TECH TIPS
TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON CONSULTING & SOLUTIONS

Inside This Issue

Understanding Cyber Security Compliance Standards |1

New FREE Report Download: IT Buyers Guide |2

The Biggest Risk Is Not The One You Don't Take, But The One You Don't See |3

Let Your Employees Know You Care With These 3 Tactics |4

3 Popular Small-Business Trends For 2023 |4

April 2023

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

Understanding Cyber Security Compliance Standards

There is an endless number of things a business owner should do for their business to be successful. They must develop a product or service that can attract customers, hire and train a team to oversee day-to-day operations, implement marketing strategies and so much more. While all these tasks are essential for your business to be profitable, your business will never get off the ground if you aren't compliant with standards that affect your industry.

Compliance standards are guidelines or rules that organizations must follow to meet legal, regulatory or industry requirements. These standards are designed to ensure organizations ethically conduct business – by protecting the rights and interests of their customers, employees and other stakeholders. When an organization does not maintain its compliance standards, it will be met with fines, legal action and other penalties.

Many compliance standards that apply to most organizations involve sensitive information protection. Here are a few examples.

National Institute Of Standards And Technology (NIST)

The NIST is a nonregulatory agency of the United States Department of Commerce that promotes innovation and industrial competitiveness. As a business leader, you must be aware of the various cyber security standards and guidelines set by the NIST. One such standard is the NIST Cyber Security Framework, a voluntary framework that provides a way for organizations to better manage and reduce cyber security risks. It's built on the following five core functions:

- **Identify**
  It's vital to understand the organization's cyber security risks, assets and the people responsible for them.
- **Protect**
  Implementing the necessary safeguards to protect the organization's assets from cyberthreats can shield companies from increasing risks.
- **Detect**
  It's important to detect when a

Continued on pg.2

Continued from pg.1

security incident occurs. This function includes activities like monitoring network traffic and reviewing logs.

- **Respond**
  By responding to security incidents as they occur and containing the incidents, people can eradicate the threat and recover from it.

- **Recover**
  After a security incident does occur, organizations must know how to restore normal operations as well as their systems and data. This process often helps people understand the importance of implementing safeguards to ensure similar incidents do not occur in the future.

Health Insurance Portability And Accountability Act (HIPAA)

The compliance standards set by HIPAA are some of the most well-known as they pertain to protecting personal health information (PHI) in the United States. HIPAA requires covered entities, such as health care providers and health plans, to ensure the privacy and security of PHI. The Security Rule and the Privacy Rule are the two main sets of regulations under HIPAA that covered entities and their business associates must follow. The Security Rule sets standards for protecting the confidentiality, integrity and availability of electronic PHI and requires covered entities and business associates to implement certain administrative, physical and technical safeguards. On the other hand, the Privacy Rule sets standards for the use and disclosure of PHI and gives individuals certain rights concerning their PHI – such as the right to access their PHI and the right to request their PHI be amended. Failure to comply with HIPAA can lead to significant financial penalties, reputational damage and, in some cases, the loss of a license to practice medicine.

> **"Your business will never get off the ground if you aren't compliant with standards that affect your industry."**

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a relatively new set of compliance standards developed by the Department of Defense to protect Controlled Unclassified Information. The CMMC is mandatory for all DoD contractors and subcontractors that handle CUI. This is a tiered certification system with five levels of maturity. Each level has a specific set of practices and processes that organizations must implement to achieve certification. As a business leader, you should be aware of the CMMC and the specific level your organization will need to achieve to comply with the DoD contract requirement. CMMC certification is audited and managed by a third party. Keep in mind that getting this certification will take ample time and effort. You'll need to implement robust security protocols and practices that may not have been in place before.

These are just a few compliance standards that may be required in your industry. Complying with these standards will help protect your business, customers and employees.

The Biggest Risk Is Not The One You Don't Take, But The One You Don't See

"The biggest risk is the one you don't take" is a mantra you'll hear motivational speakers deliver in their presentations to make the argument that you should throw all caution to the wind and *go for it* (whatever "it" is).

And while that may be a good piece of advice to get someone to take action on an idea (and get the speaker applause at the end of their presentation), truly smart, experienced entrepreneurs and business executives NEVER throw "caution to the wind" and take *wild* risks. They take *calculated* risks, weighing consequences and putting buffers, hedges, and checks in place to reduce the risk and potential losses. They look for the risk because they know unchecked optimism is not only foolish but dangerous, and Murphy is always standing by with a big wrench in hand, ready to throw it into your best-laid plans.

If you follow Warren Buffett's two rules of investing, you'll see this same caution: Rule #1 – Never lose money. Rule #2 – Never forget Rule #1.

A good question to ask yourself is, where are YOU putting your business and your money at undue risk? While you cannot prepare for and prevent EVERY risk in your business, one area where we see a lot of businesses taking huge, unmitigated risks is with their data and cyber security.

Despite the overwhelming evidence that the risk and the financial consequences of cyber-attacks are enormous, we still hear, "Nobody is going to hack us…we don't have anything they want," or "We can't get hacked because_____," with the blank being things like "we use cloud applications" or "we have a good firewall," "our people are too smart to click on bad links in e-mails," or other similar "reasons" for their false sense of security. They *explain* it away.

Candidly, it's our belief that this is not founded in confidence and logical thought but based on willful neglect and a desire to avoid spending the funds necessary to truly secure their data, their business, and their finances. And while I completely understand that nobody wants to spend a lot of money on IT, **the risk doesn't cease to exist just because you choose to ignore it.**

One of the smartest investors in the world, Howard Marks, CEO of Oaktree Financial, said, paraphrased, the less risk you perceive, the more risk there is. For example, if I don't think there's any chance I can die in a car wreck on my way to the store, I'll fail to put on my seat belt, text while I drive, and be a lot less cautious about paying attention to the road than if I thought there was a very high chance I could be in a fatal crash. The lower the risk perceived, the higher the risk actually is because we lower our guard and don't protect against it.

That's exactly why small businesses are the #1 target for hackers. They're EASY prey. Sure, they don't get the bragging rights of bringing down a company like Dole or hacking into Microsoft Azure, but hacking millions of small businesses for a few thousand dollars each in ransomware pays. You just don't hear about these attacks because they don't make the evening news, just like you don't hear about the 6 MILLION car wrecks that happen every year. Only the big ones – or the ones that seriously impact rush hour traffic – get noticed.

If you are not all that certain that you are truly and fully protected against such hacks, schedule a brief consultation call with us. We can conduct a quick and easy cyber security risk assessment and tell you for sure if your current IT company is protecting you and what level of risk you're at for a cyberattack. It's free and comes with no expectations or cost.

Remember, not all successes are measured in gains secured. Sometimes success is defined as losses avoided. If you were given the chance to go back in time and unwind 2 or 3 financial, business, or life decisions you've made, knowing what you know now, I'm sure everyone would take that opportunity. Most likely, you'd go back and warn yourself about the dumb mistakes you made and put protections in place to avoid the losses you incurred. Sadly, there's no genie in a bottle to make that happen, so an ounce of prevention against cyberattack IS, without a doubt, worth a pound of cure.

Let Your Employees Know You Care With These 3 Tactics

If an employee is unhappy working for your company or doesn't feel appreciated by their leadership team, they will search for a new job. This has left many leaders questioning what they can do to show their employees they actually care about them and their well-being. Here are a few different ways to show your team you care.

Growth Opportunities

Most employees want to work somewhere with the potential for advancement. It's important to connect with your employees through one-on-one meetings so you can determine how they want to grow professionally and personally.

Foster A Supportive Work Environment

Nobody wants to work at a business where they don't feel accepted, supported or appreciated. Go out of your way to create an inclusive environment and give your team a sense of belonging.

Recognition

Your employees want to hear about it when they do well. Don't be afraid to recognize or reward them when they're doing a great job. Simply thanking your employees for their hard work can go a long way toward improving overall morale.

Are You Micromanaging Your Team?

There are many different management styles, but one that always seems to upset employees and take away from productivity is the act of micromanaging or overcoaching. Micromanaging occurs when a leader provides instructions that are too specific while watching over the team as they perform their tasks, looking for any lapse in perfection they can then bring up to the employee. It's a frustrating practice that can send well-qualified employees running out your doors.

So, how do you know if you're micromanaging your team? Pay attention to how you're directing them. You won't get a preferred response if you tell your billing manager how to do their job. You hired these employees to perform specific roles, and they have the experience to do it well. So, let them work until there's a need to redirect or re-analyze the situation. Ask for feedback when you conduct one-on-one meetings with your team. Listen and make the necessary adjustments if they say you're micromanaging. This will help boost productivity in your business while you still get the most from your team.

3 Popular Small-Business Trends For 2023

There are new trends for business leaders to learn and explore every single year. Here are three of the biggest trends you should be aware of as you progress through 2023.

- **Investing In The Business**
  Many business owners are opting to invest more in their hiring and marketing efforts. By doing so, they're inviting new customers while improving the customer experience.
- **Updating To New Technology**
  Technology has come a long way in the last few years. Now is the time to automate certain processes and invest in new advanced technologies to help your business.
- **Finding A Mentor**
  It's difficult to run a business independently. Try to find someone who has done it successfully – and listen to their advice. The right mentor can improve nearly every aspect of your business.

"Well if you people can't fix my computer virus, maybe you can tell me what the heck the Center For Disease Control is doing with my tax dollars!"