Cybersecurity

Guidance on steps to protect your business against cyberattacks

INTERVIEWED BY SUE OSTROWSKI

Ashleigh Krick
Associate
Babst Calland

202.853.3466
akrick@babstcalland.com

WEBSITE: For more information on cybersecurity and how to protect your business, contact Ashleigh or visit www.babstcalland.com.

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

Recent high-profile cybersecurity breaches have highlighted how vulnerable even the largest businesses are to disruption. But even the smallest of businesses face risks, says Ashleigh Krick,

"Organizations may think they are not at risk and do not have valuable information, but they should think again," says Krick, an associate at Babst Calland. "It does not matter what information you have when a hacker just wants money. It's not just about data; it's also about shutting down your business to force you to pay a ransom."

Smart Business spoke with Krick about steps every business can take to protect itself.

HOW HAVE RECENT CYBERATTACKS DRAWN ATTENTION TO THE VULNERABILITY OF BUSINESSES?

Recent cyberattacks on Colonial Pipeline and JBS Foods have demonstrated the cyber vulnerabilities of even our nation's most critical industries. In May, Colonial Pipeline fell prey to a ransomware attack, forcing it to halt transportation of gasoline and other fuels on the largest refined products pipeline on the East Coast. The effect was felt by everyone along the East Coast, as disruption to gasoline supply caused consumer panic and gasoline prices to skyrocket.

Not a month later, JBS Foods, the world's largest processor of fresh beef and pork, was attacked by ransomware, causing its plants to shut down and rendering the business incapable of processing meat. We are still seeing effects from that, which could disrupt the U.S. market and international markets.

In the aftermath of these attacks, the federal government became immediately involved in how businesses were responding to ransomware attacks and questioning whether mandatory cybersecurity standards in the most critical industries are needed.

WHAT SHOULD BUSINESSES BE THINKING ABOUT CYBERSECURITY?

Every business should be thinking about about cybersecurity. First, conduct risk and security vulnerability assessments to understand your cybersecurity practices, threats and vulnerabilities. If you are unable to do an assessment internally, a consulting organization can help.

Cybersecurity risk and security vulnerability assessments identify information assets that could be affected by a cyberattack and evaluate a business's information security risks. The assessment should evaluate where your vulnerabilities lie and identify safeguards to address those. It should identify your most critical facilities, activities and information, and the potential pathways to gain access to your networks.

Also, businesses must assess where they are in terms of cybersecurity policies and practices. How do you describe those activities, and how are those practices protecting your information and systems? Are those policies sufficient, or do they need revisions?

WHAT ARE THE NEXT STEPS?

After evaluating your risks, vulnerabilities and current practices, think about an incident response plan that maps out the response if your business were subjected to a cyberattack. Who would lead that response, and how would you coordinate with internal and external stakeholders?

Review incident response plans often to keep up to date with lessons learned from internal or external cyberattacks and to address new vulnerabilities or potential pathways for malicious actors to gain access to your systems.

It is also important that businesses designate an individual internally to act as a cybersecurity coordinator. This person is charged with establishing and updating procedures, ensuring compliance, reviewing data or security breaches, leading incident response and coordinating with relevant government entities or industry data-sharing organizations. It's nice to have a plan, but if it is not followed, it's worthless.

Finally, with the significant uptick in cybersecurity incidents, businesses need to stay aware of the pathways hackers can use to gain access to their systems. The federal government and states are getting involved in privacy and cybersecurity issues, including calling for changes to laws and regulations. Businesses must stay current on changing laws and regulations and how new obligations affect their operations.

History is likely to repeat itself, and there is the potential for severe consequences to both big industry and small businesses. It's not a question of if, it's a question of when. Businesses must be asking these questions now to prepare and protect against cyberattacks. ●