EINPRESSWIRE

Protected Harbor Releases Cybersecurity Trend Report and Strategies for Cyberattack Prevention for Businesses

Protected Harbor, a IT Managed Service Provider (MSP), has released its cybersecurity trend report and strategies for cyberattack prevention for businesses

ORANGEBURG, NEW YORK, UNITED STATES, November 9, 2023 /EINPresswire.com/ -- Protected Harbor, a Managed IT Service Provider (MSP) supporting medium and large business and not-for-profits, has released its latest cybersecurity trend report for businesses. The report discusses top cybersecurity threats that are impacting businesses, highlighting the need for awareness, vigilance and network and data protection strategies.

As hackers become more sophisticated, companies are increasingly at risk for ransomware attacks, phishing scams and data breaches. Often, with small budgets and limited resources, these organizations are less likely to implement and invest in effective cybersecurity practices and regularly conduct IT audits, leaving them vulnerable to attacks.

Richard Luna, CEO of Protected Harbor, Provides Cybersecurity Tips for Businesses

Protected Harbor

In 2023, it is estimated that $12.6 billion will be spent on cybersecurity resources, which is up from $5.6 billion in 2018. Experts also expect cyberattacks to cost the global economy $10.5 trillion per year by 2025.

> “With millions of cyberattacks taking place daily, it is not a matter of if, but when an attack will be successful. Our trend report highlights the importance of conducting regular cybersecurity audits”
>
> *Richard Luna, CEO of Protected Harbor*

“With cyberattacks becoming more numerous and with the emergence of AI, it has become much easier for hackers to target and infiltrate networks and data systems. It is crucial for all business owners and IT leaders to understand these threats and take proactive steps now. With millions of attempts taking place every day, it is not a matter of if, but when a cyberattack will be successful. Our trend report highlights areas of vulnerability and the importance of conducting regular cybersecurity audits and reviews,” said Richard Luna, CEO of Protected Harbor.

The Protected Harbor Cybersecurity Trend analysis looked at different areas where businesses face the greatest vulnerabilities. These include: cloud computing, AI, Mobile Devices, Internet of things (IoT), data storage and network access. Below is an overview of findings. In addition, Protected Harbor experts also regularly publish reports and informational blogs to assist businesses in identifying best practices for protecting their data and systems from ransomware, data breaches and other cyber threats.

Cloud Computing:
With more businesses seeking efficient options for on-demand accessing data, cloud computing has grown exponentially. However, many feel “the cloud,” managed by large corporations, is safer and more secure. Cloud services are accessed by many people via third parties, making them vulnerable to attacks. Savvy hackers can breach cloud servers and data, creating the same issues as if they were to compromise an onsite server.

Artificial Intelligence:
According to IBM, the average savings for businesses that utilize AI and automation to detect and mitigate data breaches is $3 million. Today, AI software is being used as a tool by hackers to infiltrate networks and data systems. AI allows hackers to launch thousands, if not millions of attacks very rapidly. To counter these, businesses must leverage the power of AI to defend against such attacks.

Mobile devices:
With employees accessing corporate networks through their mobile devices, users should be on high alert for malware attacks. In 2022, 93 percent of malware attacks were targeted through mobile devices. These methods include phishing emails attempting to steal passwords and URLs that contain malware and viruses.

Cybersecurity Audits:
“The best defense against cyberattacks and data breaches is being proactive and conducting regular cybersecurity audits, tests and reviews. Every business, no matter how big or small,

benefits from having an MSP conduct a cybersecurity audit. It is recommended that every organization conduct an audit at least once every quarter; however, not all companies are the same. For corporations with large amounts of private data that are constantly under attack, such as medical offices and financial institutions, an audit should be conducted, at a minimum, once every two weeks," said Luna.

A cybersecurity audit will analyze and run tests on a company's IT infrastructure to ensure there are no vulnerabilities, threats or weak links in the system. The analysis will provide a detailed report identifying any cyber threats, compromised areas that need to be addressed and proposed solutions.
There are two types of audits which firms will conduct: internal and external.

An internal audit is conducted by a company's in-house IT team. Internal auditors generally have a better understanding of the organization's IT infrastructure and can run tests catered to their system's weaknesses. However, these tests tend to be biased with conflicts of interest.

External audits are led by outside MSPs that specialize in auditing in various industries and professions. Using the industry's latest software tools, they offer non-biased assessments to ensure compliance with industry regulations, standards and legal requirements.
Organizations should also proactively train and educate employees about cyber threats and their causes.

To learn more about Protected Harbor and is cybersecurity expertise, please visit www.protectedharbor.com.

###

Bill Corbett Jr.
Corbett Public Relations
+1 516-428-9327
email us here
Visit us on social media:
Facebook
LinkedIn
Instagram
YouTube