Cybersecurity

How business owners can protect data and enhance security

INTERVIEWED BY SUE OSTROWSKI

Justine Kasznica
Shareholder
Babst Calland
412.394.6466
jkasznica@babstcalland.com

Ember Holmes
Associate
Babst Calland
412.394.5492
eholmes@babstcalland.com

WEBSITE: For more information about how to mitigate your risk of a cyberattack, connect with Justine or Ember, or visit www.babstcalland.com.

INSIGHTS Legal Affairs is brought to you by **Babst Calland**.

Every business, no matter how big or small, faces the risk of a cyberattack.

"If you are on the internet or have networked assets — and almost every business does — you are at risk," says Justine Kasznica, a shareholder in Babst Calland's Emerging Technologies, Corporate and Commercial, Mobility, Transport and Safety, and Energy and Natural Resources groups. "The current geo-political climate and the Russia-Ukraine war underscore the paramount importance of cybersecurity to our national security, as Russia has threatened to counter any action the U.S. may make in support of Ukraine with cyberattacks."

Adds Ember Holmes, an associate in the Corporate and Commercial and Emerging Technologies groups of Babst Calland, "It is prudent that all business owners assess their current situation regarding cybersecurity threats, address areas that are lacking and shore up policies."

Smart Business spoke with Kasznica and Holmes about the Biden administration's response to the threat, and how business owners can minimize risk and stay compliant with regulatory requirements.

WHO SHOULD BE CONCERNED ABOUT CYBER THREATS?

Threats to cybersecurity impact every business, and ignoring these is irresponsible and dangerous. Small business owners may not think they are at risk, but they are often perceived as not having the resources larger businesses have, making them targets of malevolent attacks. This is especially true for businesses storing or processing personal or sensitive information.

There are also regulatory issues. Small businesses may be prevented from working in certain industries or with certain customers if their systems don't meet compliance requirements.

HOW CAN A BUSINESS REDUCE THE RISK OF CYBERATTACKS?

Start with a privacy security assessment. Experts ask standard questions and walk through the company's structure and systems to get a baseline assessment of the business's cybersecurity health and its awareness of regulatory requirements. They can then work within the company's budget to propose a streamlined path to compliance and shore up practices that are proactive.

Younger companies need a strategic pathway to become compliant with regulations and best practices and create cybersecurity policies and develop disaster recovery and business continuity plans.

For larger companies, issues often stem from a broad base of operational functions that don't work in concert. Focus on creating consistent, cohesive practices and policies across the organization. It is vital that those dealing with critical infrastructure services adopt a proactive security culture, and evaluate and address their vulnerabilities.

There's not a one-size-fits-all approach because there aren't overarching regulations, only industry-specific advisories and guidance, making it difficult to know how to best tackle cybersecurity. Technology is changing rapidly, and owners who think they are not at risk and fail to take steps to protect themselves are leaving their businesses wide open to a potential attack.

HOW IS THE FEDERAL GOVERNMENT RESPONDING TO THREATS TO AMERICAN CYBERSECURITY?

On March 21, 2022, President Biden released a statement advising that the Administration has received intelligence suggesting that Russia is planning to engage in malicious cyberattacks in retaliation for sanctions imposed in response to its invasion of Ukraine. It alerted business owners, especially those in the critical infrastructure realm, of the potential attacks and make them aware of Shields Up, a campaign to help prepare for, respond to and report cybersecurity incidents. All organizations must be prepared to defend against cyberattacks and to immediately respond if one should occur. The statement outlined steps the Administration has taken to strengthen defenses and strongly urged private business owners in the infrastructure sector to improve their efforts to prevent, detect and respond to cyberattacks by taking advantage of public-private partnerships.

It is critical that all business owners act before an incident occurs, when they are best positioned to secure their systems. Deal with it now — spend the resources, gain cybersecurity literacy in your operations and be ready, because it's not if, but when an attack will occur. ●