PTS

DATA CENTER SOLUTIONS

Cybersecurity Action Summary

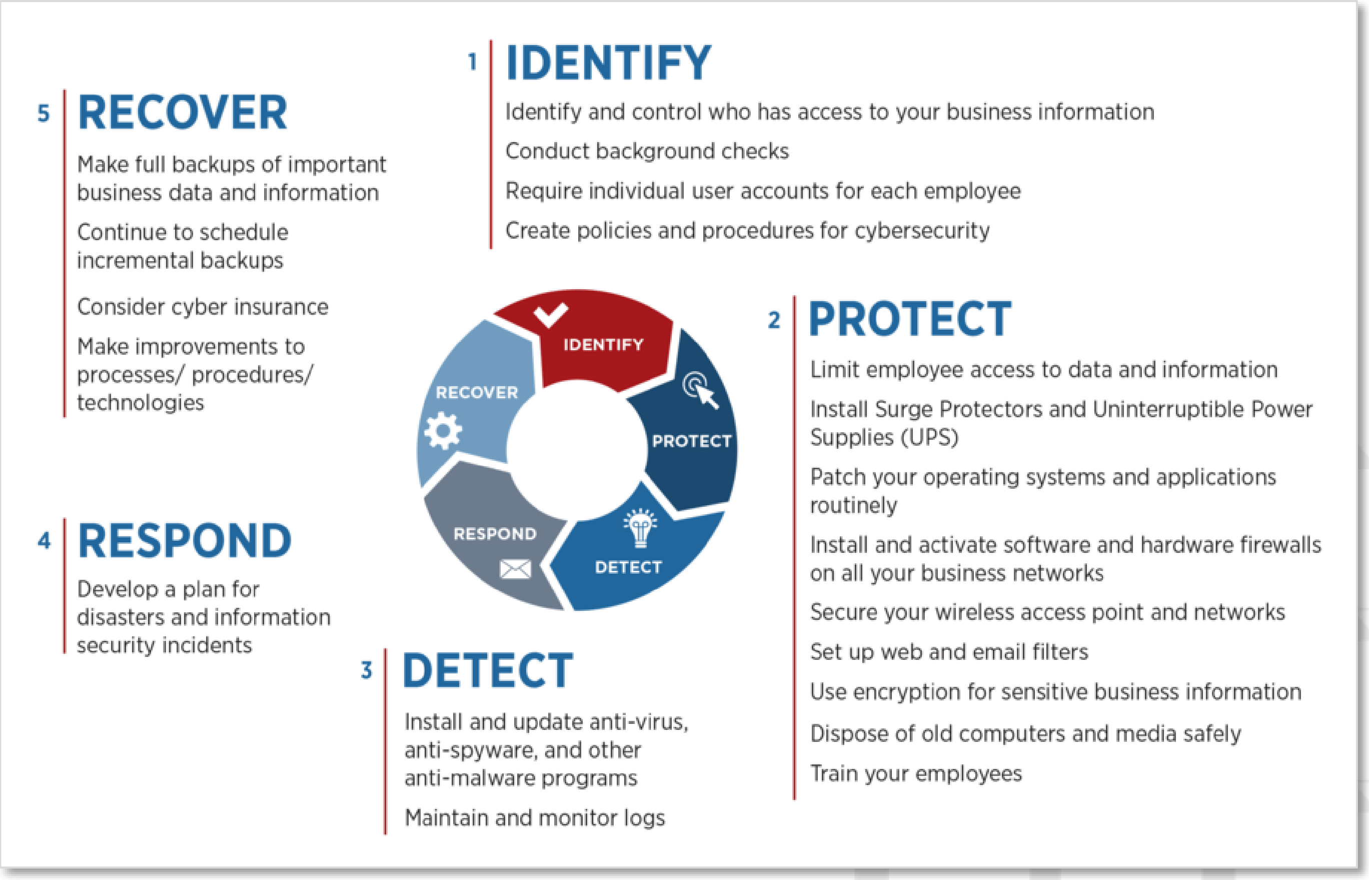
Based on the answers provided in your cybersecurity self-assessment, we offer the following action plan summary, which includes an cybersecurity framework overview, as defined by the *National Institute of Standards and Technology (NIST),* as well as recommendations and vendors providing solutions for eight (8) different functional areas.

Following these recommendations will raise your confidence level in your organization's ability to protect itself from, as well as respond to many of the threats that plague vulnerable systems – no matter who you are.

Cybersecurity Action Summary

Cybercrime is costing businessess hundreds of billions of dollars each year, and there are no indications of a slowdown. Therefore, it is extremely important for enterprises to become aware of their cybersecurity preparedness, to calculate the costs associated with reducing identified risks, and to implement a sound defense plan to manage security moving forward.

The five sections outlined in the graphic below represent the key areas of a thorough cybersecurity program. Each area focuses on either virtual, physical, and/or personnel topics, with the overall goal of helping businesses cover the breadth of cybersecurity objectives for their entire organization.



1 IDENTIFY

- Identify and control who has access to your business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for cybersecurity

2 PROTECT

- Limit employee access to data and information
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)
- Patch your operating systems and applications routinely
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

3 DETECT

- Install and update anti-virus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs

4 RESPOND

- Develop a plan for disasters and information security incidents

5 RECOVER

- Make full backups of important business data and information
- Continue to schedule incremental backups
- Consider cyber insurance
- Make improvements to processes/ procedures/ technologies

Cybersecurity Functional Areas	Vendors
1. Protect against viruses, spyware, and other malicious code Ensure all the business's computers are equipped with antivirus software and antispyware, and are updated regularly. This software is readily available from a variety of vendors who each provide regular patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.	• Webroot • Sophos • Trend Micro • Kaspersky Lab • Symantec
2. Secure your Networks Safeguard your internet connection by using a firewall and encrypting information. If you have a wifi network, make sure it is secure and hidden. To hide your wifi network, set up your wireless access point(s), wireless controller, or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Also, Password protect access to the router.	• Internal Staff • Security Consultant • MSSP
3. Make backup copies of important business data and information Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically, if possible, or at least weekly, and store the copies either off-site or in the cloud.	• Veeam • Zerto • Microsoft Azure • Sungard • Datto
4. Establish security practices and policies to protect sensitive information Establish policies on how employees should handle and protect personally identifiable information, and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.	• Internal Staff • Security Consultant
5. Educate employees about cyber threats and hold them accountable Educate your employees about online threats and how to protect your business's data, including safe use of social networking sites. Depending on the nature of your business, employees may be introducing competitors to sensitive data about your firm's internal business. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses. Hold employees accountable to the business's internet security policies and procedures.	• Ninjio • Internal Staff • KnowBe4 • Wombat • PhishMe
6. Require employees to use strong passwords, and to change them often Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication.	• LastPass • Dashlane • Keeper
7. Create a mobile device action plan Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.	• Internal Staff • Security Consultant
8. Perform an annual cybersecurity risk assessment Information security risk assessment is an ongoing process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information Systems. Information security risk assessments are part of sound security practices and may be required (HIPAA, PCI, DSS, SEC, OCIE, FINRA etc.) • **Qualys Vulnerability Scan** • **NIST / HIPAA Assessment** • **Insurance Review**	• Internal Staff • Security Consultant • Audit Firm