

A STEP-BY-STEP METHOD TO SECURING YOUR BUSINESS

Cybersecurity is hard for mid-size businesses. Limited budget, lack of qualified resources, too many products and services to choose from are some of the reasons why security is hard to implement. In this step-by-step guide, we will go through a practical approach on how to secure your business.



Introduction

There is no shortage of bad news in the media. Cybersecurity is a real threat to business of all sizes. Large corporations can throw a lot of money and resources into it, but mid-size companies are at a serious disadvantage. Most mid-size businesses do not have the right resources or budget to tackle the problem. Very often, they don't even know where to start. Having spoken to several mid-sized business owners, I am asked one or more of the same questions by each business owner.

Where do I start?

I have done the following things, is that sufficient? If not, what else must I do.

Which product(s) should I buy?

How do I know if my infrastructure is secure?



As a business owner/leader, your goal is to do everything that is practically and financially feasible for you to protect yourself from malicious actors.

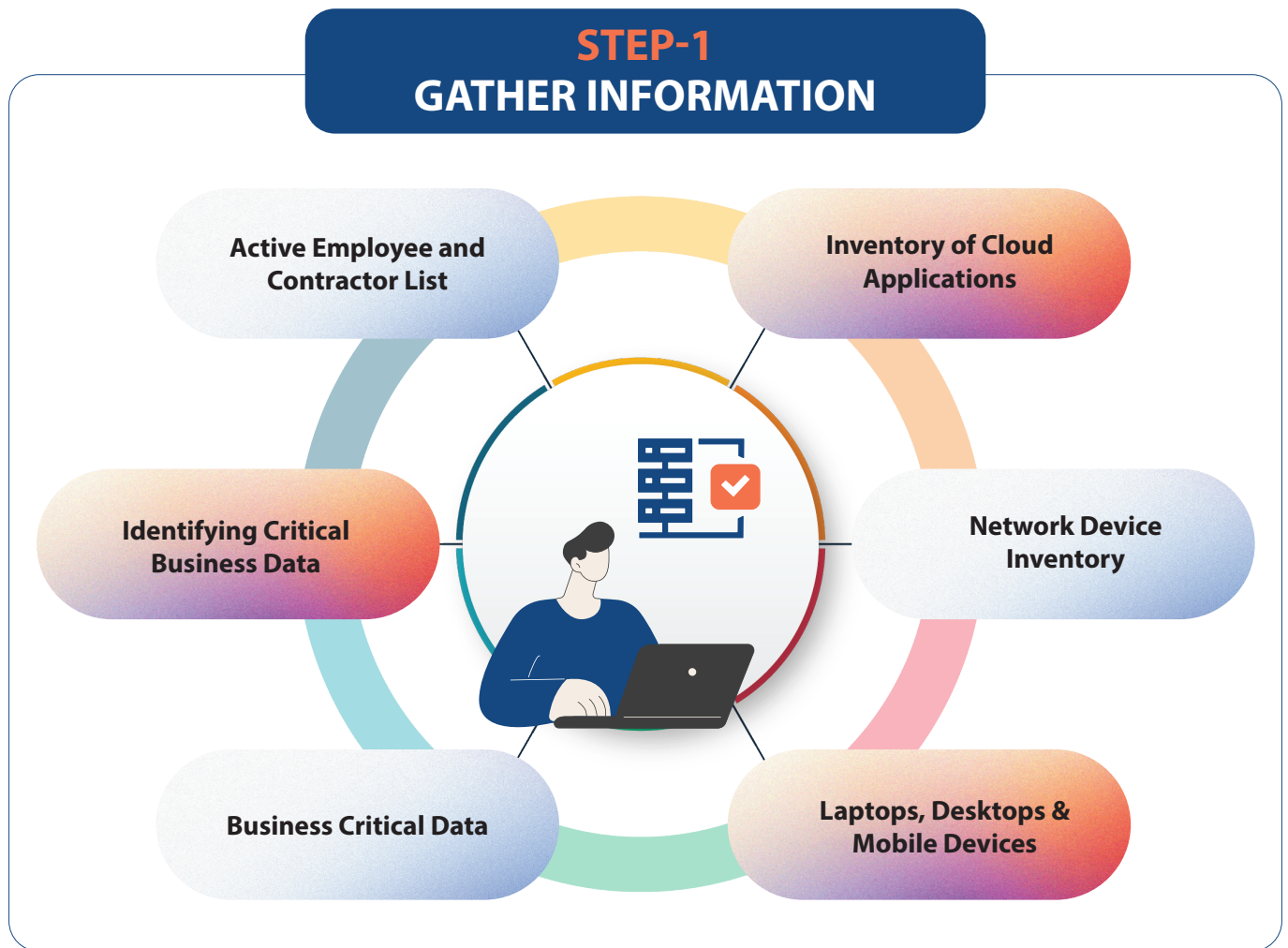
Cybersecurity is a lot like taking care of your health. There are things in your control and there are things outside of your control. If you don't take care of things that are in your control such as eating healthily, exercising and getting good sleep, it will eventually have a negative impact on your health. It could be tomorrow, or it could be a few years from now. But it will certainly happen. Then there are things such as being struck by a drunk driver or an earthquake, which are totally outside of your control. Similarly, in cybersecurity, some things are within your control such as the following:

- Ensuring that an effective anti-malware product is protecting all endpoints,
- Enabling multi-factor authentication for all employees and contractors; and,
- Applying security patch updates in a timely manner.

Then, there are things outside of your control. There could be unknown vulnerabilities in the software products you are using. To address this risk, you can purchase insurance to protect yourself from yet-undiscovered vulnerabilities that are beyond your control. As a business owner/leader, your goal is to do everything that is practically and financially feasible for you to protect yourself from malicious actors. In this e-book I want to put together simple step by step instructions on how to protect your company within your budget. As in the case of taking care of your health, when it comes to protecting against cybersecurity, what you do every day diligently is what matters the most. It's not about buying the most expensive tool and not using it to its potential.

Whether you are at the early stages of your business or you have been in

years of operations this guide will help you get to a secure state methodically. Remember, the goal is to get just enough security for your business needs, nothing more, nothing less.



Step 1: Gather Information.

You can only protect what you know about. If there is a server sitting in your IDF and no one is aware of it, then you certainly are not protecting it. If your employee subscribed to a cloud application and your IT team is not aware of it, it is a risk that you are unaware of.

Your first step is to gather information on the following things.

- Network Device Inventory
- End User Device Inventory
- On-premises and Cloud application inventory
- Active Employee and Contractor List
- Identifying Critical Business Data
- Identify Business Critical Process

Depending on your business size, complexity and workflow, you can either use a paid tool to do this for you, or it can be something as simple as an excel sheet.

Tip 1

Process is more important than the tool. First make your process crystal clear before you invest in a tool. A tool may look nice but may not meet your requirements and process.

For example, if your device inventory is only a couple of hundred devices, you don't necessarily need to purchase any expensive solutions for inventory management. The process is more important than the solutions.

Tip 2

Think about the process on how to maintain the list.



Step 2: Set up Governance

This is the most important task before you start spending money on products and solutions. For mid-size companies this may seem like a daunting task. However, it doesn't need to be. You don't need to write all your security policies from scratch. You can easily use existing policies available freely or for a minimal fee you can get someone to write the policies for you. About 75% of security policies of most companies will be the same. If you follow a certain security standard or are bound by HIPAA, PCI or other such certifications, you may need some additional checks.



A good BCP gives a strategic advantage for business during adverse events because they can be up and running within a certain period of time while their competition without a BCP may be still figuring out how to bring business back to normal condition.

Identify Stake Holders

For mid-size companies the stake holders are usually the CEO, Director of IT, Director or Information Security or similar roles. There could be a few other people, but it is usually not a massive team. The most important piece is identifying who is responsible for what. This will help you respond faster and in a definite way when a security incident happens.

Create Security Policy

A security policy talks about the measures you take to protect the company from cybersecurity and other threats. It does not talk about specific products or configuration. For example, all users accessing company data must use 2 factor authentication. The solution you use can be anything.

Create Data Governance Policy

You have already identified business critical data in Step 1. In this section you will document how you will protect sensitive data. Who is allowed to access it, modify it and destroy it. How will you recover data in case of an accidental deletion.

Create Business Continuity Plan

When covid happened, a lot of companies struggled to continue their business. Companies had not planned for a situation where employees cannot come into the office. This is no different than a natural disaster such as an earthquake or cyclone that makes it difficult to operate in normal office conditions. A well drafted BCP will help companies identify the critical components required to operate the business and how they can continue to do business in case of disruptions caused by events that are outside of their control. A good BCP gives a strategic advantage for business during adverse events because they can be up and running within a certain period of time while their competition without a BCP may be still figuring out how to bring business back to normal condition.

Setup Security Review Meeting

Security review meetings are a critical feedback mechanism. It is like doing your annual health checkup. Your review meetings can be quarterly, half-yearly or annual. But at least one meeting a year is must to do a complete review. Doing review will not only help improve security. Security review can also cut down cost. Review meetings are good time to check when contracts are up for review. What products and services have become redundant. What new business work flows are added and what new threats needs to be addressed.

Setup Incident Management Response

Setting up an incident response process and testing it out is like doing your fire alarm drill at work. It helps you keep your cool and follow the process that is already defined instead of panicking and making more mistakes.

Tip 3

Do not worry about making all your policies perfect in the first iteration. Security is an ongoing thing as you go through your quarterly or annual review you will start making changes to the policy. What is important is having a policy in place so that you can keep improving it.



Step 3: Manage Your Identity

In step 1, you have already gathered your hardware and software inventory. Your next step is to ensure that you have a mechanism in place to protect both. This is where Identity Management comes into play. If you set this up properly, it can take a lot of pain away from your daily operations. Once again, before you go buy that shiny identity solution, follow the steps below and ensure that your requirements are well documented.

Create RBAC Mapping

Create the various roles that your company needs for security. These roles can be Employees, Contractors, Network Operators, Network Administrators, Finance Administrators and so on. In Step 1, if you downloaded the sample template, there is a column for Business Impacting and Sensitive Data. These two fields are useful in deciding what user roles are allowed to do what function. Attached is a simple RBAC mapping you can use.



Unused licenses cost companies thousands of dollars each year. It also causes significant security risk.

Document Onboarding and Offboarding Process

When an employee joins the company, there should be minimal task for the IT department for provisioning all the accounts for this user based on the employee's role in the company. A laptop will be ordered or taken from inventory, imaged to the latest approved image, applications installed, accounts provisioned and handed or shipped to the employee.

Identify Service User Accounts

Service accounts are critical for automation. Wherever possible use API based service accounts for better security. If 2FA can be implemented for service accounts, it must be enabled. Only disable 2FA for service accounts when it is necessary.

Enable 2FA

2FA must be the standard for all applications and devices. If you need an exception, it should only be for applications or devices that are not business critical or do not hold sensitive information.

Prepare for SSO

At this point you will know if your existing identity solution will meet your needs, or you need to have a new identity solution. Your identity solution must help you manage your identity efficiently. It must give you options to automate the onboarding and offboarding of employees. It should automatically put users into the right groups and give them access to applications they need access to.

Implement Enterprise Password Manager

For your network administrators and other employees who manages the accounts for the company, get an enterprise password manager. Not every employee needs a password manager. Only employees who manages multiple accounts require one.

Schedule a Monthly or Quarterly Call to Review Identity

Unused licenses cost companies thousands of dollars each year. It also causes significant security risk. Reviewing the license usage at a reasonable frequency can cut down both cost and security risk. This can be part of your security review meeting.

STEP-4 PROTECT DEVICES



Step 4: Protect Devices

Even though Steps 3, 4 & 5 are listed in that order, the reality is that you will have to go back and forth a few times to do the required tweaking.

In this section we will go over how to protect devices such as laptops, physical servers, IoT devices and other network devices in your environment. Depending on the size and scale of your environment, this section can be very short or can be long. If your company is going with a cloud first approach and has absolutely no on-premises infrastructure, then the only device that you need to protect will be the laptops. But if you have phone systems, physical servers, IoT devices, printers and other network devices, you definitely have some extra work to do.

Install Anti-Malware

Installing an anti-virus/anti-malware solution with Endpoint Protection and Response (EDR), is a mandatory step. You have several solutions to choose from. Make sure you are using a cloud managed solution.

Patch

Unpatched servers are one of the biggest preventable reasons for breaches. Patch everything on a regular basis. You must have a patch chart that you update monthly.



Unpatched servers are one of the biggest preventable reasons for breaches.

Encrypt Hard Disk

Wherever applicable, ensure that all hard disks are encrypted. This protects data in case of a theft or loss of device.

Disable USB Port or Enable Auto-Scan

Depending on the line of business you are in, you can either choose to completely disable the port for all or select employees. At a minimum, you must enable scanning of USB drives for potential malware.

Backup Data

This is your insurance policy against several things. Ransomware, accidental deletion, fire or other natural disasters can put you in a position where you do not have access to the data. Back up and having a BCP in place is your way out of these situations.

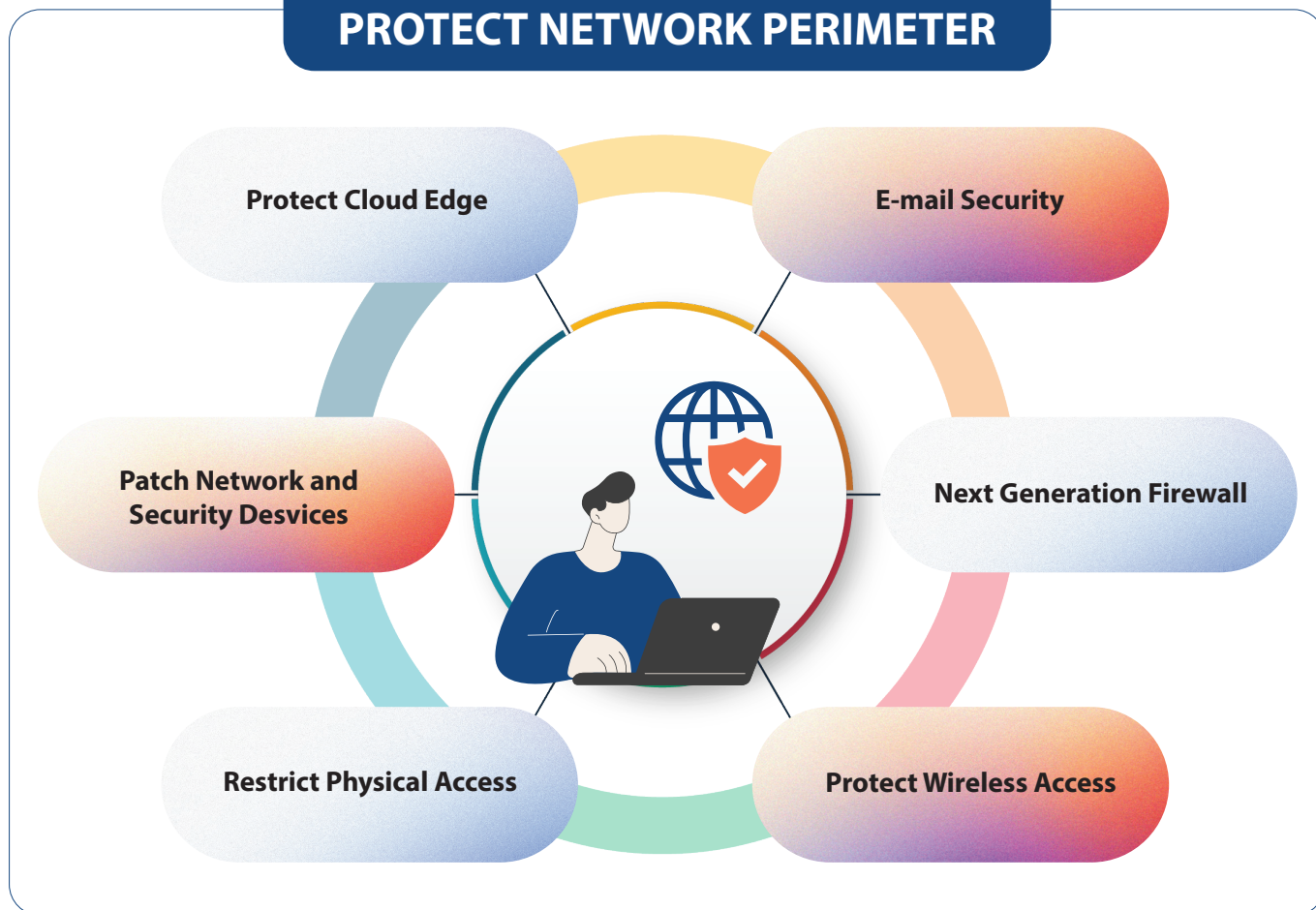
Manage Centrally

With the work force no longer restricted to physical office, central management of devices is important for security and efficiency. You may want to remotely wipe out a laptop that gets stolen. When an employee resigns, you may want to disable the access to their device remotely.

Tip 1

Make it a policy that employees do not store files on the local drive of their laptop. Instead, let them use a cloud-based storage service such as Sharepoint or Onedrive. When an employee loses a laptop, you will not lose valuable data along with it. Anything that is on the shared drive can be easily replicated on to the new laptop.

STEP-5 PROTECT NETWORK PERIMETER



Step 5: Protect Network Perimeter

Life was easy for network and security engineers when employees were restricted to office space. Your firewall protected your network perimeter. Your only exception was VPN users. Those days are long-gone. With most of your services now in the cloud, your network perimeter cannot simply be a firewall anymore. You need a virtual perimeter to protect your cloud applications. This is where Secure Access Service Edge (SASE) matters.

Implement E-mail Security Solution

E-mail is the biggest hole in your network perimeter. Someone sitting remotely in the corner of the world can send you a malicious file via e-mail. Without an e-mail security solution, you are a sitting duck for the bad actors.

Implement Next Generation Firewall

Traditional firewall has limitations. A next generation firewall is the minimum requirement in today's threat landscape.

Protect Wireless Network

Are you still using a pre-shared key for your employee wireless network. You absolutely do not want to use a pre-shared key for corporate wireless network. Migrate to EAP-TLS if you want proper protection for your wireless network.



With most of your services now in the cloud, your network perimeter cannot simply be a firewall anymore. You need a virtual perimeter to protect your cloud applications. This is where Secure Access Service Edge (SASE) matters.

Protect Cloud Edge

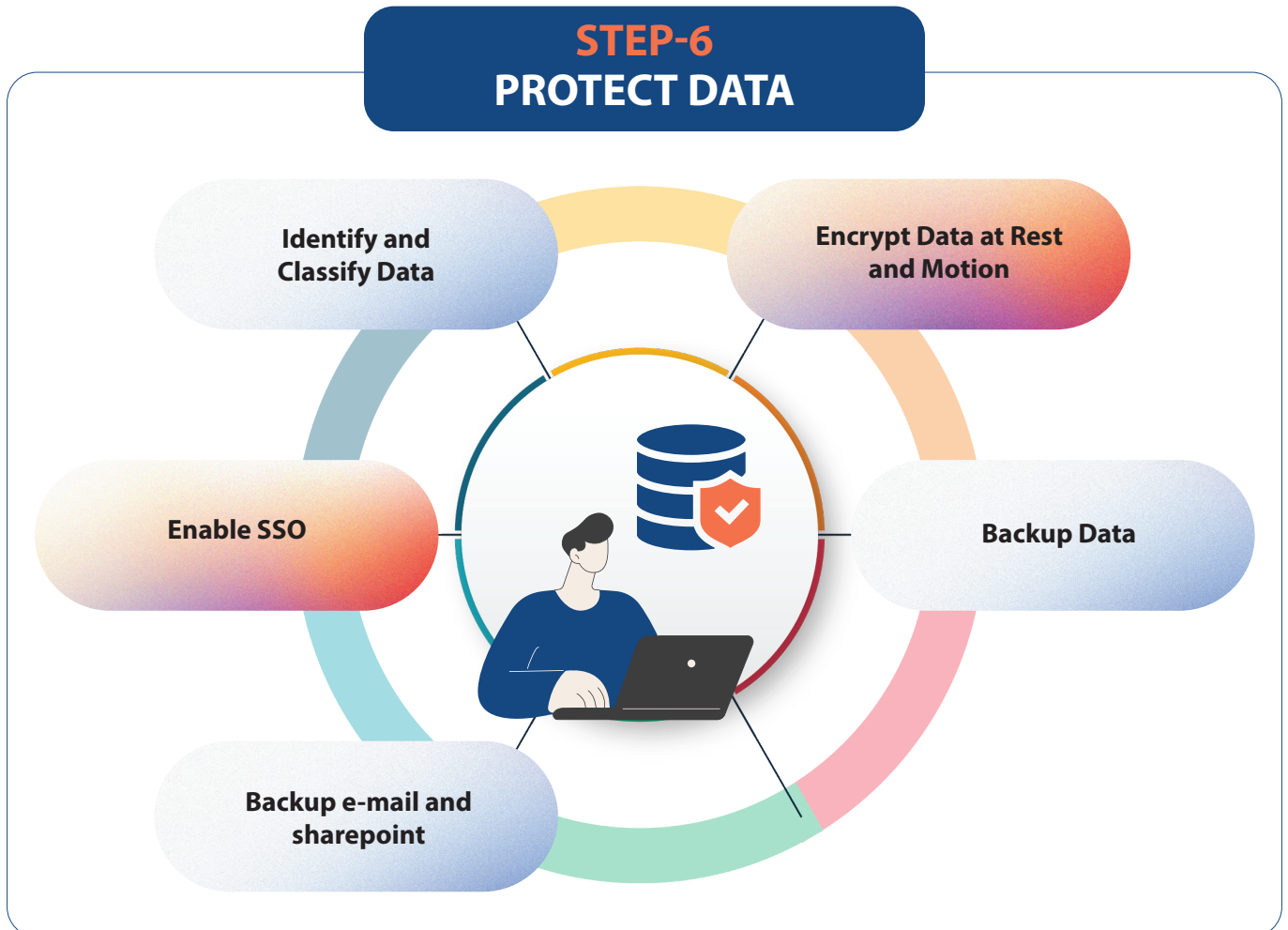
Do you know who is remotely trying to break into your office365 or salesforce account? You can be assured that enough people are trying to do this. You have almost zero visibility into this today. Cloud is Secure is the wrong mantra.

Implement Secure Web Gateway

Prevent your employees who love dogs from clicking on that well placed discount coupon for dog food and accidentally downloading malware. Thanks to social media, bad actors know what your employees love and want. E-mails are a lot more targeted. Implementing a Secure Web Gateway can add protection from these. Patch Network and Security Devices This is a repetition. Just calling it out again for network and security devices.

Restrict Physical Access

Even if you are small company, just don't give chances for people to wander into the server room. It is common sense approach.





Most of the bad actors are after your data. The more valuable your data, the more you protection you need to put in.

Step 6: Protect the Data

Most of the bad actors are after your data. The more valuable your data, the more you protection you need to put in. If are in a regulated industry, you will have additional mandated requirements. Irrespective of that, it is a good idea to protect data.

Identify and Classify Data

The first step to protecting data is to identify the data you have and classify it to respective buckets. Often times, businesses ignore data that is in the plain sight. For example, your e-mail and attachments in it can contain sensitive data. A printed document lying on the printer can be sensitive data. Your SharePoint or file server could be containing tremendous amount of sensitive data. Unless your data is structured, you may need a software solution to classify data.

Role Based Access Control for Data Access

Once you do the classification, the next step is to put the necessary controls on who can access or modify data. The RBAC sheet you created in Step 3 will be your guideline. Encrypt Data and Rest and Motion The title itself speaks for what needs to be done in this section.

Backup Data

This step is already covered in Step 4. But you may have found out additional data that was considered earlier.

Back up E-mail and SharePoint

Some of you may be thinking why there is a separate section for e-mail and SharePoint back up. There is a misconception that e-mail, and SharePoint are automatically backed up since it is a cloud service. The reality is that all e-mails and SharePoint files can only be recovered for 30 days if someone accidentally or intentionally delete. More than once have we run into situations where e-mails and SharePoint files were deleted and could not be recovered. It is easier to back up than get a lawyer involved.

STEP-7 MONITORING AND TESTING



Step 7: Monitor, Test and Train Employees

If you have diligently followed Step 1 through 6, then you have a few solutions in place and dashboards to look at. But how do you know if your business is secure. This is where vulnerability scanning, and penetration testing comes into picture.

Perform Vulnerability Scanning

Vulnerability Scanning identifies known vulnerabilities in the software and hardware in your environment. There are thousands of known vulnerabilities in various systems used by businesses. It is not possible to manually look at each one of your systems and see if it has a vulnerability. A vulnerability scanner automatically scans your network, identifies the systems, performs checks to see if there is any known vulnerability in any of your systems. Perform vulnerability scanning every quarter or these days you can have vulnerability scanning as service where they continuously scan your environment.

Perform Penetration Testing

With penetration testing you are allowing a security engineer to find ways to break into your network. He/she gathers information that is publicly available or provided by you to see if there are holes in your network that can be exploited.



You can spend hundreds of thousands of dollars buying great security software. But if you are not monitoring it on a daily basis, you will eventually pay the price for this.

Monitor Your System

This is the most important bullet in this entire series. You can spend hundreds of thousands of dollars buying great security software. But if you are not monitoring it on a daily basis, you will eventually pay the price for this. You have to continuously monitor the system to understand what is happening. You will have to make necessary tweaks so that your security solution is not disrupting the business.

Provide Cyber Security Training to Your Employees


Phishing attacks are one of the biggest cause of breaches. Doesn't matter how much protection you put in, your employees can be a victim of social engineering. They can click on links share through other medium than e-mail. They can share sensitive information without realizing the consequences. Training on cyber security must be provided to every employee.

Purchase Cybersecurity Insurance

Just like your health and safety, there are things outside of your control in cybersecurity. A software that you purchased may have an unknown vulnerability. An employee may fall for a social engineering hack. This is where cybersecurity insurance will come into picture.

Back up E-mail and SharePoint

Some of you may be thinking why there is a separate section for e-mail and SharePoint back up. There is a misconception that e-mail, and SharePoint are automatically backed up since it is a cloud service. The reality is that all e-mails and SharePoint files can only be recovered for 30 days if someone accidentally or intentionally delete. More than once have we run into situations where e-mails and SharePoint files were deleted and could not be recovered. It is easier to back up than get a lawyer involved.



BEYOND STEP 7

If you have managed to implement step 1 through 7 successfully, you are in a better shape than most of the businesses. These steps are a very pragmatic approach to security without throwing in any particular, product, standard or other jargons.

Every business is unique. Depending on the line of business you are in, you will have to make some adjustments or bring in additional services and products to meet the security needs of the business. For example, if you are in healthcare; you will be required to adhere to HIPPA. Data governance and Data Loss Prevention may be of higher importance for your business. Your Data Loss Prevention solution needs to more comprehensive.

Continuous Evaluation of Security Needs

Security threat is never static. The malicious actors are always finding new ways to break in and steal information. Many of the security products in the market today were developed in the last 3 to 5 years. For example, SASE and SSE was only coined by Gartner in 2019. Today any company with a cloud presence and remote work force cannot be considered secure without SASE and SSE.

We don't know what the new threat will be coming in the following days. Security needs must be evaluated on a regular basis. At a minimum, an annual review must be conducted. This will prepare you to stay ahead of the game and not end up with nasty surprises.



Headquarters

111 Lindbergh Avenue, Suite F, Livermore, CA 94551

Technology Hub

18, 4th 'C' Cross, 1st, Main Road, Koramangala Industrial Layout, 5th Block,
Bengaluru, Karnataka 560095

Contact

Phone: 1-925-233-3366

E-mail: sales@consltek.com | <https://www.consltek.com>