Modern Cyber Security Standards for a Mid-Sized Business

Most businesses that have any connection to the internet — and that, in turn, is most of them — should take cyber security very seriously. The consequences of ignoring cyber security as a basic element of your business can be disastrous. From downtime to lost customer data to lost customers, the possibilities go on — each worse than the last. It's crucial, therefore, to understand modern cyber security standards, especially as these relate to mid-sized businesses. Understanding these standards is the first step toward putting them in place and reaping the benefits therein.

Why Your Business Needs a Cyber Security Framework

Establishing a cyber security framework is one of the best first steps to take for a range of reasons.

Understanding Threats

When your business establishes a cyber security framework, it can better understand what threats it faces. When protection against a certain potential threat isn't built into the framework, it's a great time to interject the simple question of "why" into the mix. Then, the stakeholders involved can better understand why the system is being protected against what it is and why it isn't being protected against certain other threats that may not be so urgent.

Sets Priorities

As much as we'd all like "protect against every threat right now" to be a plan of attack, it just isn't. Operations have to start somewhere and conclude somewhere, and those two points cannot be the same point. By establishing a framework, we're better able to decide which threats are most crucial to address immediately and which can be done later.

Determine a Plan of Attack

There are actually several security frameworks out there. At Access One, we recommend using the national cyber security framework (CSF) from the National Institute of Standards and Technology (NIST). There are other options, certainly, but choosing a framework such as the NIST CSF covers the bases quite effectively.

Prioritize Budget on Critical Security Controls

In the midst of all the things that users have to consider in light of cyber security standards, two of the biggest to focus on are budget and controls.

Ensure Resources Are in Place

The budget is the primary scope of available resources. If a cyber security plan exceeds the budget available for it, then it will be immediately lacking — and often lacking in unexpected ways. By establishing a budget immediately and sticking to it, it will be clear what you can have, what you can't have, and what you may need to set up for the next update.

Controls Represent Industry Best-Practices

While your budget determines your outer range of operations, controls represent what you should focus on immediately. This is particularly true for those using CIS controls from the Center for Internet Security. These points, separated into basic, foundational, and operational controls, help establish just what areas should be a focus. This allows you to better adhere to your budgetary restraints and identify immediate areas for improvement to be staged during future funding cycles.

Why Your Policies and Cyber Security Standards Need to Be Written

Keeping your security standards written is crucial on a few levels.

Knowing What's Policy at a Glance

Writing down policy ensures that everything that is policy is present in the same place. When you only tell people what policy is, it becomes difficult to refer back to that policy later on. A newspaper advertising sales rep once noted: "The spoken word is like the air, but the printed word is always there." It might sound a bit smarmy, but it's no less accurate for the poetic touch.

It Contains the Basics

A basic security policy should at least include several key points, including policy on password creation and use, the acceptable use policies for email, internet, and the like; data access policies for sensitive data; physical security policies; and a few others. By having all of these policies in one place, you're better able to address them if they need to be changed in some way.

Prevention of Security Fatigue

By writing down security policies, you can see at a glance just how many such policies you have. If it becomes clear that you have so many security policies that no one can get the job done, then you become aware it's time to pare down that list to focus on the essentials.

A Roadmap to the Future

We know how written policies clarify what's official policy immediately, but there's a flip side to this coin: We also know what isn't policy, or at least not yet. By knowing what businesses have established as policy, we can match these policies against changes in the field. Such matching lets us see where our weak points are and how we can modify the policies we set up to address the shortcomings that appear later.

A Yardstick of the Present

The best part about written policies is that we see what's policy immediately. As previously noted, this means a way to immediately tell what's going on. It also gives us a way to measure our current performance against our current goals. If we treat written policies not just as rules, but also as goals — these are the cyber security issues we want to address most — then we can quantify what we want to do in relation to what we're doing right now and how far we've come toward those goal policies.

Why Your Risk Assessment Needs to Include Business and Technology Risks

While many cyber security-related risks are fairly common and already widely known, some risks are more subtle. Thus, businesses that understand that there are both business and technology risks to consider in their risk assessment have the best chance of coming out ahead.

Improved Focus

By acknowledging and understanding the business-specific risks involved, businesses know what to focus on first. By understanding business-specific risks, businesses know which issues are most likely to appear first, and which issues are less likely to hit and can wait for future funding expansions. Few have the necessary resources to immediately prioritize absolutely everything, so by knowing the business-specific risks that are most likely to hit, resource allocation accordingly becomes a means to improve responses.

Cultural Benefit

Businesses that understand business-specific risks have another advantage here, too, in that they can apply the benefits of corporate culture to security. A business that understands the risks a phishing attack can pose can, in turn, use one of the best counters against phishing: direct employee assistance. Because phishing attacks target email — and your employees are the ones most frequently in contact with email — training employees to spot this highly specific risk case will allow many phishing attacks to be blunted before they even start.

Collateral Damage

Understanding business-specific risks often leads to businesses thinking in new ways beyond just the business-specific risk. For instance, a business that understands that an attack may take place unnoticed until it's too late can also understand that there's a clear need for a backup plan in case such an attack happens. This leads a company to start considering disaster recovery and business continuity issues. The same backup systems that allow a company to recover from a ransomware attack, for example, can also be applied if the company experiences a fire, flood, or earthquake. These risks weren't considered as part of cyber security planning, but they become considered nonetheless.

Considering Change

For those not familiar, change management is a term that connotes an active role in planning for one of the great business constants: change. With change management, we're forced to slow down the pace of change and manage it — not reacting but acting along with it. Change management also requires an active consideration of unique business risks. For instance, if we just set our systems to update the second a patch is available, that might be a smart idea from a cyber security point of view — unpatched systems are a big risk — but that tactic might not be smart elsewhere in the business. If we update our firewalls as patches arrive, that same firewall may stop all traffic from flowing while an update is in progress. That means downtime and loss accordingly. It may be better, therefore, to hold off on that update until after hours, when there's no other traffic to get in the way. With change management, we must stop and consider issues like this, making it perfectly suited to consideration as part of unique business risks.

How to Get Started Putting the Best in Cyber Security Standards to Work

Establishing the right kind of cyber security standards and actually putting them in place will mean your business survives where others don't. You improve your protection against a data breach and improve the odds you'll avoid downtime as much as possible. You'll also better protect your customers' data, keep those customers in the fold, and, for those businesses who come under regulatory scrutiny, you'll better survive inspections and audits to continue delivering your services.

For the best in cyber security standards and world-class IT security solutions, reach out to us at Access One. We have a range of services from email protection to employee training to help protect the system against threats before they even have a chance to strike. Get in touch with us to start the process, and protect your systems against the worst of cyber security threats.