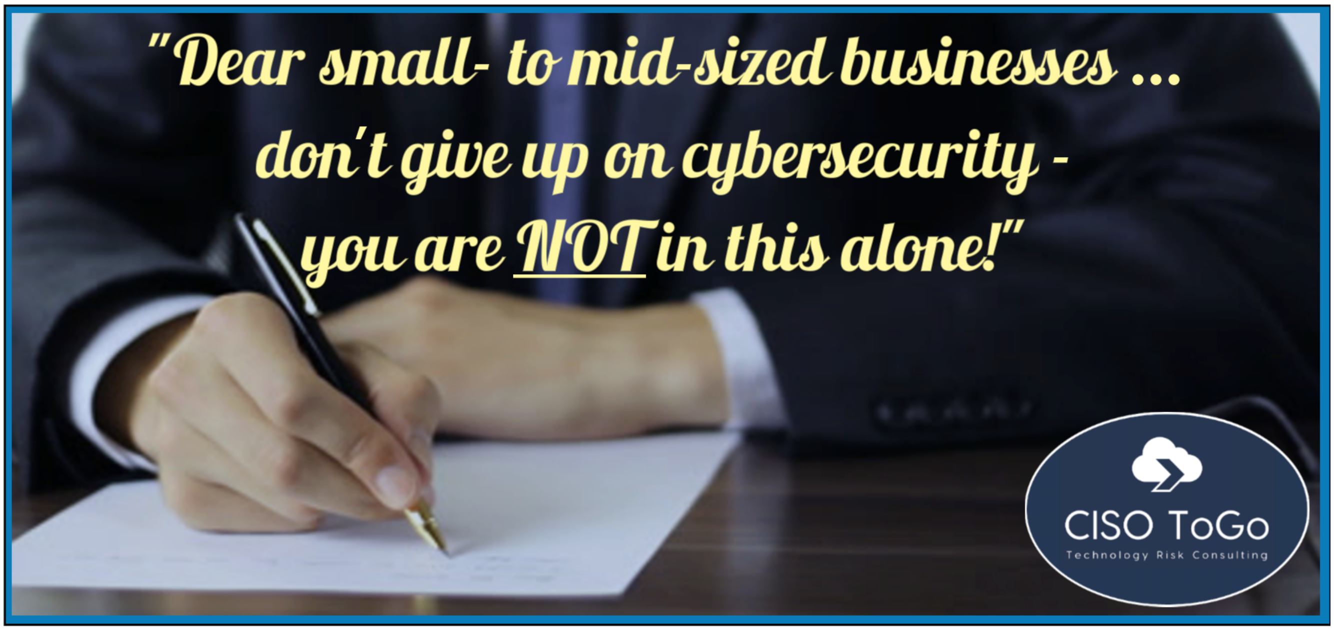
CISO ToGo
Technology Risk Consulting


"Dear small- to mid-sized businesses ...
don't give up on cybersecurity -
you are NOT in this alone!"
CISO ToGo
Technology Risk Consulting

When the focus is often on the big hacking and ransomware cases involving multinational companies and governments, small- and medium-sized businesses can often feel left behind and powerless. But help is available!

In today's increasingly hostile environment, every enterprise, whether big or small, should be concerned about cybersecurity and have access to protection from hackers, scammers, phishers, and all the rest of the host of bad actors who seemingly sprout up daily all around the world.

Yet time and again, we see small- and medium-sized businesses (SMBs) feel left out in the cold, an unaddressed market segment that finds real protection either too expensive or far too complex to adopt. Thus, cybersecurity becomes an "afterthought", or an "add when we can", service that leaves SMBs far more vulnerable than the corporate giants, because the bad guys know that they will be more successful attacking unprotected organizations than those they assume have deeper investments in stopping them.

If you haven’t already, start thinking about security NOW!

It might be tempting to think that it’s too late at this point for an organization with limited resources to start investing in cybersecurity — after all, if the bug guys still get hit, what’s the point in trying to catch up? But actually, there are plenty of reasons to start thinking about cybersecurity right now. The advice from industry and government to SMBs is united in this regard and aligns well with the ancient Chinese proverb that states, “*The best time to plant a tree was 20 years ago; the second-best time is today.*”

There is, in fact, some rather pragmatic advice that can be offered to resource-strapped SMBs around how they should be looking to protect themselves. The most basic is this ... don’t defer; get the program started, and enhance further, as you are able! Additionally, however, there are a few common-sense, low-cost, and high-return fundamental strategies that we would suggest:

- Maintain visibility into your network — if an SMB has one, then it is incumbent upon administrators to know every item touching the network.
- Implement multifactor authentication (MFA) everywhere possible.
- Ensure all network access is role-based — no one who doesn’t need to see a system should be able to touch it (again, with access granted through MFA).

Beyond these fundamentals, we further recommended that companies put in place the ability to **verify the provenance of their data**. That’s just smart practice for any business, and why many countries are looking to keep tabs on where data comes from, regulate what data should be protected, and in some cases determine how it should be treated. SMBs should be aware that regulatory regimes are also for their protection, not just the big guys — regimes such as GDPR and the European Data Act (EDA), which details data ownership and “*gives individuals and businesses more control over their data through a reinforced data portability right, copying or transferring data easily from across different services, where the data are generated through smart objects, machines, and devices.*”

Governments offer help for small and medium-sized businesses

There’s more government help available for SMBs than might be immediately apparent. Recently, the US and UK governments have undertaken efforts that are timely and readily available to address shortcomings and bring resources to the table for the SMB.

In the US ...

The United States has created a Small Business Cybersecurity Community of Interest (COI) within the construct of the National Cybersecurity Center of Excellence (NCCoE). The NCCoE, established in 2012, provides businesses with practical information on securing their information technology. At the inaugural Community of Interest (COI) event in March 2023, US Deputy Secretary of Commerce Don Graves commented that,

> “*This initiative will help to make sure that NIST’s guidance is both meaningful and practical for smaller companies and other organizations to put into use. Beyond benefiting the NCCoE and its participants, this new community of interest promises to improve the return on all of NIST’s investments in cybersecurity research, standards, guidelines, and practices.*”

The NIST COI initiative is designed to get SMBs into the mix and to bring to the forefront resources so they may become cybersecurity aware and hardened. Couple this with the plethora of resources provided by the Cybersecurity and Infrastructure Security Agency (CISA) and every SMB has a healthy slate of resources to advance their knowledge considerably. For instance, some of the topics addressed by CISA for the SMBs include securing supply chains and assessing vendors and vendor security posture.

In the UK ...

The UK’s National Cybersecurity Centre (NCSC) offers its own cyber action plan, which includes a free assessment for small organizations. The online assessment normally takes between three-to-five minutes to complete. The assessment walks the user through a basic cyber hygiene survey. The results are analyzed immediately, and the user is given a “personalized action plan” that the business can do right now to heighten its cybersecurity posture as their takeaway.

Lindy Cameron, NCSC CEO, has gone on record for noting that, while small businesses are the backbone of the UK economy,

> "... *we know that cybercriminals continue to view them as targets. That's why the NCSC has created the Cyber Action Plan and Check Your Cyber Security to help them boost their online defenses in a matter of minutes. I strongly encourage all small businesses to use these tools today to keep the cybercriminals out and their operations on track.*"

In other governments ...

The US and UK are not alone in providing sound advice and resources for smaller enterprises. The Canadian Centre for Cyber Security has a small-business information portal as well as offering Cybersecure Canada, a cybersecurity certification program for SMB organizations – and, among a growing list of governments, Australia also has guidelines for SMBs.

Final Thought

SMBs who avail themselves of advice from industry professionals and research the resources available to them from national and local governments will find that they *are* able to achieve a modicum of cybersecurity at little or no cost. Then, as we previously suggested in this white paper, they will be in a better position to continually assess their situation and close those gaps which carry the highest risk as they are best able.

If you are still left feeling a bit overwhelmed with the task of beginning or enhancing your cybersecurity program, that's where CISO ToGo, LLC can assist, reach out today ... we'd be happy to discuss exactly how we can help!

WRichmond@CISO-ToGo.com

1-401-264-0880

CISO ToGo
Technology Risk Consulting