THE TOP 10 THINGS YOUR BUSINESS CAN DO FOR CYBERSECURITY

Like it or not, cyber regulations are here to stay, but they're excellent for business. Follow Jerry as we count down the top 10 things you can do to improve cybersecurity. Then plan for next steps with our interactive tool, found at SynchroNet.net/10Things.

SynchroNet

SynchroNet.net

THE TOP 10 THINGS YOUR BUSINESS CAN DO FOR CYBERSECURITY

Meet Jerry, SynchroNet's CEO: your guide and expert IT partner. Jerry's going to count down the top 10 things you can do to improve your cybersecurity.

At the end of this countdown, you'll be ready to fill in your personalized planning worksheet to prioritize action items. If you have any questions, ask Jerry at AskJerry@SynchroNet.net.

IN THIS GUIDE, YOU'LL LEARN:

- How to prioritize the highest value initiatives that will improve your cybersecurity.
- What key technical terms mean in plain English so that you know what you need and why.
- Why taking action is essential, even though cybersecurity can be daunting.
- What other resources are available for you from SynchroNet.

WE ARE GATHERED HERE TODAY TO...

Yes, we're here for a reason. We want to wrap our minds around what we need to do to be more cybersecurity savvy.

Did you know that 99.9% of American Businesses fall into the Small Business Administration's definition of an SMB (small or medium-sized business)?* These organizations – from sole proprietorships to mom-and-pop shops to steadily growing enterprises with 10, 20, 50, 100, even 500 employees – employ almost 50% of the US workforce.

With so much invested by so many entrepreneurs, it's no wonder that states like California, New York, Connecticut, and others are legislating that businesses take steps to protect their organizations from exploitation by cybercriminals. But each law has exceptions, vague language, and only shows its teeth after a breach has occurred.

As a result, many SMBs aren't sure how to fully comply or whether to even try. Some fatalistically say they'll deal with next steps if or when they face a breach. Others question their ability to achieve these laws' ultimate goals: to be safer online as they do business in a connected world.

Well, we're here to tell you three things:

1. A breach is NOT inevitable if you take reasonable precautions, even though cybercriminals continue to demonstrate their proficiency, ingenuity, and diligence in parting people and companies from their hard-earned dollars.
2. Taking any of the steps in this guide helps. Taking all of the steps helps the most. Whatever you can do to follow cybersecurity best practices will only help you. Do what you can, and keep adding extra security measures when possible.
3. Cybersecurity regulations exist for your protection. And ours. And theirs. And everyone's. They are intelligent, realistic, and achievable – even on limited budgets.

*Source: U.S. Census Bureau, 2020

#10 SECURE YOUR FIREWALL & WI-FI

Change the username and password on your firewall. Then secure your primary Wi-Fi. These steps accomplish different things and are essential:

- Securing your firewall makes it harder for criminals to hack into your network.
- Changing your Wi-Fi password means only authorized users can use your network & access your corporate files and applications.

STEP 1: CHANGE THE FIREWALL'S DEFAULT SETTINGS

Follow Jerry's advice: First, address your firewall, which likely came with factory-set credentials (which are also posted online).

- Ensure your firewall is not using default settings.
- Set a strong username and password combination (see #9 in our countdown for more details).
- Document the new credentials in your secure, online password vault. You do have one, right??

STEP 2: CHANGE YOUR WI-FI PASSWORD

Next, lock all non-employees out of your corporate Wi-Fi by changing the username and password regularly (perhaps annually).

If necessary, set up a guest Wi-Fi account where local network access is disabled. Reap an added benefit: former employees won't have your new credentials either.

#9 DECIDE WHO GETS TO SEE WHAT

STEP 1: TAKE BACK THE KEYS TO THE KINGDOM

It makes sense to give a housekey to a responsible teenager but not to the four-year-old. Similarly, giving an employee access to specific files, folders, and even applications should be based on their responsibilities.

Only give employees access to the files, folders, and applications they need to do their jobs. Nothing else.

Restricting unauthorized access to sensitive information through role-based permissions is called "*access controls*." This user management policy grants (or denies) authenticated users' access to specific resources.

Access controls limit risk, and you can easily remove permissions as needed.

Follow Jerry's suggestion by matching roles to access privileges within your organization. Then assign users to those roles to systematically restrict confidential data.

Now that you've got users' access privileges organized, further secure your data by ensuring that all laptops and workstations are adequately protected. How do you do that? Two words: STRONG. PASSWORDS.

STEP 2: ESTABLISH A STRONG PASSWORD POLICY

Require users to set new strong passwords on their PCs and laptops. Each password must be unique (as in, used once, and only once, no matter what) and should follow these principles:

1. At least 12 characters long.
2. Include UPPER and lower case.
3. Include special ^%$*! characters.

Combinations of simple words, like Sky_seriesGo#12 or RedTroll=8*7, are simultaneously hard to crack and easy to remember. (Versus 8@rL`J^qwj!2Q]=V; have fun with that one.)

#8 WRITE YOUR POLICIES DOWN

Your organization needs policies in place to protect sensitive information. These policies aren't just a To-Do to check off your list and forget. They are living documents that include vetted and approved guidelines, schedules, accountabilities, and step-by-step procedures to address the *who-what-where-when and how* of cybersecurity.

Your policies form the backbone of your overall "Cybersecurity Program," which answers the critical *why* behind all cybersecurity regulations:

- WHY define how you'll manage your technology, people, access, and controls?

HERE'S YOUR LIST OF POLICIES

At a minimum, we advise you to include the following essential (or recommended**) policies in your Cybersecurity Program documentation.

These policies should not come from your IT department but rather from your business development department/leadership team with guidance from your legal team and input from your IT team.

1. Access Controls and Identity Management Policy
2. Asset Inventory and Device Management**
3. Business Continuity and Disaster Recovery Planning Policy
4. Customer Data Privacy Policy
5. Data Governance and Classification Policy**
6. Incident Response Policy
7. Information Security Policy
8. Physical Security and Environmental Controls Policy
9. Risk Assessment Policy
10. Systems and Application Development and Quality Assurance Policy (** if applicable)
11. Systems and Network Monitoring Policy**
12. Systems and Network Security Policy
13. Systems Operations and Availability Concerns Policy**
14. Vendor/3rd-Party Service Provider Management Policy

This list comes from the requirements of the 23 NYCRR 500, a robust cybersecurity law affecting businesses overseen by the New York Department of Financial Services. It's the gold standard of state-mandated cybersecurity regulations.

Before you say, "*Ha, I'm not accountable to the NY DFS; I'm freeeeee,*" did someone (i.e., Jerry) say, "NY SHIELD Law?" If you don't know what that is, assume this list is your problem.

Feeling overwhelmed? Email me at AskJerry@SynchroNet.net to receive our *Cybersecurity Program Policy Definitions*, which explains what each policy is and gives advice on writing it.

#7 TRAIN YOUR PEOPLE

Hold your employees accountable. Make it a goal to:

1. Conduct regular training – at least monthly – so that employees:
   - Can quickly and accurately identify phishing and spear-phishing emails and know what to do in an emergency.
   - Are empowered to recognize and rebuff social engineering tactics.
   - Understand the fundamentals of cybersecurity, like how to:
     - Safely use public Wi-Fi.
     - Avoid the traps of removable media.
     - Improve data security when accessing the corporate network remotely.
     - Create secure passwords (and NEVER reuse them)
     - Minimize the risks of regular Internet and Email usage to complete tasks for work.
2. Distribute an electronic copy of your Cybersecurity Program documentation to each employee – and then show them how they fit into your business' cybersecurity efforts! They need to understand:
   - Your Acceptable Use Policy (which is part of your Information Security Policy, right?).
   - Your Business Continuity/Disaster Recovery Plan.
     - What constitutes an emergency?
     - How does someone report an issue, like an outage or a potential breach?
     - What is the step-by-step plan?
   - What's in your Incident Response Plan and how to use it.
     - Run a live simulation to see how your team does; you may realize they need extra training.

#6 UP YOUR EMAIL GAME

STEP 1: FILTER YOUR EMAIL

Install the best email filter possible, ideally a professionally managed, enterprise-level filter that scans inbound AND outbound email for viruses, malware, and many other threats.

If you think your team can deal with spam email themselves, remember that 48% of all email traffic is spam. How many of those spam emails have ransomware, trojans, viruses, malware, or other creative scams in them? (If only they'd use their powers for good... Those jokers are no joke.) And how many can you afford for your busy executive team or staff to accidentally open or execute?

The tragedy is that the best email filter in the world still won't catch every possible threat. That's why #7 in this list is so essential:

> Training is your ticket to a more secure environment. How can you avoid the danger if you don't know how to recognize it?

STEP 2: DETERMINE WHO NEEDS TO USE ENCRYPTION

A robust enterprise-level email filter may have mission-critical add-ons, like encryption. Encryption enables certain users to securely share protected information to conduct business (i.e., patient health records, financial statements, legal documents, human resources records, intellectual property, etc.).

#5 BACK UP YOUR DATA

Establish a schedule for backing up your data. Backups should be:

1. Complete

How much data can you afford to lose? We assume your answer is, *"Not very much."*

- Use a schedule that includes a plan for your backup versions in the Cloud. Ensure you have a backup version for:
  - Each day, each week, and each month
- Retain these versions for one year.

Don't just back up files; back up applications, settings, etc., so that if you need to restore from a specific point, you'll have *everything* you need to get back to work.

2. Unaffected

Your backup needs to avoid ransomware and viruses (so, it's either in the Cloud or not attached to your network where it could be infected). *"Not attached,"* you say? Well, not for long, anyway! Connecting your backup device only *during* the backup process is inconvenient. That's why most backups are to the Cloud.

3. Secure and Encrypted

Who has access to your backups? The list should be short, well-documented, and connected to the point people tied to your business continuity/disaster recovery plan. Contact information should be current and at your fingertips, so you can easily reach the team in an emergency.

4. Both Local and Offsite

Mayhem is all around us, so take it from Jerry:

An offsite backup reduces your risk and means your business continuity plan remains intact. (Even if your server is abducted by aliens, flooded, burned, meteored, snowed in, vandalized, or … worse.)

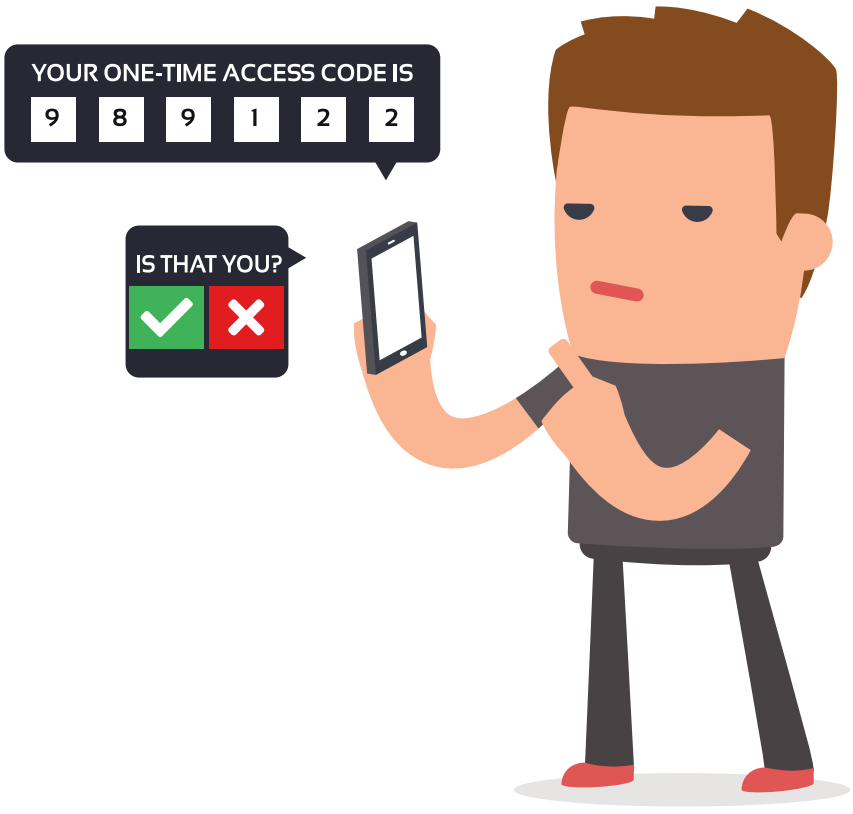
#4 VERIFY ACCESS TO THE BIG STUFF 2X

Two-factor or multi-factor authentication (2FA or MFA) adds additional layers of protection to the critical applications that house protected data. It may mean an added expense, but it's worth it!

1. A user must first log in with an accurate username/password combination.
2. The user then verifies their identity by providing a code or clicking an emailed verification link, etc.

This extra verification step ensures that only authorized users with access to controlled data sources (like their cell phones or email accounts) may successfully log in.

MFA is more secure than 2FA because you have additional verification points than just a text message, which can be spoofed. But overall, 2FA is better than ØFA (as in, better than nothing). All critical systems should have 2FA or MFA engaged.



#3 PREVENT AND DETECT MALWARE

The era of buying a boxed Anti-virus/Anti-malware (collectively called "AV") from Best Buy is over. Threats have grown so sophisticated that your best bet is to have a professionally managed enterprise-level AV with endpoint detection and response (called "EDR"). What does this mean?

1. Endpoints are users or devices (like PCs, Laptops, Phones, Servers) that connect to the network. Users, i.e., your executive team, HR, sales, accounting, and other team members, are using email, web browsers, and files.
   - Users are also using apps, clicking on URLs, and regularly dealing with email/browser-based advertisements, pop-ups, and more.
2. An enterprise-level AV program with EDR uses real-time threat intelligence to protect users from the perils of regular activity.
   - AV programs work by preventing and or detecting the presence of potential malware – like computer viruses, trojans, or ransomware – before they can penetrate and infect a device.
3. An AV is *not* a firewall. It does not replace a firewall.
   - Instead, AV delivers a crucial protective layer at the user level to catch the malicious threats that might otherwise sneak in.

To be effective, an AV with EDR needs to be installed *on every endpoint device.*

No workstation, laptop, desktop, server (etc. & etc.) left behind!

#2 SUPERCHARGE YOUR FIREWALL

We put fences up to make it harder for intruders to access our homes and properties. Well, networks need fences, too. A firewall is that fence.

A firewall is hardware or software that:

1. Blocks unauthorized access to your network.
2. Permits legitimate communications and activities, as if through a gate in the fence.

Blocking unauthorized access is relatively easy. It's much harder to find illicit activity dressed in proper authorizations (as in, a wolf in sheep's clothing). For instance, a firewall *can't*:

- Identify when an authorized user sends protected information due to a phishing scheme (this is bad).
- Tell when a flaw within an approved application is exploited by a cybercriminal, opening a tunnel into your network (this is worse).

Since a firewall can't prevent either of these scenarios (and many others), you need to implement a firewall with an Intrusion Detection System ("IDS") and traffic filtering. An IDS gives your firewall more 'eyes', the same way a couple of security cameras give security guards more visibility into space around the gate. Traffic filtering enables you to "Always Block" Web content from unsafe or inappropriate sites.

An IDS inspects all inbound and outbound network activity. It can't *block* harmful traffic, but it can *alert* your IT security administrators of any intrusion attempts or suspicious activity patterns that may indicate an attack on the network. Then your IT professionals can take steps to harden your network.

A firewall supercharged with an IDS is a valuable piece of defensive architecture to help you better spot the bad guys.

#1 TAKE A DEEP BREATH AND DIVE IN

We've reached the most crucial step of all in this countdown: Take a deep breath and dive in. Do this by:

1. Fill out the planning worksheet to help you prioritize your weak areas to close the gaps. Find it at SynchroNet.net/10Things.

2. Create a structure to manage your Cybersecurity Program (including the key areas presented in this Top 10 Guide for SMBs.
   - Most organizations deputize a leader or executive to serve as the Chief Information Security Officer ("CISO"), whose role is to oversee the program and ensure critical protections are in place.

3. Inspect what you expect.
   - Want your team to follow your Cybersecurity Program?
     - Then test their understanding of your program policies (#8) through ongoing training and live incident response/disaster recovery simulations (#7).
   - Want your network to be safe?
     - Then follow up with your IT support staff to double-check your network security (#10), access controls (#9), email filters (#6), 2FA/MFA (#4), anti-virus with EDR (#3), firewall configuration (#2), etc.
   - Want to overcome a ransomware attack or natural disaster quickly?
     - Then inspect your backup policies (#5) and test whether your entire team knows what to do in an emergency (#7 again).

4. Don't assume all the risk.
   - Procure sufficient cyber liability insurance to protect your business. Your coverage needs depend on the sensitivity of the data used in your organization and industry.
   - Only work with vendors who also prioritize cybersecurity.

IT'S TIME TO GET STARTED

BUT WAIT, THERE'S MORE...

You likely noticed the reference to the NY SHIELD Law in #8. If you want to know more about what NY SHIELD means for your business, we've created more than a dozen free resources just for you. They are available at SynchroNet.net/SHIELD.

Importantly, if you work through this Top 10 Guide for small and medium-sized businesses, you'll be well on the road to NY SHIELD compliance. (That's no coincidence either. At SynchroNet, we're hyperfocused on your success. You're welcome.)

Questions or Comments?

1800 N America Drive, West Seneca, NY 14224
SynchroNet.net | 716-677-2677 | AskJerry@SynchroNet.net