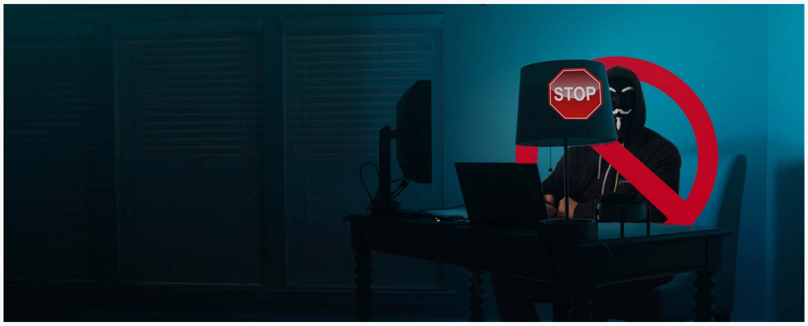
EINPRESSWIRE

# Why Web Security Is Imperative for the Modern Corporation

*Think of how much of your company’s daily operations rely on a stable online network to run, and then imagine what would happen if that were to be compromised.*



OTTAWA, ONTARIO, CANADA, February 26, 2021 /EINPresswire.com/ -- We don’t live in the wild west anymore. Modern day robberies aren’t done by masked outlaws who break in take money – they’re done by sophisticated hackers who can rob unwitting companies blind without them even knowing. For any SMB or enterprise corporation, cyber security must be taken extremely seriously, as with the massive integration of tech with the daily operation of corporations, if a system is hacked and taken down, or data is stolen, it can be absolutely detrimental to the company and cost them not only money, but also client trust, which is often worth even more.

Cyber attacks can often be dismissed as a non-issue or something that takes the backburner. Even when a company will hire out a full security team to guard the actual premises, they may take a more relaxed approach to their online security and data protection. The truth though is that a company’s online security needs to be held at the same – or higher – standard as their physical security measures. The bottom is that not only is there as big a threat online compared to physical, but the effects of an online attack can be astronomical, there’s no telling exactly how much damage a hacker can do to a company’s online system or what information they can steal until it happens.

So what can your company do to prevent an online attack?
What if instead of being reactionary with cyber security measures, your company was proactive? There are cyber security agencies that employ their own “hackers” who can test your online system (referred to as Penetration Testing, or pentesting for short) to find any vulnerabilities, and see what data they can extract. They then provide feedback and a plan on what you can do to secure your systems and protect the data.

In addition to seeing what outside hackers can get access to in your system, these penetration testing companies also conduct internal penetration tests which see what information is accessible via an internal attack. To test this, the pentesting company will take the different access levels that each of your employees have and test the internal network to see if there is any additional data that they would have access to that they are not supposed to see. Again, they would then provide a full report of their findings, and a plan to fix any weaknesses in the systems to mitigate the risk of an actual attack.

Just think of how much of your company’s daily operations rely on a stable online network and need access to various programs to run, and then imagine what would happen if that were to be compromised. This is why cyber security needs to be of paramount importance to corporations. With a properly secured network, your company can save time, money, and protect sensitive data and hold onto the trust of your clients and customers.

Anna Anthony
Ideabytes Inc.
+1 613-355-0411
email us here