What's the F in Cybersecurity?

FAILURE IS NOT AN OPTION

Your guide to cybersecurity and what makes the grade

DEFENDIFY®
All-In-One Cybersecurity

THE “F” IN CYBERSECURITY

The “F” in cybersecurity can rear its ugly head when completing a cybersecurity assessment that shines a light on all the things we should be doing, but probably aren’t (yet!).

It’s the last thing you want to see at the top of the page: A great, big, red “F”. You thought you had things under control, but perhaps not. There’s more to it than meets the eye and now you’ve got your work cut out for you. The good news? You are not alone and there are ways to start improving today.

We’re not here to tell you about the importance of cybersecurity, let’s leave that to the news outlets and regulators. What we are here to tell you is what cybersecurity is, *and* what it isn’t:

CYBERSECURITY IS A POSTURE, NOT A PROJECT.

It’s a function in your business that spans people, process, and technology. Cybersecurity isn’t just for IT staff, but everyone in the organization. And it’s NOT just for big banks and corporate goliaths, but for *every single* business.

CYBERSECURITY IS NOT A WIDGET YOU PLUG IN THAT MAGICALLY JUST WORKS.

Sure, antivirus and firewalls are baseline cybersecurity tools we all have and use, but let’s be very clear, they are in many ways the tip of the iceberg in what makes up a truly strong cybersecurity posture.

As a modern business in the digital information age, everyone has something sensitive to think about: From the basics, like financial and employee information, to the not-so-obvious like go-to-market strategies, customer data, and intellectual property. For yourself or for those who you do business with, there is a lot at stake and a lot to protect.

We know a cyber breach is devastating. It can result in substantial financial losses (often hundreds of thousands to millions of dollars), operational downtime, and irreparable damage to reputation and customer trust. It’s not surprising more businesses are now requiring cybersecurity assessments from their vendors. This means that you need to be prepared to show that you understand what the latest cybersecurity risks are, and that you have things—including customer data—locked down and secured.

Can you make the grade? Let’s find out...

ASSESSMENTS & TESTING

You just don't know where you stand unless you benchmark with assessments and testing. Before going out and buying the next fancy security software you saw online, it is important to conduct a full review of your organization's cybersecurity posture in all areas.

A cybersecurity controls assessment is like taking a test on the overall cyber-hygiene of your organization, identifying weaknesses, and scoring you on the strength of your cybersecurity posture.

HOW DO YOU KNOW WHAT TO LOOK FOR?

One of the more important cybersecurity developments over the past decade has been the rise of security frameworks from organizations like NIST which can assist you in this assessment. In some cases, your use of a given framework may come as part of a business or compliance requirement, but in every case, these frameworks act as a blueprint for what your organization's cybersecurity program should look like.

There are several security frameworks available that focus on the various controls needed for a robust cybersecurity posture. Some of the more common frameworks include:

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC):

CMMC is in play for contractors who provide services to the Department of Defense. The government understands that most contractors hold sensitive government data and in order to protect it they need to ensure that is protected the same way the does. CMMC has it's own framework with varying levels and organizations will hire third party assessors to become certified.

ISO 27000 SERIES

The ISO 27000 series of standards come by way of the International Standards Organization (ISO). The 27000 document itself provides an overview in how to identify and manage security vulnerabilities. As with some of the other ISO standards, it is possible to receive certification for compliance with the standard.

NIST PUBLICATIONS

There are several different frameworks that have been created by the U.S. National Institute of Standards and Technology, which began as far back as 1990. Most of these standards have been published as part of an "NIST 800" series of documents. One interesting element of this framework is that it specifically takes into account the differing capabilities and resources of smaller businesses, helping to set guidelines accordingly.

These are just a few examples and there are enough different frameworks that it can leave even compliance specialists perplexed. But it is a good exercise to find what frameworks will fit your needs, situation, and industry segment. Don't forget that these security frameworks will provide guidance to your organization and validation in communicating with clients that you have a serious cybersecurity program in place.

ASSESSMENTS & TESTING

HOW DO WE KNOW WHERE WE STAND?

The outcome of a control assessment can be concerning for some, but it doesn't have to be. When first getting started, most organizations without in-house security teams will not get an 'A' grade on their assessments. A large majority have to work their way up—over 90% according to Defendify customer activity—many of whom start with an "F" in cybersecurity. Regardless of where you stand, at least you'll know where you stand! The assessment should not only identify areas of weakness, but also provide recommendations for improvement. As you fill security gaps, future assessments should deliver a higher grade of your overall cybersecurity strength. Here are a couple other common ways of further evaluation:

VULNERABILITY SCANNING

Automated vulnerability scanning tools will help you quickly identify security weaknesses across systems, networks, devices, websites, and applications. These tools identify and then should prioritize remediation tasks based on the level of risk. And once in place, they should run regularly and report back to help institute a model of continuous improvement in what we all know is an ever-changing technology landscape.

PENETRATION TESTING

Test the strength of your cybersecurity through a "penetration test" (or pen test). This is done by a certified "Ethical Hacker" (sometimes called a "White Hat Hacker") who attempts to breach your networks and systems to gain access to your data in a controlled environment. Through this test, you will see proof of any successful breach, how access was gained, and what data was impacted. In other words, you're hiring a "good" hacker, asking them if they can get to the crown jewels, then getting a report back with how far they got, the holes they found, and where to button things up.

POLICIES & TRAINING

People are certainly capable of making mistakes that can result in a costly cyberattack. The human factor in cybersecurity is a big one: According to the *2021 Verizon Data Breach Investigations Report,* one in every three cybercrime incidents involves tricking someone into engaging with a malicious phishing email. Counteracting these tendencies spotlights how crucial it is to provide regular cybersecurity awareness training.

WHAT DRIVES CYBERSECURITY AWARENESS UP AND ERRORS DOWN?

There are many methods to train employees (from the C-Suite to interns) on how to detect a cyber threat and what to do if one is discovered. For example:

PHISHING SIMULATIONS

A common tactic is to deploy phishing campaigns that mimic actual malicious emails, but are sent at your own organization. The goal is to see who is clicking on what, and more importantly, to drive awareness and alertness. Phishing simulation solutions should provide education at the point of failure, and deliver a detailed report showing who took the bait, and who is excelling in their cyber education.

AWARENESS TRAINING

Providing regular cybersecurity awareness videos and organizational-wide trainings will help keep cybersecurity best practices top of mind. Content can be bite-sized (e.g. sent in monthly format, just a few minutes long) and in longer form (e.g. classroom style), but should always be interesting, engaging, and relevant.

POLICIES

Having a clear technology and data use policy is a necessary tool to govern how employees are expected to access and handle sensitive company information and technology. This policy is a great way to train employees on what data is considered confidential, who is allowed access to it, and how it should be handled. For example, the policy might outline if personal devices are authorized to access company systems and how passwords are to be implemented when using applications.

A team that understands how best to protect the company from cyberattack means that everyone can (and should) play the role of a cyber-defender.

DETECTION & RESPONSE

There is no such thing as being 100% secure. That's right, you heard it here, straight from the cybersecurity professionals. That's why when we think about cybersecurity, we have to be both proactive and reactive.

BUT WITH ANTIVIRUS AND FIREWALLS IN PLACE, WHAT'S TO WORRY ABOUT?

These cybersecurity basics certainly continue to play a role, but it is important to keep in mind what they can and cannot do:

ANTIVIRUS SOFTWARE

Traditional antivirus software scans for known malicious threats on computers and servers. The key word here is "known." Traditional antivirus works by cross-checking processes in your computer against a virus signature database, sort of like a dictionary of known malware. When it finds a match, it flags the process running as a virus or potentially harmful. Otherwise, if the execution isn't recognized as a threat, the antivirus lets it through and keeps running. The limitation of traditional antivirus is that it relies on an existing virus signature database—something that is updated, not in real time, but only every so often (e.g. hourly or daily). With 4+ new malware threats created each second of the day, advanced threats like ransomware and zero-day threats, which are not yet known by the "dictionary," can slip by even "next-generation" antivirus which touts AI that can detect and block. How? Attackers study how even the best antivirus products work and customize attacks that circumvent what the product is known to protect against. It's important to understand that cybercriminals are people and successful breaches have involved humans using creative strategies to bypass and disable top ranked antivirus solutions to avoid detection during the attack.

FIREWALLS

A firewall monitors the data that comes in, at, and out of your networks. It can do things like block traffic from geographies where you don't do business, detect patterns that indicate a probe or attack, and restrict user access to unauthorized sites. Again, we're talking about "known" things to look for with some of the same considerations as mentioned with antivirus. But while a well-configured firewall can be effective, it is far from being a comprehensive solution for defense. Hackers know firewalls and their weaknesses, including how hard it can be for IT professionals to effectively configure, monitor, and maintain with limited time and resources. A wide variety of attacks can bypass a firewall in different ways, and a firewall will not prevent access from an attacker who has stolen legitimate credentials from one of your users or who is targeting cloud applications (such as email) that live outside the boundaries of the firewall.

The traditional duo of firewall and antivirus remains necessary, but it is important to keep in mind it's just a small portion of a truly comprehensive cybersecurity program.

DETECTION & RESPONSE

NOW WHAT? WELL… CONSIDER A CYBER ALARM SYSTEM.

A building alarm with siren is good, but one with 24/7 monitoring with live human response is better. The exact same thing goes for cybersecurity.

Today your IT systems can be monitored for anomalous behavior with a security response team that identifies and contains active threats 24/7. This dedicated team can monitor endpoints, networks, email systems, and cloud applications armed with tools that alert, rank, and track all the potential security issues that have cropped up. When an alert requires investigation, security professionals jump to action and contain threats as they happen.

This might sound complex and expensive, and you're right, it can be: On average a full Security Operations Center (SOC) staffed by well-trained security analysts monitoring an organization comprehensively can sometimes take years and millions of dollars to stand up. That's where outsourcing starts to make a lot of sense, especially for organizations without security teams:

MANAGED DETECTION AND RESPONSE (MDR)

MDR can be considerably more cost-effective and achievable for organizations lacking a 24/7 security team. But speed to safety is another factor as well: An organization can bring itself up to speed in this way considerably faster than building it themselves. We're talking weeks, not months or years.

SO, WHAT DO YOU DO IF THERE IS AN INCIDENT?

Perhaps an employee emails sensitive data to the wrong person, or a laptop housing sensitive data is lost or stolen. An Incident Response Plan is a document that details what to do if a cyber incident occurs and who on the team (internally and externally) is responsible for what. Ideally something stored away that never needs to be used, but especially important to have ready if something does happen. Reducing the time to address an incident can make all the difference in the world in terms of spread and severity. In some cases, it can mean the difference of staying in business or losing a business entirely.

FAILURE IS NOT AN OPTION

I think we all agree, cybersecurity is one course nobody wants to get an 'F' in.
It's also not something you need a master's degree in to implement yourself:

CYBERSECURITY FRAMEWORKS EXIST FOR YOUR BENEFIT.

While some may seem daunting, many of today's cybersecurity tools are built around them and help you navigate them.

IT'S A MODEL OF CONTINUOUS IMPROVEMENT.

An assessment helps you know where you stand and ongoing testing can ensure you only get better. Start now, rinse, and repeat.

KNOWING IS HALF THE BATTLE.

Sharing that cybersecurity is a priority and providing some guidelines sets the stage. Training can be fun and simple. Everyone is a cyber-defender.

YOU DON'T HAVE TO GO IT ALONE.

Not everyone can staff security experts or manage a deep cybersecurity tech stack. Just like your customers do with you, outsourcing can save time and money.

So, the answer to the big question of whether you can make the grade is undoubtedly:

YES!

You absolutely *can* (and should) make the grade. And you can start today, simply by taking a look in the mirror.

So what's next?

FAILURE IS NOT AN OPTION

Speaking of not going it alone, know that Defendify is always here to help.

Defendify works with organizations just like yours, most without dedicated security teams, every day to streamline cybersecurity across people, process, and technology.

What's your cybersecurity strength?

[✓ A] B C D F

Get an idea of where you stand with Defendify's quick and free health checkup and cybersecurity grade at:

www.defendify.com/mygrade