A New Age of Cybersecurity: Why Upskilling Employees Against Ransomware Attacks is More Critical Than Ever

Corporate cyberattacks from ransomware are seeing a sharp global increase. New Leaf Technologies says the best defence is the constant upskilling of employees.

Don't get caught in a hacker's net — protect your company with cybersecurity training.

CAPE TOWN, WESTERN CAPE, SOUTH AFRICA, June 6, 2024 /EINPresswire.com/ -- Among the various types of cyber incidents launched globally, ransomware attacks pose an ongoing threat. According to the annual Kaspersky Incident Response 2023 report, ransomware attacks accounted for every third cybersecurity incident in 2023, and there has been a 30% increase in the number of ransomware groups operating across the globe.

While governments are regularly targeted, such as the April 2024 hack of El Salvador's national cryptocurrency wallet, and Iranian hackers compromising an IT network connected to an Israeli nuclear facility in March this year, businesses have not gone unscathed. Hackers are increasingly targeting businesses for personal or sensitive commercial data that they can use for ransom and are using artificial intelligence (AI) to automate and accelerate those attacks.

> To prevent attacks and mitigate damage, companies need to create a culture of cyber awareness and empower their IT teams through knowledge of current, new, and emerging threats."
>
> *Michael Hanly, CEO of New Leaf Technologies*

One of the biggest recent breaches occurred when a sophisticated SQL injection attack hit file transfer giant MOVEit. The same attack also targeted the U.S. Department of Energy, British Airways, pension funds, non-profits, and more, ultimately affecting 2,771 organisations and over 95 million individuals.

In the healthcare industry, the U.S. UnitedHealth Group confirmed it paid a US$22 million ransom to ransomware group BlackCat to protect 6 TB of sensitive data stolen during a February 2024 Optum ransomware attack. The attack ultimately caused US$872 million in financial damages.

Michael Hanly, CEO of New Leaf Technologies, says BlackCat's attack is a prime example of the rise in Ransomware-as-a-Service (RaaS) platforms. RaaS is a cybercrime business model in which ransomware operators write software, and affiliates pay to launch attacks using the software.

The most recent RaaS attack occurred in May this year, when the Storm-1811 cybercriminal group deployed RaaS Black Basta ransomware to access Microsoft's Quick Assist features, impacting 500 organisations globally. They performed a social engineering attack by pretending to be a trusted contact, such as Microsoft technical support, to gain initial access to target devices.

Hanly warns that although enterprises are high-value targets due to the volume of data they store, smaller companies are often more vulnerable to extorsion due to a lack of resources and updated training. He says that the ransom is just one part of the cost, which racks up quickly when you consider device cost, network cost, downtime, people time, lost opportunity, etc.

According to research by Gartner, human failure and the lack of skilled talent will be responsible for over half of all major cyberattacks by 2025. Hanly says, "Companies need to accept that they'll probably be targeted sooner rather than later. To prevent attacks and mitigate the damage, they need to create a culture of cyber awareness across the company and empower their IT teams through knowledge of current, new, and emerging threats and how to respond quickly to them."

New Leaf Technologies offers first-in-class cybersecurity training that can help businesses cultivate a culture of cyber awareness, empower their workforce with essential skills, and fortify their defences against potential threats, ensuring the protection of their sensitive data, reputation, and overall business continuity.

The course offers customised cybersecurity training programmes that cater to industry-specific challenges and company risk profiles. Enrolling provides experiential learning, interactive simulations, and hands-on exercises for practical experience in identifying and mitigating cyber threats.

About New Leaf Technologies:
New Leaf Technologies is an eLearning company based in South Africa that provides top-of-the-line learning software and services to corporations, training companies, and educational institutions. The company offers over 30,000 off-the-shelf courses and tailor-made course content, along with turnkey design and production services that create holistic eLearning

experiences. For more information about New Leaf Technologies, visit newleaftech.com.

Emma Hanly
EH&Co
hello@emmahanly.com
