How to Conduct a Cyber Resilience Assessment

What's Cyber Resilience - And Why Does Resilience Matter?

A company's cybersecurity program must be regularly assessed to ensure that it is sufficiently equipped to handle a cyber-attack and aligned with its cybersecurity needs. These assessments test a company's cyber resilience.

But what, exactly, is cyber resilience, and why is it important to a company? According to The National Institute of Standards and Technology, cyber resilience is the "capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources."

In layman's terms, cyber resilience is keeping a company's data secure while detecting and foiling threats before they can do any damage. Cyber resilience has a company's back, making sure all is okay within the cybersecurity arena and giving the proverbial thumbs up to a company that its cybersecurity program and its employees have the strength and skills to overcome even the worst ransomware battle.

Assessing Cyber Resilience in the Modern Enterprise

Just how do companies set about assessing their cyber resilience? This assessment checklist should help virtually any business ascertain its cyber resilience:

1. **Identify** risks and potential cyber-attacks by creating a list of risks, threats, and possible sources of hacking. As Ben Franklin once advised, "An ounce of prevention is worth a pound of cure." Franklin's advice applies to the identification of factors that might lead to a cyber-attack.
2. **Ensure** that current IT resources and assets are protected at all times. Having a list of current plans, policies, procedures, systems, and technologies is vital, as is examining how the company currently responds to data breaches and other attacks.
3. **Test** cybersecurity plans and procedures, identifying potential weaknesses and ferreting out misinformation.
4. **Train** cybersecurity team members so that they know how best to address cyber threats and that they are familiar with the company's cybersecurity systems and software. In addition, every member of the company must be trained on cyber-attacks and must understand each person's role during such an attack.

Assessing Cyber Resilience with Continuous Vigilance: Why Consistency Matters

Routine cyber resilience tests will help safeguard data and teach companies how their cyber security program can be made stronger, thus helping to identify and address potential risks before they arise.

Think of it this way - to maintain the integrity of our teeth, we undergo regular check-ups and cleanings. Similarly, to be cyber resilient, companies must regularly update and enhance their code armor (beef up their cybersecurity programs). Why so diligent? Well, you can bet the bank that cybercriminals are regularly updating and perfecting their own codes in order to wreak havoc on the unfortunate company that has not maintained the integrity of its cybersecurity program.

In addition, companies also need to train their employees so that they will know what to do to properly handle elevated cyber threats and actual cyber-attacks.

Creating a Resilient Enterprise in Today's Threat Landscape

Companies that are cyber resilient can actually benefit from cyber threats and attacks by turning these unfortunate events into learning opportunities to strengthen the company's cyber security programs, thereby experiencing sustainable, inclusive growth.

The bottom line? Companies willing to conduct ongoing cyber resilient assessments, train their employees how to handle cybersecurity events, and closely and routinely examine the company's needs for protecting sensitive data, will be well prepared for any cyber-attack event.