November 20, 2019 by Cam Breen

FILED UNDER : DATA & SECURITY

Developing an Effective Cyber Security Management Plan

If you are responsible for your corporate information security strategy, there is no doubt that your job is a hard one. Even though the amount of time in the work day hasn't changed, everything else about it has: businesses continue to expand the volumes of data they generate, IT systems are becoming increasingly complex, and cyber threats continue to evolve with cyber criminals becoming more intelligent and creative as time goes on.

It is up to IT leaders to mitigate risk and to keep client and employee data secure. In a previous blog post, we introduced a simple risk assessment framework and a set of security controls and standards to help reduce your risk. However, what actions can business and IT leaders take to start turning this advice into a strong information security risk management plan?

If your organization doesn't currently have a cyber security management plan, or needs to create a more effective one, we have put together some tips that will help.

1. Evaluate your current cyber security strategy

One of the first things you will want to do is evaluate your existing security strategy, including the technologies, controls, policies and protocols in place. While this might sound obvious, there are many IT leaders that overlook what is already in place before they begin implementing changes.

By assessing current plan components, you will be able to note:

- their effectiveness or ineffectiveness
- what needs improvement
- the reasons modifications are required

Maybe there was a problem with how the plan was implemented, a lack of resources, or a lack of follow-through by management that can be addressed?

As for evaluating the current security environment, has it been properly maintained or are there holes in the infrastructure that have been left unattended? What types of additional resources might you need? How security-aware are your staff and colleagues? What is the company culture regarding security like?

This holistic self-assessment is imperative in arriving at the best possible cyber security management plan for your organization.

2. Understand your cyber security risk and tolerance

Once a thorough evaluation of your environment is completed, the next step is to fully understand cyber security risk in relation to your specific organization and business operations.

For most companies, there will be gaps in their cyber security protections. Pragmatically, some of these will be acceptable; however, others will surround mission critical areas and demand investment. Creating a complete list of threats and vulnerabilities, and then prioritizing them according to business impact, will be the quickest way to ensure that your security plan is effective in areas that require the most attention.

3. Collaborate with colleagues and stakeholders

Although skills and experience are important reasons why IT professionals are offered their jobs in the first place, suggestions and ideas from colleagues, junior staff, external peers and industry groups can help inform your plan. Insight and experience come from all types of sources and fresh perspectives can offer new ways of doing things (or prevent you from repeating the mistakes others have already made).

It is also important to integrate across internal groups, including senior management, technical security, information assurance and physical security groups. Building comprehensive representation, and a close-knit team, is vital to the success of the changes you want to see.

Aside from people, there are many resources available to help you build an information risk management strategy. One of the most popular is the NIST Cyber Security Framework, but there are many similar ones out there that are good starting points.

4. Set security measures and controls

Once you have determined all the vulnerabilities that represent risk to your security infrastructure, it is time to establish the best solutions to contain them.

There are myriad measures and controls that can be put into place as part of a cyber security management plan; what's important is that there are processes for implementing your best fit controls and measuring their effectiveness. One important example of a control is your incident response procedure. While this could be a full blog post unto itself, knowing what to do if a breach is detected is fundamental to a successful risk management plan. This should outline the steps to take when triggered, including what to do, who to contact, and what follow-up is required for preventing this type of occurrence from happening again.

With security controls and measures in place, you will be able mitigate the effects of cyberattacks and be proactive in future avoidance.

5. Create a dynamic security culture

This is potentially one of the most important elements in the entire cyber security plan. You can adopt a strong security strategy and have great resources, but if your staff and stakeholders aren't on board, how successful will it be?

Leadership begins this culture shift by ensuring that a security plan is created and that everyone is well-informed about it. The plan then needs to be implemented, disseminated, and adopted. This should include awareness training for all employees, frequent refresh sessions, regular communications with updates and reminders, and plenty of beneficial resources.

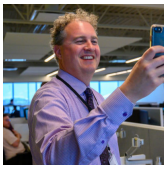
It is crucial to emphasize that security is everyone's responsibility and that even simple mistakes can have devastating consequences. A single infected email opened by an unsuspecting employee can cause a severe data breach. This can result in disruption, financial damages, and a hit to your reputation. People are imperative to the success of every cyber security risk management plan and they need to be incorporated appropriately.

What are you waiting for?

Having an effective and continually improving cyber security management plan is not just an option– it is a necessity. No matter what industry you are in, protecting the data of your company and clients is essential. Emphasizing these 5 areas will help focus your efforts and have you on the right track to a new or better cyber security management plan.

Not sure how to start?

WBM Technologies is one of Canada's top IT solutions providers. If you are interested in learning more about cyber security, or just need to get started, please contact us today.



Cam Breen

Cam is on the marketing team at WBM Technologies and has helped them become one of the best and fastest growing IT solution providers in Canada. Cam is passionate about finding powerful stories of innovation, achievement and success within the Western Canadian IT community, and sharing those stories for all to learn from (and celebrate!). Cam and his family live in Calgary, AB where they love finding new adventures to share together—big or small.

Connect on LinkedIn