C&W Business

Creating, maintaining, and elevating your security posture

Many organisations purchase security services on an ad hoc basis. A new threat emerges; they examine tools to address it and then deploy one. This approach is often born out of necessity, but there is a better way to manage the threat landscape—that is, to take a more holistic approach in establishing the company's security posture.

An organisation's cybersecurity posture refers to its ability, strength, and overall readiness to thwart a potential attack. It assesses all the applications in place, as well as the products, controls, tools, processes, policies, and training programmes that a business has implemented to protect itself from outside threats.

Caribbean businesses move quickly today, much faster than they did in the past. Evaluating their security posture holistically enables them to step out, recognise how everything fits together, and, most importantly, understand what pieces are missing.

Fortify your security posture

Without a clear understanding of its security condition, an organisation will be vulnerable to attack. Nowadays, the threat landscape is quite significant. Cybercrime-inflicted damages estimated at $8.4 trillion globally in 2022[1], and the number is expected to reach $10.5 trillion in 2025[2]. Those damages go beyond the immediate and direct impacts. They also include business disruption, reputational damage, data breaches, financial disruption, regulatory penalties, compensatory payments, and legal troubles.

To create and maintain a strong security posture, an organisation must evaluate its technology systems, processes, and resources. Corporations then need to think like a hacker and identify where they may be vulnerable.

It requires a cross-functional, company-wide strategy—usually driven by the information security and workplace technology teams, backed by senior sponsorship from the business. This cross-functional team should ask themselves:

- Do we have a clear view of all of our systems and applications?
- Is there a comprehensive understanding of the types of threats and vulnerabilities in the IT ecosystem, company business applications, and security tools?
- Are there tools and processes in place to detect and mitigate attacks?
- How quickly can we respond to an attack?
- How can we prevent them?
- Do we have an incident response plan in place, with accountable owners clearly identified?
- Are these individuals aware of their responsibilities in this scenario?

With these questions answered, it is time to take a closer look at the organisation’s technology assets.

[1] Homeland Security - Secure Cyberspace and Critical Infrastructure

[2] Forbes - 10.5 Trillion Reasons Why We Need A United Response To Cyber Risk

Inventory all technology assets

The first step in the process is determining what technology the enterprise has in place. The reality is that many businesses struggle to draw their technology footprint. Departments buy systems as needed, often without IT's approval or knowledge. Older systems are sometimes forgotten. An audit establishes the baseline for what has to be protected.

Conduct a security assessment

Next up is looking at the technology and business assets through a security lens and map assets against potential vulnerabilities—as there are many—that adversaries use to break into a business network and profit. Malware, ransomware, viruses, compromised credentials, phishing, inadequate software patching, device misconfigurations, and poor encryption provide unguarded entryways for outsiders.

Create a map of your attack surface

The asset inventory and attack vectors make up the attack surface. Knowing which of its assets and the ways in which attackers may try to compromise them guides the business in fortifying its security posture.

Then, they list the controls already in place to detect, prevent, and respond to security risks. Do they have firewalls? Have they deployed intrusion detection systems? After identification, businesses need to assess the effectiveness of their tools and processes in preventing security breaches. From this exercise, they can see which areas need to be reinforced.

Identify business needs and objectives

Networking introduces risk into the organisation. Although a firm's fundamental priority will always be to protect the organisation from all cyberattacks, trade-offs are made in how much of an investment is dedicated to securing its infrastructure.

Buying every possible security solution is not economically feasible. Therefore, understanding the business requirements becomes imperative. These needs determine which security holes can do the most damage. The firm then develops a priority list and starts working its way down from the top of its to-do list. Companies also need to be sure a risk owner has a plan to fix issues before they lead to a breach.

This triage approach allows organisations to then put resources behind mitigating those threats that pose the greatest potential business impact. Enterprises then create a cybersecurity framework to address the threats. The framework provides clear steps: identify potential risks, implement protective measures, detect cyberthreats, respond to security events, and recover after an attack.

Continue to evaluate critical security vulnerabilities

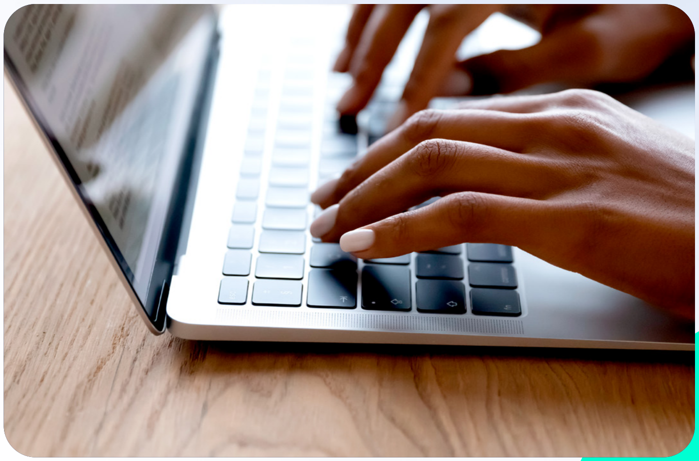
The cybersecurity landscape constantly changes. In order to protect themselves against threats, companies have to continuously monitor and evaluate both emerging risks and the strength of their IT systems. Sometimes, new threats arise quickly and need to be bumped to the top of the priority list.

Conduct cybersecurity training

Employees are the weakest link in the security chain. They know the least about the threats, but they can cause the most damage. Clicking on a phishing email lets an intruder into the company network. Rather than be an entryway, they need to become gatekeepers against security threats.

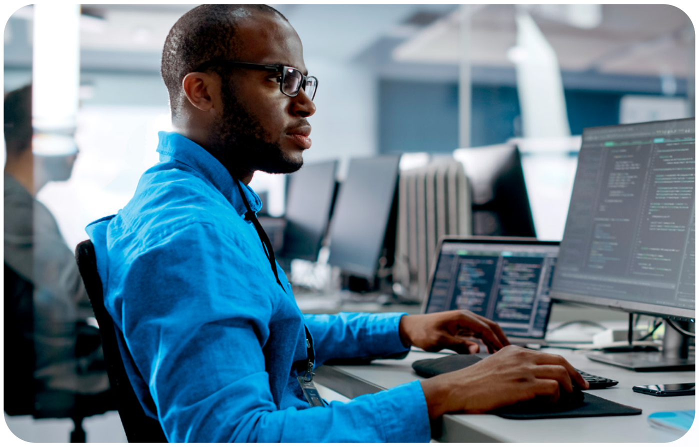
Professional development and cybersecurity education enable them to understand the cybersecurity basics. When running the training, avoid getting bogged down in technical details.

Instead, frame the problem in a business context: how much time and money will they and the company lose if the bad guys are successful? Only companies with well-informed employees can create a strong security perimeter.



Conduct a security assessment

Caribbean enterprises rely more than everon their networks to run their businesses. One downside of growing connectivity is that networks become larger and more complex. Hence, securing them becomes problematic. Third parties specialise in network security. They augment an IT staff's knowledge by adding their experience working with many other businesses.



Networks offer enterprises not only new ways to expand their businesses but also new paths for bad guys to exploit. Understanding how all of their technology and business pieces fit together helps organisations see where holes have arisen and how much damage they may cause. By evaluating their security posture, corporations use that knowledge to close up holes and stay a step ahead of the threat.

C&W Business can help organisations establish a comprehensive security posture by providing the necessary tools, processes, and training programmess to detect and mitigate attacks quickly. Our team of experts works with businesses to identify their unique needs and objectives in order to provide tailored cybersecurity solutions that protect their infrastructure. With C&W Business, organisations can stay ahead of the evolving threat landscape and safeguard themselves from the damaging effects of cybercrime.

At **C&W Business,** we're your catalyst for transformative success. From Cybersecurity to Cloud, Data Centres, Unified Communications, and Connectivity, our streamlined solutions ensure scalability and security. With the Pan-Caribbean region's largest and most reliable network.