Spirity
TOMORROW;TODAY

Five tips to keep your organization protected and compliant even without an in-house CISO

Content

Introduction

It’s no secret that cyberthreats pose an existential threat to your business. From ransomware to noncompliance penalties – the dangers are clear and present.

SME/SMBs realize that they need in-house, c-level, ongoing and strategic cybersecurity guidance. They need someone with his or her finger on the pulse - who can assess risks and vulnerabilities, create and execute a comprehensive cybersecurity plan, ensure compliance and safeguard business continuity.

Yet unlike large enterprises, most small and medium businesses simply don’t have the resources to bring a full-time, experienced Chief Information Security Officer (CISO) on board. Finding, hiring and retaining a CISO is one of the most challenging and expensive human resources challenges. The benefits are clear...but so are the costs.

Even if an in-house CISO is not in your current scope, you can still take meaningful steps towards a solid cybersecurity strategy and actionable cybersecurity policies, leveraging your existing IT resources. To get started, here are five things your team should be doing, yesterday...

The Five Tips

Tip 1
Know your assets

In cybersecurity as in life, you can't protect what you don't understand. It's crucial to find and map both internal and external assets, no matter how far downstream they may be. And once you know what you've got, you still need to understand which (if any) assets are vulnerable, and how so.

The problem is that a manual cyber asset inventory for an SME can take tens of hours of labor - and needs to happen at least monthly to be effective. And IT ecosystems are dynamic. That means that as soon as an assessment is conducted, it's obsolete - leaving you exposed to new and unknown gaps in security.

→ **ACTION ITEM:** There are many free or relatively inexpensive commercial platforms that help you identify and classify compute and storage assets. These tools not only offer an automatic assessment, they also maintain a continuously-updated status database for each asset. This means that when an update or patch is installed, your assessment is automatically updated, too. Check out Rumble or Axonius to get started.

Tip 2

Know your Data

It's easy to underestimate the volume and breadth of data held by your organisation, especially with the increasing use of third-party SaaS platforms, used to handle different business processes. Data classification is the process of categorizing data into relevant subgroups so that it is easier to find, retrieve, and use.

If you have already classified storage assets, one way to do it is to review the data held on each asset, whether it is publicly available, commercial or personal, and it's level of sensitivity. This inventory will be critical when putting together a cybersecurity plan, ensuring regulatory compliance and applying or renewing cyber insurance.

→

ACTION ITEM: Ensure you know what type of data you deal with. Data is typically classified into four categories:

- **Public data:** data which is freely accessible to the public. It can be freely used, reused, and redistributed without repercussions.
- **Internal-only data:** This type of data is strictly accessible to internal company personnel or internal employees who are granted access.
- **Confidential data:** Access to confidential data requires specific authorization and/or clearance. Types of confidential data might include Social Security numbers, cardholder data, M&A documents, and more.
- **Restricted data:** Restricted data includes data that, if compromised or accessed without authorization, could lead to criminal charges and massive legal fines or cause irreparable damage to the company.

There are many inexpensive tools to support data classification. Broadly speaking they are either manual, automated or hybrid.

Tip 3

Understand compliance requirements

Compliance is top of mind in all companies, especially SMEs and SMBs. Failure to comply with regulations can result in hefty fines that damage your bottom line. And compliance issues when publicly revealed can seriously damage your company's hard-won reputation with both customers and employees. What's more, today liability extends beyond the company itself. CEOs, managing directors and board members are personally liable for implementing and monitoring compliance systems.

In the tangled web that is compliance, one basic challenge for SMEs and SMBs is to identify what exactly they need to comply with. Frequently, organizations end up trying to comply with frameworks that don't actually apply to them. And when they try to do so - it can be a daunting, resource-consuming task. The fact is that most compliance frameworks require basic steps towards policy organization and accountability rather than an extensive technical implementation. So once you know which requirements exactly you need to meet, many tasks can be handled by your existing staff using freely available templates.

→ **ACTION ITEM:** Before you spend money to tell you what to do, do your homework and understand the broad strokes of what you need based on where you're located, what you do and where you customers are.

For example, even if you use a third-party credit card processor, you may need to be PCI compliant. Check the PCI standards that apply to you and ensure (for instance) that you're not unknowingly processing or handling PII. Similarly, under GDPR even if you're a US company, you need to be compliant to do business in the EU. Check carefully that none of your IT infrastructure uses providers with EU-based assets, because if they do, GDPR applies.

Tip 4

Cyber insurance, smartly

Cyber insurance has become a precondition of doing business in many sectors. For customers, partners and investors – if you don't have cyber insurance, many organizations will not do business with you.

At the same time, the cyber insurance landscape has changed dramatically in recent years. Today, insurers are no longer willing to rely on simple cybersecurity checklists for policy underwriting and may simply not offer coverage if a cyber insurance prospect doesn't meet a growing list of demands.

For SMEs and SMBs, who lack both the deep pockets and the in-house resources their enterprise colleagues enjoy, this is a sea change. Companies unwilling or unable to meet and verify compliance with these demands will pay increased premiums, suffer reduced coverage, or find themselves uninsurable.

→ **ACTION ITEM:** Get cyber insurance. But do so smartly. Cover all your bases and understand what the exact requirements are.

What's more, despite the tight market, you can both negotiate rates and scope of coverage. For example, ensure that your coverage includes ransomware, and if so, up to what amount?

Tip 5

Use a vCISO Service

A CISO continuously assesses your organization's cybersecurity posture, risk level and compliance gaps, builds a plan to remediate the gaps and manages its ongoing execution and optimization.

But most SMBs and SMEs don't necessarily need a full-time, in-house CISO. They can simply leverage Virtual CISO (vCISO) services provided by their managed service provider – and get everything an in-house CISO would provide – at a fraction of the cost.

vCISO services often use technological platforms to manage your organization's security posture, risk level and compliance readiness, that allow you to get full visibility into the existing gaps and progress that have been made.

→ **ACTION ITEM:** Start using vCISO Services - have a cybersecurity expert define and manage your organization's security strategy, assess your current risk and compliance posture, generate policies that are tailored for your organization, create a remediation plan, ensure execution and track progress over time.

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/virtual-ciso

to learn more.