EINPRESSWIRE

October is National Cybersecurity Awareness Month: Are Businesses Prepared to Withstand a Cyberattack?

Cyber Protection is Business's New Superpower. Here Are Integrity's Top 5 Best Practices Every Business Needs to Implement Before the Next Cybersecurity Breach.

BLOOMINGTON, ILLINOIS, USA, September 20, 2021 / EINPresswire.com/ -- Cybercrime increased 600% in 2020 because of the pandemic. Ransomware emerged in 2021 as a national security issue. So, what are the top things businesses can do to protect profits, data and have peace of mind? Integrity has identified the top five actions businesses need to take today.

INTEGRITY TECHNOLOGY SOLUTIONS

Integrity Technology Services is a trusted business & technology partner specializing in cybersecurity and compliance for financial, healthcare, and other regulated industries.

> If you are asking if your small to mid-sized company is at risk, the answer is yes. It isn't a matter of IF you will be attacked, it is a matter of WHEN you will be attacked."
>
> *Scott Stevens, CISSP*

Integrity's Chief Information Security Officer Scott Stevens, a Certified Information Systems Security Professional (CISSP), emphasized the importance of protecting your business prior to an attack. "The risk is real," he said. "Just this year, bad actors attacked multiple schools, financial institutions and hospitals. Once data is accessed, the attacker encrypts it and sells it back to the owner."

• In 2021, hackers who attacked Colonial Pipeline, an oil company, received over $90 million in bitcoin (Business Insider, 2021).
• The average downtime a company experiences after a ransomware attack is 21 days (Sophos, 2021).
• It is estimated a ransomware attack will occur every 11 seconds in 2021 (Cybercrime Magazine, 2019).
• While many of the businesses got their data back, of the 1,263 companies surveyed by Cybereason in 2021, 80% of victims who submitted a ransom payment experienced another attack soon after, and 46% got access to their data but most of it was corrupted.

Stevens continued, “If you are asking if your small to mid-sized company is at risk, the answer is yes. It isn’t a matter of IF you will be attacked, it is a matter of WHEN you will be attacked. Because Integrity’s IT security best practices help protect highly regulated businesses, you can be sure that they have the necessary vigor to withstand attacks against your SMS business.”

Integrity’s Top Five Best Practices

Integrity has developed a set of five best practices that help small-and-medium-size businesses harden their systems against attack, identify their vulnerabilities and plug the holes in their security processes. Here are the five steps they advise businesses to take:

1. Audit your cyber-readiness to understand the multi-faceted potential for cybersecurity vulnerabilities. Attackers often strike secondary targets such as medium-security devices like printers or medical devices, networks (i.e., employees working at home), endpoints (a customer accessing your services on a tablet) and your supply chain members. You are truly only as strong as your weakest link.

2. Promote a culture of cyber security with your people – both employees and customers. Educate both groups. It is very common to find people underutilizing appropriate security measures. Institute best practices like multi-factor authentication. Train employees to identify email phishing. Ensure both groups have strong passwords. Then test the strength of the implementation.

3. Exchange legacy cyber protection for end-to-end, AI-based protection. While having this type of protection won’t stop an attack, it may eliminate loss or significantly reduce it. Traditional antivirus protection is dependent on “signature-based threat identification,” which can’t happen until your data is already breached. With endpoint detection and response, or EDR, unusual behavior is detected, and the system responds automatically to the threat without the need for a human to intervene.

4. Enable multi-factor authentication. Cybercriminals have become adept at stealing login credentials. Even the most-savvy employee is still occasionally duped into clicking on a phishing email. Enabling multi-factor authentication means that no matter how clever the criminal, they will still be missing one or more factors, preventing access.

5. Stay on top of security updates. A great deal of cybercrime is avoidable. Not responding immediately to security updates is like leaving the door to your house open when you know there are thieves in the neighborhood. While security updates may seem mundane, they are anything but. They mean that a company like Microsoft has discovered a security vulnerability that could put your business servers and data at risk. The faster you install that crucial security patch, the safer your business will be.

ABOUT INTEGRITY TECHNOLOGY SOLUTIONS

Integrity Technology Solutions is a Bloomington-based Managed Security Service Provider specializing in compliance and working with regulated businesses and organizations. Integrity helps businesses dealing with sensitive data protect against looming cybersecurity threats Integrity features a fully staffed help desk that provides immediate response and support, a dedicated information security team, and a C-Suite of experienced technology advisement resources ready to help your business. Integrity brings compliance and security expertise to its partners, keeping them in front of an ever-evolving technology landscape. For more information, go to integrityts.com

Christine Heine
Integrity Technology Solutions
+1 309-840-3702
chris.heine@onefire.com