DEFENDIFY®
All-In-One Cybersecurity

QuickStart Guide
to Preventing Cyberattacks

DEFENDIFY®

We know you're here for the "How" but as every good guide should, we can't help but start with a little bit of "Why."

That said, feel free to skip ahead—we won't tell anybody!

Want 3 free tools to get started?
Get the Essentials Package

As easy as ABC.

We developed this *QuickStart Guide to Preventing Cyberattacks* to help you get your cybersecurity program off the ground and to assist you with the fundamentals of cybersecurity, many of which are so often misunderstood and misconstrued. To make it easy for you and anyone inside your organization, we use straight talk, not tech talk.

There are a lot of ways organizations realize they need to improve their cybersecurity:

- For some, it's simply the constant barrage of cyber incidents showcased in the media every day—we just can't seem to get away from it, can we?
- For others it might be the C-Suite or Board of Directors abruptly raising the hot button issue—and their eyebrows as they realize what's at stake.
- For many, it's the moment when that unexpected cybersecurity questionnaire lands on their desk—straight from their best customer or partner.
- And we certainly can't forget about good ole' compliancy, it can come in many shapes and sizes—government, insurance, and industry regulations abound.

Whatever the case, there is no question: cybersecurity has become a household conversation and an essential part of every organization's operation.

The challenge is, cybersecurity can be complicated with a lot of moving parts.

Whether we like it or not, cybersecurity is about much, much more than quick software you might install on your computer. The reality is, there is no silver bullet, and cybersecurity requires multiple layers of defense:

- Assessments and Testing
- Policies and Training
- Detection and Response

And of course, every organization is different; in practice, employee count, IT infrastructure, and team skillsets. Which makes getting a cybersecurity program off the ground feel like an uphill battle. Especially when most can't truly afford to have a full-time, dedicated cybersecurity expert on staff (they're almost impossible to find, not to mention prohibitively expensive).

So, cybersecurity often takes a back seat. But it doesn't have to.

It's true, cybersecurity has traditionally been an enterprise thing. Good gracious, some banks spend over $500 million a year and staff over 3,000 IT security professionals! Indeed, that level of security is out of reach for the vast majority. But in comparison, most organizations don't have thousands of employees with computers and servers located in countries all over the world to protect. The good news is, the same level of cybersecurity is not necessary. Think back to those banks—you wouldn't ever consider installing the state-of-the-art surveillance system they would, right? But you can certainly do better—everyone can and should. And you don't need an army, or a PhD, behind you to do it.

A is for Assessment

A is the first letter in the alphabet, and the first letter in Assessment…
your first step in your cybersecurity improvement process. Before you start buying and deploying the next fancy security software for your new laptops or servers, you need to begin by conducting an overarching review of all aspects of your cybersecurity posture by performing cybersecurity assessments.

Cybersecurity Risk Assessment

A checkup without a stethoscope.

There are lots of clichés for describing this, so just for fun we're going to go ahead and use one: Just like you go to the doctor and get a full physical, you should do the same thing with your company's cybersecurity.

Most cybersecurity risk assessments will follow a questionnaire process based a standardized checklist of controls you compare against. You might think control frameworks (i.e. from NIST, CIS) were designed only for industry compliance requirements and intended for the big banks and DOD contractors of the world. While that may have been the case in the past, they are now being used by organizations of all sizes in all sectors.

You can perform a cybersecurity risk assessment and self-assessment today yourself, or hire an outside company to conduct one for you. The result should be a report that outlines where you have strengths and weaknesses.

A good assessment report should also include remediation steps that provide guidance on how to begin resolving weaknesses. An overall score or grade can also be included, quickly identifying where you stand. Perhaps you scored a C-. Your goal can now be to move your organization to a B and then onto an A. With the report and score in-hand, you will be able to identify where to begin, where to budget first, and how to assemble an improvement plan accordingly.

WHAT'S THE FREQUENCY?

At least annually, if not more. And always when major changes are made to the network, environment, and/or IT infrastructure.

Vulnerability Scanning

This is not a test of your personality.

Cyber criminals use their own tools to identify vulnerabilities in your IT resources that they can exploit. These might exist on your computers, printers, security cameras, or software applications used by your teams today. They can even exist on various other unsuspecting Wi-Fi connected devices like the company coffee machine.

Once brought to the attention of the manufacturer, they usually fix the vulnerabilities with patches and updates. However, it's important to remember you may need to proactively apply those patches and updates to your systems and you need to try and do so before an attacker exploits them.

A good vulnerability management program will include the use of a vulnerability scanner. These scanning tools can scan internal and external networks as well as websites and web applications, actively hunting for security vulnerabilities on your behalf. Once detected, you'll get notified and will be able to prioritize remediation based on severity—thankfully some of the better tools will group findings for you. There may be many, and you may not be able to get to them all right away. So, start with the critical ones first, then move through lower severity level ones next. Quality vulnerability scanners will also provide you key knowledge and advice to remediate each of the vulnerabilities discovered to help make the job easier.

WHAT'S THE FREQUENCY?

Ongoing, at least monthly, no less than quarterly.

Penetration Testing

If they push on the door, can they get in?

Hey, not all hackers do bad stuff. In fact, many of them are not only good people but very good hackers. You can even hire them to try and infiltrate your systems (i.e. a penetration test) just like the bad hackers might, and then provide you with a report of their findings. Ethical hacking is a cybersecurity testing technique that is standardized, approved, and recommended. And everyone should consider doing it.

The first step with penetration testing is scoping the work. Since many have never done one before, it often starts with an external network test. Basically, this is a test from outside your network to see if there is any exploitable point of entry into your network.

By simply providing your IP address, the external test can be conducted (by humans!) using technology tools and techniques that go well beyond what you might see with automated vulnerability scanning. The result is a professionally prepared report showcasing findings along with a risk rating and remediation recommendations.

WHAT'S THE FREQUENCY?

At least annually, if not semi-annually. And potentially when major changes are made to the network, environment, and/or IT infrastructure.

Compromised Password Scanner

Hello, is any password out there?

Follow recent reports of major breaches and you will realize that criminal attackers often obtain passwords as a big part of their thieving activities. This is really bad news as it is estimated that a majority of employees use the same passwords (a.k.a. password recycling) for all of their accounts, including their personal ones which can result in a domino effect once in the hands of criminals.

Stolen credentials can provide criminals substantial financial incentive as they then sell them through the underground marketplaces in the Dark Web. They pawn them to buyers who will then use them to hack into accounts and conduct further crimes. Remember, since one user's passwords might open many website doors (such as your financial system or your document storage solution), these passwords can have a significant value in the criminal marketplace.

Stolen password scanning gives you the ability to detect if employee passwords are found in the Dark Web. When a scan completes and an employee's credentials are found, it's time to have that user change their password on all accounts, as soon as possible.

WHAT'S THE FREQUENCY?

Ongoing, at least monthly, no less than quarterly.

B is for Baseline

Plans, Policies, and Procedures…What fun!
This is the category that makes most people sigh out a loud—and we're not talking about a sigh of relief here.

While it might not be the most exciting part of cybersecurity, it is without a doubt a key aspect of every good cybersecurity program. Getting a proper baseline of documentation in place can truly help solidify your cybersecurity posture and operations.

Technology Acceptable Use Policy

The “please do” and “please don’t” for your employees.

Some people’s cybersecurity hygiene is downright awful.To their defense, most have never been trained on cybersecurity or have ever cared about how they use their computer and mobile phones. Who’s going to hack me? This mindset will follow employees in and around your organization, so get in front of them and set the guidelines.

A technology and data use policy should explain in detail to the employee how they are expected to use company devices, passwords, and technology, including best practices like how to store and share files. This can extend to include treatment of personal devices on company networks (we’ve all heard of BYOB, but there’s a new acronym in town: BYOD is for Bring Your Own Device).

It’s important your policy be written using simple terms and natural language (think straight talk, not tech talk) so that everyone can easily understand expectations.

Once developed, use it is an educational tool. Each and every employee should be trained to the policy. And in doing so, just like we did at the beginning of this guide, remember to highlight the “Why” behind what is being shared—it will improve morale, understanding, and enforcement. For example:

“As we just reviewed in the policy, please do not connect your personal phone to our company network…BECAUSE, your device does not have the same technology protection as what we have installed on our company devices.”

Once trained, have your users sign off on the document ensuring their understanding and acceptance.

WHAT’S THE FREQUENCY?

Review, update, and train to it at least annually and any time a new employee joins the team.

Cyber Incident Response Plan

Every good scout is prepared for what might happen.

Preparing for an incident is not only a great way to walk the woods, but also to navigate cybersecurity. Even with an amazing cybersecurity program in place, it's still possible an incident can occur. Having a decisive plan ready to go can save your company significant time, effort, and dollars, perhaps even the company itself.

Your plan should include how to deal with things like a breach of sensitive data, ransomware, and even a lost company computer. It should have a clear step-by-step approach to rectify the situation detailing who will conduct specific tasks as needed. That means names, roles, and responsibilities so that you can act fast and effectively if a situation presents itself.

Remember to review the plan as a team to ensure everyone knows their roles and responsibilities in the unfortunate case of a cyber incident.

WHAT'S THE FREQUENCY?

Review and update at least annually and always when there are key personnel changes to anyone enlisted in the plan.

C is for Culture

It’s time we all join the Cybersecurity Culture Club! Since your users are on the front line, you absolutely must include them in your cyber defense strategy. They are the ones who receive the emails, have valid access to your sensitive data, and can make or break a cyber incident. Your loyal following can be one of your best defenses…everyone a cyber-defender!

Phishing Simulations

A catch and release strategy for your employees.

Here's the reality: Your email filter doesn't stop all malicious emails. Criminals are constantly upping their game to get their emails to your employees' inbox. Unfortunately, they're pretty good at it and reports show that a large number of attacks start with a phishing email. Some of these emails are tricky with files or malicious links built into them. As an example, others leverage pretexting (i.e. gathering information, fabricating stories, social engineering at it's best) with the attacker impersonating the company CEO asking for the employee to send a file.

Employees are working quickly, and with many now working from home, there has never been more distractions. Training your employees on how to slow down and be able to identify email-based attacks is an essential preventative measure that everyone must undertake. Phishing simulation tools enable you to send your own phishing emails to your employees. They come in a variety of designs, just about anything and everything you can think of. A few common examples include:

- Notices from IRS (i.e. "your tax refund is here"),
- Requests from the IT team (i.e. "please update your password"),
- Alerts from delivery services (i.e. "your package is on its way, here's your tracking number"),
- Social media requests (i.e. "let's connect, we have 4 contacts in common")

A phishing simulation tool can provide you reports on how your team is doing over the year and identify repeat offenders so that you can focus further training towards them.

When an employee receives the email, they have two options: (1) take the bait and interact with the email, or, (2) identify it as fraudulent, flag/delete/move on. If they do act like that hungry fish and strike the bait, they will be presented with training (usually a quick tidbit, video, and/or quiz) that will help them understand how to do better next time.

WHAT'S THE FREQUENCY?

Ongoing, at least monthly, but not weekly, and no less than quarterly.

Cybersecurity Awareness Videos

Kind of like Netflix for Cybersecurity.

They say it takes 10,000 hours to master a skill, unfortunately there are not enough hours in the day to make all your users cybersecurity pros. But you can still help them get better with a model of continuous improvement.

Once-a-year cybersecurity training for all your employees can be helpful, but 365 days is a long time before the next one. Take some tips from the construction industry: they do regular “toolbox safety talks” throughout the year to keep safety top of mind and you can follow a similar cadence for your cyber training.

Let’s get serious, nobody is going to pay attention to long, boring cybersecurity training sessions! The great news is, today’s cybersecurity training can be fun and fast. They may even have a short quiz baked in to gauge effectiveness and ensure everyone is paying attention. Many are delivered light-heartedly with entertaining storylines and in micro-sessions just a few minutes long. No binge watching required, and users might actually start to look forward to the next episode.

WHAT’S THE FREQUENCY?

Ongoing, at least monthly, no less than quarterly.

Rewards & Recognition

You *can* include ice cream.

As you start building out the cultural aspect of your cybersecurity program it might come with some reluctance or even pushback from users…one more thing they have to do that they didn't have to do before! That's why it's important that it is clearly explained to the leadership team and all users why these programs are put in place, how they help improve cybersecurity, and what it means to potentially save the company from the sometimes irreparable damage of a cyber incident.

Have some fun with your program! Many organizations have implemented the Carrot Principle: for employees who pass phishing simulation testing and complete their monthly video training they are rewarded with gift cards, prizes, or even small awards for being a cyber-defender. Perhaps some friendly departmental competition is your company style? See how the sales team does versus the finance team with a little cyber-competition! Setup the leaderboard, track the points, and crown the winners. Adding gamification, rewards, and recognition is a relatively small step that can really help your program create a buzz and be a big success.

WHAT'S THE FREQUENCY?

This one is up to you, just be sure to tie it back to your other cadences and not be too intermittent with it.

D is for Do It

We talked to A, B, and C and they said this guide just wouldn't be right without D! Cybersecurity is a posture, not a project. Making cybersecurity a top priority is a choice everyone has. We hope this guide shows you it doesn't have to be an overwhelming one and there are simple ways to get started, and started right now.

D is also for Defendify, the publisher of this glorious guide! Defendify is the leading all-in-one cybersecurity platform, on a mission to make cybersecurity possible for *every* organization.

What's next?

Learn more and kickstart your cybersecurity today FREE at **www.defendify.com/essentials**