No doubt you worry about the success of your business. But as it grows, a new source of worry is likely your ability to protect it against cyber, compliance, and other IT risks.

> *"... an average company is affected by a serious calamity every three to five years ..."*

Entrepreneurs are typically more attuned to opportunities than threats, and it's easy to push risk and compliance issues to the bottom of the list. But these concerns have a way of making themselves priorities – when we least expect it! It's said that an average company is affected by a serious calamity every three to five years, and if not being prepared could mean the end of your business.

Most businesses can categorize risks as either external or internal. An external issue might be disruptive climatic event like Hurricane Irene, or the recent heat waves across North America and Europe. Another external issue is the imperative to comply with shifting data protection regulations. Security concerns are constant, and in the worst case can result in a cyberattack that destroys all your data. Then there are the events that nobody could have foreseen, such as when one of our clients had a minor subsidence in their building that required evacuating for weeks. Internal threats could include unpleasant surprises like data theft; being dropped by a main client; or losing long-term access to your main business system.

Whether external or internal, though, your business is worth protecting. That's why you must understand potential risks and prioritize them. Some may be almost impossible to protect against. Others may, after analysis, not be worth concerning yourself with. Whatever the case, you must understand your risks, so when things go wrong — and something always goes wrong! — you're as prepared as possible.

> *"Nothing should be off the risk-and- issue agenda, even scenarios that are contentious or even extremely unlikely."*

Facing Up to Your Risks

The first step for any executive team is to hash out the risks and issues your business faces. Generic concerns about security aren't good enough: you should know specifically what and where your risks are, and at the very least have a plan for them, even if that plan is "do nothing."

One of the first things we recommend that clients do is to create a risk/issue log. Any competent IT leader will do this soon after joining a company. But if your business doesn't have a risk/issue log, then it's time you started one.

A risk/issue log, of course, defines all the risks within the business. To be an effective tool, it needs to describe the risk; outline the likelihood of its occurrence; estimate the potential damage to the business; and,therefore, how important it is to resolve. Nothing should be off the agenda, even scenarios that are contentious or extremely unlikely.

Once you've created the log, it needs to be maintained and managed. An out-of-date risk/issue log is useless. It's important to note the difference between a risk and an issue. A risk is something that may happen, while an issue is something that has happened. Examples of risks that could turn in to real-life issues include:

- Structural failure in a new office building forcing the immediate need for an alternative site.
- Multiple network link failure when an external contractor cut the cables — meaning no Internet, no email, no files!
- An IT Service Provider going bust and leaving a company without any support or access to their servers.
- The company's underground parking lot flooding and threatening the power supply to the whole building.
- 200,000 files taken over by ransomware.

The risk/issue log, and its maintenance, is just the beginning of proper risk management. Next you must appoint a high-level executive to be responsible for setting up projects to resolve or mitigate the most urgent risks.

> “Major security breaches happen when no one at executive level has the time or expertise to ask the right questions and to make the right compromises”

Keeping Up With Compliance

Today, compliance is a risk for every business, especially when it comes to data protection and privacy. US rules are complicated and may differ by state, or even municipality. The European Union’s General Data Protection Regulation (GDPR), which went into effect in May 2018, can actually be considered a global data protection law, in that it applies not only to business that work with data of EU citizens — it applies to companies that work with such businesses as well.

Don’t underestimate the GDPR. First, compliance is likely to require many changes to even non-European businesses, not only in technology, but in processes, policies, sales, and marketing. Second, compliance failures risk a fine of up to four percent of global revenue!

Another regulation affecting many of our clients is Payment Card Industry (PCI) compliance. In this case, compliance is required if you have any kind of payment processing. It may depend upon how, exactly, your business deals with payment processing; but anything other than tokenized payment processing risks an audit, a penetration test, and on-going fines.

Fines for PCI compliance infringements usually kick in when there’s a security breach. The fines and costs can mount up very quickly, even for those companies handling just a few thousand credit cards.

If your business is in the financial services sector, then the level of compliance is far more wide-ranging. You will likely be dealing with multiple regulatory authorities in multiple countries, and the rules will be quite specific. For example, Britain’s Financial Conduct Authority (FCA) has guidelines on the use of social media. And, of course, there are the many sector-specific compliance or regulatory requirements; each sector has its own set of regulations.

Since compliance can be so complicated, it’s likely that you’ll need third-party compliance professionals. Therefore, remember to budget for it. And professional compliance experts tend to create very, very long lists of actions; so, you’ll need someone with a balanced, sensible, and commercial viewpoint oversee the project.

The first steps are to learn which regulations apply to your business; appoint someone at executive level with responsibility for compliance; and then maintain that compliance.

> “Establish how you will handle a crisis in advance. Who’s in charge during a ransomware attack, because decisions need to be made on the spot?”

Physical Security and Cybersecurity: Where To Start?

Every company needs physical security, on-line data security, and process fidelity — especially because there are so many ways that today’s mobile businesses can be compromised without anyone knowing about it.

Here are ten key steps to security in the real world and online:

1. First and foremost, look at perimeter security, including both the physical security of your office and the security of your systems. All networks make contact with the outside world, and these points of contact must be firewalled. Experts in systems and firewall management need to configure this equipment and to keep it current.
2. Access to systems should be on a least-privilege policy. For example, when an employee has access to a system, the default is that he or she has no rights to anything. Then privileges are granted only to include the data and processes they require. If your systems don’t follow a least-privilege system, then you are significantly exposed to fraud, cyberattack, and human error.
3. All systems and software must be up-to-date and properly patched, especially antivirus and anti-malware software. These systems only work well when they know what they’re up against.
4. To protect your data, it should be encrypted by default and accessible only to those with the approved rights. Where you have customer data, particularly user accounts and passwords, ask your IT team whether the data is “hashed and salted,” which will make it very secure, even if your systems are breached. It is unforgiveable nowadays to be holding unencrypted customer data (known as “clear or plain text”).
5. Canny criminals know that your employees are the weakest link on the security chain. Criminals have become highly adept at social engineering — that is, manipulating people to their own ends. For instance, it’s not unusual for a criminal to email the CFO posing as the CEO, asking for money to be wired to a (fictional) supplier’s (real) bank account. Your best defence is to put sound financial processes in place and spend time on training and awareness for your staff.
6. Your data and systems should also be regularly backed-up and stored offsite, preferably with no connection to your live systems (known as an “airgap”). Ensure the backups include multiple versions of the same document, in case of undetected corruption or malicious encryption. Having a decent data backup can be the difference between having a business post-disaster and not.

7. Software and web applications must be built by trained experts — because good developers can build secure software, and bad ones don't — and you won't necessarily know which they are! Ask whether they are designing to meet the OWASP Top 10, and consider getting an independent penetration test, which can likely be done for under $10k.
8. Create a "secure culture," wherein taking this stuff seriously is encouraged. Make sure that your "generals" and "lieutenants" are demonstrating good habits. If they write their passwords on post-it's, then their staff will do the same ... and one day you will probably find yourself hacked!
9. Establish how you will handle a crisis in advance. For instance, make sure it's crystal-clear who's in charge if there's a ransomware attack and decisions need to be made on the spot. In the EU, for example, GDPR makes specific requirements about notifying the authorities if you suffer a security breach. Who in your company is responsible for this? Because failure to do so will result in a fine.
10. Get certified — this will give a focus and purpose to your efforts to improve security. Look for a recognized and well-respected certification. This will provide you with a standard accreditation that directly demonstrates to you, your company, and your customers that you take security seriously and that your systems are well-managed. Clients can be won simply because you stand out by having a desired (sometimes, required) certification.

> Standard processes are actually empowering for staff. They know what they can (and can't) do, which across the business increases a feeling of trust.

Reputation is Everything

Aside from the obvious operational and financial impact of a cyberattack, data leak, or compliance-related prosecution, your reputation will suffer the most damage.

If customers know you've had a breach, they may never buy from you again. Certainly, you can be sure that they'll tell their own contacts. Not only will it affect your reputation with customer, but it will also make it harder to attract the best people to work with you or remain with you moving forwards.

You can be sure that after such a calamity, your competitors will be leveraging your failure to their advantage, and businesses that work closely with you may start to distance themselves to limit collateral damage. It's possible that suppliers will remove or reduce your credit terms, and it's almost a certainty that your insurance costs will increase (or you may not be able to find coverage at all).

A note on insurance: cyber insurance is a good way to avoid the potentially disastrous consequences of a cyberattack. It will help cover the cost of repairing your reputation and getting systems back up and running. Never settle for cyber insurance thrown in with your normal business insurance; get proper advice and know what you're buying. And remember you need criminal insurance to cover stolen funds.

Process is Good

A set of standard business processes is the foundation for withstanding the potentials setback of security breaches and compliance problems.

In fact, these processes help avoid many such problems in the first place: most of the time, particularly with social engineering, criminals get someone to do something that doesn't follow the usual process, whether that's clicking on a link or giving away a password to someone who's called them to fix a nonexistent computer problem.

It may be boring but standardized processes could save your business a ton of money and time, as well as providing your staff with a sense of confidence. Standard processes are actually empowering for staff. They know what they can (and can't) do, which across the business increases a feeling of trust, and leaders are freed up to perform more value-adding tasks and you reduce the reliance on key individuals, which reduces risks and makes the business more scalable.

Take the time to write good processes — ones that are transparent, easy to understand, and auditable. Make sure the team understands them, and then regularly check they're being followed.

> Secure systems enhance the reliability of your business and improves the service to your customers.

Take Control of It Before It Takes Control of You

It would be very easy to get overwhelmed by all this "stuff" about business risk, security, and compliance. But when done well, it's an enabler for growth, rather than a barrier: good security begins with a well-organized business with a simple structure. And a well-organized business empowers staff, frees up managers, and makes the business more scalable.

Secure systems enhance the reliability of your business and improve the service to your customers. When clear processes are in place, it's also easier for staff, because they always know how to operate, whether it's a normal business day or a crisis. So, while staying on top of your risks and issues will certainly protect your business, it will also help to drive your business forward.

Don't expect to get everything sorted out quickly. Creating the secure and standardized environment you'll need to resolve these issues will take time. But if you set an agenda and a plan with some ownership at the highest level, you'll get it done.

Having trained and experienced cybersecurity professionals available to you can reduce an organization's risk exponentially. And when (not if), the organization does get attacked, that experienced can mitigate the incident and help to get the business back up and running quickly and efficiently ... **and this is where CISO ToGo can help**!

If you'd like to discuss exactly how we can help, get in touch or visit us at:

www.CISO-ToGo.com

Locations: throughout the United States

Email: WRichmond@CISO-ToGo.com

Phone: 401-264-0880

CISO ToGo, LLC ...
because security is everyone's concern, but it's OUR business!