WESTERN NEW YORK
THE DAILY RECORD
Part of the BRIDGETOWER MEDIA network
■ JUNE 23, 2022

Cybersecurity webinar advice: keep current on employee training, changes in laws, regulations

■ ANDREA DECKHERT

CYBERSECURITY should be a top priority for any business, regardless of its size or industry, according to one legal expert.

"You should be thinking seriously about your data security and privacy," said Anna Mercado Clark, a partner at Phillips Lytle LLP.

Anna Mercado-Clark

Mercado Clark – who leads the law firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice teams – was one of the panelists at last week's RBJ and Daily Record's webinar on cybersecurity.

At the webinar — sponsored by Just Solutions and Phillips Lytle — local experts discussed the latest cybersecurity trends and suggested ways businesses can stay as protected as possible.

Mercado Clark spoke about bad actors' intentions when they target a business for a cyber-attack.

She noted that most hackers are not interested as much in gaining access to a company's data and are, instead, more interested in locking that data. Such an action prevents a business from accessing it and, in turn, impacts the company's day-to-day operations.

Since the company that was compromised wants to regain access to its data to continue business operations, company leaders may be willing to pay a ransom, she explained.

Mercado Clark said it is unlikely a universal federal law related to cybersecurity would come to fruition any time soon but did speak about cybersecurity laws in several states that businesses need to know about.

It doesn't matter if the company has a physical presence in the states with cybersecurity laws, either, she noted, adding that if they have customers there, they are likely subject to those laws.

Such laws relating to cybersecurity will continue to be rolled out, she said, adding that in 2023, four states – Connecticut, Colorado, Virginia and Utah – have cybersecurity laws being implemented.

David Wolf

David Wolf, vice president of Just Solutions, spoke of several ways a business could improve its security posture.

Among them is having a human firewall, Wolf said, adding that employee training can increase awareness of a potential breach or scam that may present itself as suspicious emails or bad links.

Such employee training is key and needs to be done regularly, Wolf said.

"It's not a one and done," he said. "It's a continuous process."

Other ways businesses can protect themselves from cybercriminals that Wolf spoke of included using encryption and having continuous backup of its data, as well as using multifactor authentication.

The latter is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

Claire Farszmil

Claire Farszmil, specialty marketer and account manager with Lawley, said most insurance carriers require businesses to use multifactor authentication to obtain a cybersecurity policy or even have one renewed.

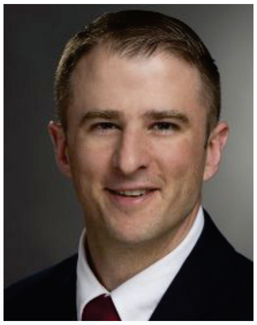
Such policies have increased in popularity – and in price – over the years, as the number of businesses impacted has risen.

> *Having a password is no longer enough security to protect one's data.*
>
> **—CLAIRE FARSZMIL**

Five years ago, if a company had a firewall, cybersecurity policies would cost them around $1,000. Today, several more requirements are necessary, and the average policy price is around $10,000, she noted.

"Having a password is no longer enough security to protect one's data," Farszmil said.

She expects premiums to continue to increase over the next 12 months, as well as carriers tightening up what they are offering.



Justin Pelletier

Justin Pelletier is the director of the Cyber Range and Training Center in Rochester Institute of Technology's ESL Global Cybersecurity Institute.

The institute at RIT is focused on educating and training cybersecurity professionals, developing new cybersecurity and artificial intelligence-based knowledge for industry, academia and government, and performing systems and network security testing for a range of partners.

Pelletier predicts that the use of AI and data analytics will increase when it comes to cybersecurity.

With an increasing number of businesses experiencing a cyber-breach, it often becomes more about how a business handles it and moves forward, he said.

"It doesn't have to be a disaster sentence for the organization if you handle it right," Pelletier said.

Reprinted by EnVeritas Group with permission from The Daily Record.
www.enveritasgroup.com TM062722