CYBER RISK MANAGEMENT

CYBER FACTS & OBSERVATIONS

WHAT IS A CYBER POSTURE AND WHAT IS CYBER RISK MANAGEMENT?

It may just be a naming convention but it's important to understand the order and logic of these activities. Even more confusing is that often words are used interchangeably when the subtleties between them are crucial for your business's bottom line.

Two terms which appear to be synonymous – Cyber posture and Cyber risk management – are not at all the same, and refer to completely different things.

Cyber posture refers to your company's current resilience and attitude to Cyber security threats.

- *How strong are your current defences against possible vulnerabilities?*
- *Is your data as safe as you need it to be?*
- *Is your team up-to-speed with the latest potential threats?*

Cyber risk management, on the other hand, is all about the measures and procedures your company takes to fortify it's posture.

UNPACKING THE DIFFERENCES BETWEEN CYBER POSTURE AND CYBER RISK MANAGEMENT

Cyber posture involves taking a holistic, deep dive into your company's defences and evaluating its resilience to threats right now. You can think of your company's Cyber security posture as its overall defence level.

The National Institute of Standards and Technology (NIST) defines Cyber as *"the security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defence of the enterprise and to react as the situation changes."*

In effect, this means that awareness of your company's Cyber posture provides you with insight as to how vulnerable you are to Cyber-attacks and data breaches.

Working with a Cyber security team that understands vulnerabilities will enable you to stay multiple steps ahead of attacks. Determining your Cyber posture is a crucial first step in this process, since it serves as a starting point for your overall Cyber defence strategy.

This is exactly where Cyber risk management enters the picture. Let's begin with a definition:

"Cybersecurity Risk Management means; technologies, practices, policies; that address threats or vulnerabilities in networks, computers, programs and data; flowing from or enabled by connection to digital infrastructure, information systems, or industrial control systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance."

The essence of Cyber risk management is recognising the threats to which your business and vertical market are most vulnerable.

For example, payment pages are critical for eCommerce players, whilst email domain configuration is vital for banks. Product catalogues are crucial for commerce B2C players, but not for banks, and so on.

It's critical for your organisation to possess the know-how to identify and manage the risks associated with its business model.

Huntsman®
Defence-Grade Cyber Security

CYBER POSTURE AND CYBER RISK MANAGEMENT – PRETTY MUCH INDISPENSABLE

Given today's climate, prevention cannot be the only component of Cyber risk management; companies must also have procedures in place of how to respond to Cyber-attacks, aka Incident Response Management.

EVALUATING CYBER POSTURE: INTERNALLY AND EXTERNALLY

Evaluating your company's Cyber posture requires a set of strategies which can be classified into two key approaches: and both are essential to building a strong Cyber security roadmap.

The first phase approach is internal to your company and demands an honest assessment and internal review of your organisation.

- **Data Assessment:** This begins with accounting for your most sensitive data. Who in your organisation has access to which information, and how is it handled? Whether that's an upcoming fashion line, pricing data or a soon-to-be-announced promotion, who in the chain of command is privy to which information? If you're unable to answer these basic questions or identify the most sensitive data in your vertical expertise, protecting your data will be impossible.
- **Incident Response:** Many companies fail to take the pre-emptive step of creating incident response (IR) documentation, but waiting for a vulnerability to be exploited before articulating a response plan is no longer viable. How prepared is your company for the next incident – i.e. do you have clear IR procedures in place? Plus, what are some of the steps that can be automated as part of an IR policy to various threats? For example, when should IR procedures call for closing web interfaces, and when is it more ideal to secure them but keep them open?
- **Security Controls:** Are your company's security controls set up? Ensuring as much is vital for finding potential vulnerabilities and keeping your company safe. Without controls, your other efforts will be for naught.
- **Employee Education:** Your Cyber posture will only be as strong as its weakest link, and all too often the weakest links are your company's employees. In most retail businesses, employees have the authority to process the returns of goods, and in one such case a dishonest employee operated a return fraud scheme on the dark web, enabling people to submit fraudulent refunds. Also, it's impossible to underscore the relationship between human error and Cyber security. Maintaining a robust Cyber posture requires a healthy security culture and a highly engaged team that's committed to learning.

The second phase is external: you also have to go beyond your company's walls to gain an outsider's perspective to begin strengthening its Cyber posture.

Each of these strategies has a common aim of placing your company one step ahead of potential hackers.

- **Attack Simulation:** Pen Tests and other white-hat hacker techniques reveal the readiness of your company's defences. For many companies, Pen Tests are a much-needed wake-up call. As industry experts have begun to realise, "nothing beats the real thing." Data breach emulation can prepare your company like nothing else. Bring in Cybersecurity Experts: Employee education is a crucial piece of the external review, including bringing in experts to help improve employee awareness of Cyber security beyond the very basics, helping them brush up their knowledge.
- **Advanced Security Solutions:** Relying on employee education alone is never enough; investing in advanced technology and/or Cyber security solutions is needed to manage your threats and vulnerabilities proactively.
- **Third Party Vulnerability:** A vulnerability in one of your vendors can be exploited by hackers to gain access to your company's data. For example, earlier this year hackers compromised millions of credit cards used at Saks and Lord & Taylor stores through a weakness in a point-of-sale (POS) system. Before doing business with a vendor, ask about their Cyber defences to ensure they aren't creating security risks for your company.

THE ONGOING WORK OF CYBER DEFENCE

With Cyber criminals constantly developing new ways to exploit vulnerabilities, evaluating your company's Cyber posture is in no way a one-time challenge.

Continuously adapting and evolving dynamically with both internal and external assessments is the name of the game. Neglecting either approach will leave you vulnerable.

EDGE IT GROUP LTD
FUTURE THINKING TECHNOLOGY

0800 808 5270
https://edge.org.uk
enquiries@edge.org.uk