Having the Right Tech Tools will Keep You Cybersafe

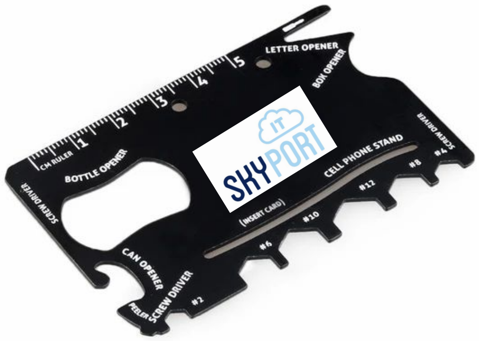
By Daniel Marcellus

Managing a system without the right tools is like eating a steak dinner without a fork and knife. Sure, you might be able to make it work, but it's less effective and the end result can get messy. In the tech world, having the proper software, hardware and training makes all the difference in protecting your patient's data from falling into the wrong hands. Having proactive technology in place and staying up-to-date on social engineering tactics can prevent your team from wasting precious time on trying to rectify a security issue, whether it's from a data breach or an employee succumbing to a phishing campaign. If you're looking to minimize security risk and stay compliant, you can implement these recommended tools into your current IT infrastructure:

- Gap Analysis
- Policies & Procedures
- Multi-Layered Protection
- Security Audits & Remediation
- Security Monitoring and Reporting

Gap Analysis

First thing's first: your company should be aware of any holes in its current information systems performance. Once your IT environment is assessed to determine if requirements are being met, you'll receive personal recommendations on what steps to take towards remediation.



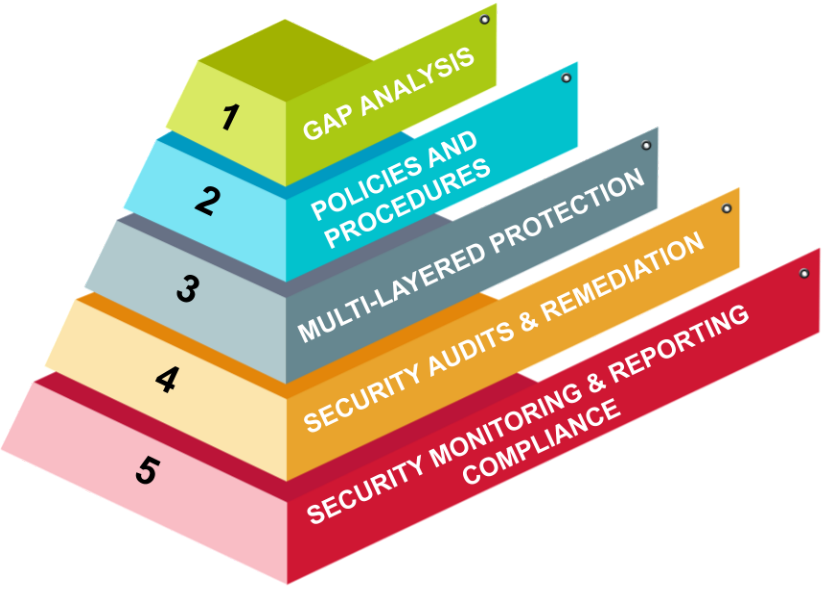
Security Policies & Procedures

Having succinct and informative guidelines available for your staff means they'll be adequately knowledgeable in the proper protocols for your business. Depending on the individual needs of your business, you may need specific policies or procedures on internet usage, software downloads, or other non-tech related subjects. Customized templates based on your company's needs are available on an as-needed basis.

Multi-Layered Protection

Just one level of protection isn't good enough to thwart a hacker or other malicious entity. Using a multi-layered approach makes it more frustrating-- and more difficult-- for someone to use your information against you. Tools like spam filtering, 24/7 monitoring, and remote support simplify the process so your employees don't get stuck untangling the mess.

Security Audits and Remediation
Audits are necessary to make sure any current IT staff is following proper policies and procedures. There's a few different types of audits that may be relevant to your business: Network, Security, and PCI-DSS audits. Remediation occurs once your work plan is developed. From there, needed services can be implemented to address any issues that arise. Your security is fully managed and your IT is provided with the tools needed to keep you safe.


1
GAP ANALYSIS
2
POLICIES AND PROCEDURES
3
MULTI-LAYERED PROTECTION
4
SECURITY AUDITS & REMEDIATION
5
SECURITY MONITORING & REPORTING COMPLIANCE

Security Monitoring and Reporting
This step is necessary to keep everything running smoothly.
Managed Services are based on proactively monitoring and remediating issues in real time to keep hackers and other "bad guys" out. By utilizing various tools, your systems stay patched and protected through a layered approach at multiple layers and levels in your global IT infrastructure. Proactive support means your company will receive prompt notification in case of any problems.

Want to learn more? Check out skyport-it.com and choose your industry, or go to skyport-it.com/question question to send us a message.

Feel free to contact us directly at 585-582-1600.