Security Standard (PCI DSS)—also govern the protection of sensitive financial information. PCI DSS is not a federal law, but a common contractual obligation with payment card processing companies.

Cybersecurity can seem difficult to understand, and implementation can feel overwhelming… even for doctors of audiology! Media, software vendors, and cybersecurity professionals sometimes focus on fear and alarm around insecurity, but protection is a positive component of keeping people and businesses safe and successful. Below is a very brief self-assessment to help gauge your security practices today and to identify areas where improvement may be needed. Go down the list and add up the number of boxes you can check. If you're unsure about a question, leave it blank.

- ☐ We have a cross-cut shredder and use it regularly.
- ☐ We have a Business Associate Agreement (BAA) with all third-party partners (hearing aid, earmold, cochlear implant, equipment manufacturers, office management system companies, accountant, etc.).
- ☐ Every employee using a computer has an individual account and private password.
- ☐ We have a password policy in our Employee Handbook.
- ☐ Passwords are kept confidential and not shared with others.
- ☐ My business email password is different from all my other passwords.
- ☐ Computers are kept updated and patched at regular intervals (e.g. weekly).
- ☐ Anti-virus is installed and running on all computers.
- ☐ Computer screens lock automatically after 5 minutes of inactivity.
- ☐ We log activity on our network and have the capability to identify suspicious behavior.
- ☐ Data backup is performed regularly (e.g. weekly).
- ☐ Annual training for identifying spam and phishing emails is conducted with all employees.
- ☐ Our practice website is secured with SSL (e.g. HTTPS).
- ☐ We have an annual vulnerability assessment or penetration test conducted on our network and website.
- ☐ Employees are not allowed to access the Office Management System (EHR/EMR) from home.

Your score:_____

- **If you scored 12-15**, congratulations! Consider yourself savvy about security risks and countermeasures; continue your proactive steps. It's important that you audit your cyber situation on an on-going basis and remain persistent with training and updates.
- **If you scored 8-11**, you've made some effort to secure your business against security incidents and cyber attacks. However, you need to consider your risk factors more closely and take some corrective actions.
- **If you scored below 8,** you are at high risk, without necessary measures to protect your business. Take immediate action to become more informed about security threats and the steps you can take to minimize your risk.

Whatever your score, security requires continuous vigilance because threats are persistent and evolving. There are many mitigations you can take to protect yourself and your business, including policy, process, and technology. Three critical actions should be first for business owners to protect your essential functions: policies, updates, and training.

1. **Create and Enforce Company Policies.** Every employee plays a role in protecting the business. Employee manuals describe the appropriate conduct and behavior for employees, and cybersecurity is an essential component. These policies are the first line of defense to protect the business from dangerous behavior. Policy is a low-cost and legally-defensible guard against cyber incidents. You should consider a remote access policy, a wireless communication policy, password protection policy, email policy, and digital signature policy. The SANS Institute and cybersecurity professionals can offer templates for these policies.[1]
2. **Enable and Run Software Updates.** Nothing in life is static or perfect, and computer programs are no exception. Hackers routinely exploit known vulnerabilities in common software. Software is very complex, and even the best vendors routinely find and fix bugs. Updates patch these known security holes, but also provide improved performance and new features. Many programs, including Windows and web browsers, offer automatic updates that can make security easy.[2]
3. **Provide Annual Security Training.** Hackers often target human weaknesses to break into computers, including malicious email attachments and links. This is known as social engineering and there is no 100%, foolproof way to prevent criminals from attempting it. But there are ways to protect against it, including strong policies, consistent and persistent training and awareness, and vigilant system maintenance. These are only effective if they are consistently implemented and reinforced; one click, one divulged password, or one employee wanting to be helpful can undermine your efforts. You can add this annual security training to your annual HIPAA training.

This year, make a resolution to fully evaluate where cybersecurity is needed to protect your business. If needed, hire a security professional who can provide advice and implementation tailored to your situation. Then take concrete steps to ensure that you are adequately protected. Schedule one hour this month for all employees to take basic or refresher training on good cyber hygiene. Keeping your practice safe and secure is achievable! ■

Josiah Dykstra, Ph.D. is Founder and Cybersecurity Consultant at Designer Security. He has more than 15 years' experience in cybersecurity research, practice, and education. He can be contacted at josiah@DesignerSecurity.com.