wizer

How Would You Spend $10K Yearly On Cyber Security?

This document is a follow-up to a question we asked the LinkedIn security community. The question was, “You’re a small business owner (Think Restaurant, small accounting firm). You have $10K (which is still a lot for many of them...) to spend yearly on cyber security. How would you spend it?”

This is the link to the original post.
https://www.linkedin.com/posts/gabrielfriedlander_cybersecurity-infosec-informationsecurity-activity-6557595362071232512-kisg

Over 150 security experts replied! This document is a summary of their recommendations and provides a simple explanation of what needs to be done and why. The target audience is small business owners. This is not a “Do-It-Yourself” document, but rather a guide to help you hire the right security expert, what to ask for, and what to expect while keeping things under budget.
Let’s begin:

Don't Do It Yourself

If you are not a security expert then find someone who can help. The risk of doing it on your own is too great, partner with an individual consultant or company. Here are some key takeaways when looking for help.

1. It is better to look for someone who is not affiliated with any specific vendor.
2. Not every IT person is a security expert, so make sure they have security expertise.
3. It could be a security consultant or a company.
4. It is also advised to ask how do they secure their own business, to ensure they "eat their own dog food" when it comes to security.

Not Every Business Is The Same

The level of tolerance and risk acceptance varies among businesses and business owners. The amount of money you invest in security is directly related to the level of risk the business or owner is willing to tolerate, as well as the likelihood of a breach. So before you begin securing your company, you need to answer a few questions.

1. How does the business make money? What are the critical apps or assets that if breached can cause large damages to the business?
2. How comfortable is the business with downtime or revenue loss?
3. Who has access to business critical assets, apps, and information, and what will happen if they get hacked?
4. Does anyone have access to business apps or data from home or remotely? What about vendors?
5. Are there regulations the business must comply with such as PCI, HIPAA or GDPR?

It is important to understand that you cannot go from 0% to 100% overnight, it’s a gradual process, so focus first on the biggest risks to your business.

Basic Security ($3000- $5000) Part 1

The bulk of the expense for basic security is labor related (3-5 days of work), since most of the technology solutions are either free or inexpensive.

1. **Data backups**. Backups are extremely important and are a must-have. This is especially important in the case a hacker uses malware to lock you out of your computer(s). Make sure the backups are located off-site and not connected to your network, so if your business is hacked the hackers won't have access to them. These backups should also be password protected.
2. **Internet access constraints**. Depending on the type of business, try to limit access to the internet as much as possible. For example, do not allow employees to browse the web from your POS terminal. If hacked, then all your customer credit card information could be stolen. Some businesses limit employees from accessing the internet and have dedicated a standalone Chromebook laptop for accessing the payroll and accounting systems.
3. **Security awareness training**. Educate your employees about cyber threats! If employees are not trained then the risk they will get infected increases dramatically. Develop a mindset where they're looking out for suspicious emails and practicing how to avoid becoming a target. There are many security awareness solutions, including free ones (https://wizer-training.com) that include training videos.

Basic Security ($3000- $5000) Part 2

4. **Multi-factor authentication**. Enable Multi-factor authentication wherever possible - this basically means that you will need to enter a code that is sent to your mobile device whenever you log in to apps like your online accounting. This protection adds another layer of security in the event your password is stolen. Most apps have this option.
5. **Computer access control**. Lock down your computers - make sure employees have limited permission, for example they should not have permissions to install apps. And verify that only the absolutely necessary applications are installed.
6. **Firewall**. Obtain a firewall and configure it properly. This will limit who can access your business from the outside and will control how data exits your business. If you are using Windows based computers, then enable Windows Firewall on all workstations - blocking incoming connections.
7. **Inventory and patch management.** This will allow you to know what is installed and ensures all apps, computers, and POS systems are updated and patched to the latest versions. Unpatched computers and apps are open doors for hackers… so make sure they are always up-to-date.
8. **Password policies**. Setup complex password policies and make sure employees do not access computers with Admin accounts. Employees should never share passwords. They should have a dedicated login account.
9. **Termination policies**. Make sure terminated employees don't have access to business systems and emails anymore.

10. **Health check and vulnerability scanning.** This should be performed once a quarter and will basically check for any issues with applications or computers on the network that may allow hackers in. Hackers are also using vulnerability scanning on your network to try to get in, so you better be ahead of them.
11. **Anti-virus software**. Install and use this software on all computing devices.
12. **Vendor compliance**. If you need to comply with regulations such as PCI, then process your credit card transactions using a vendor that complies with this regulation.
13. **Email security gateway**. Using this system will check incoming emails for viruses, malware, spam, and other types of attacks before the email arrives to your inbox.
14. **Virtual private network (VPN)**. This will ensure that if anyone connects to your network they will be unable to watch or access the data you are sending over the network, for example, the password you are using to log in to different apps.

Advanced Security ($5000- $10,000)

The basic security section was composed mostly of labor for setting up the basics of protection. The advance security section includes ongoing monitoring and is referred to as “Managed Security Services”. This will be offered as a monthly service and will monitor your network for security issues and hacking attempts. Some of this activity will include:

1. **Cloud based Logging**. Almost all apps have internal logging. These logs include information about how the app is behaving. These logs can be valuable for early detection of cyber attacks or investigating an ongoing attack. These logs are very large in size and require special software to collect and analyze them.
2. **Smart Anti Virus (EDR)**. This software is the next generation of Anti-Virus.
3. **Penetration testing**. After you have the basics covered, you may want to hire a company that will attempt to hack your organization. This will give you an idea of how well are you protected against cyber attacks and what else can be done to better protect your business (This may require an extra cost).
4. **Website Whitelisting.** Because visiting infected websites is often a main vector of attack for hackers, it makes sense to whitelist the websites your business uses for its operations. Whitelisting involves only allowing employees access to websites that have been added to the list of approved sites, all other sites are blocked.
5. **Data Loss Protection (DLP)**. Prevents sensitive information from leaving your business.

And What If Things Don't Go As Planned...

An incident response plan is basically a plan for what to do if your business gets hacked. How you respond to each incident depends on what has happened. For example, if all of your computers were locked by a hacker demanding payment to unlock them, you may take different actions if you have a backup and can restore everything versus no backup. Or what if your customers' credit card information was stolen, then an incident response plan would guide you to who you should notify and what actions you should take to put and end to the breach. To speed recovery, you may find it valuable to have pre-prepared simple flowcharts and contact lists of people and organizations requiring contact in the event of a breach. These suggestions are important to ask whoever is responsible for securing your network, and make sure that the plan is easy to read and is rehearsed...you never know when you will need to use it.

Additional Useful Resources...

The first is the U.S. NIST Small Business Act, it was passed into law in August 2018, it provides cybersecurity resources to SMBs to help protect them against cyber attacks. The second is the UK Cyber Essentials, which is a government information assurance scheme that encourages organizations to adopt good practice in information security. Both resources are government backed frameworks designed to help small business in protecting against cyber threats.