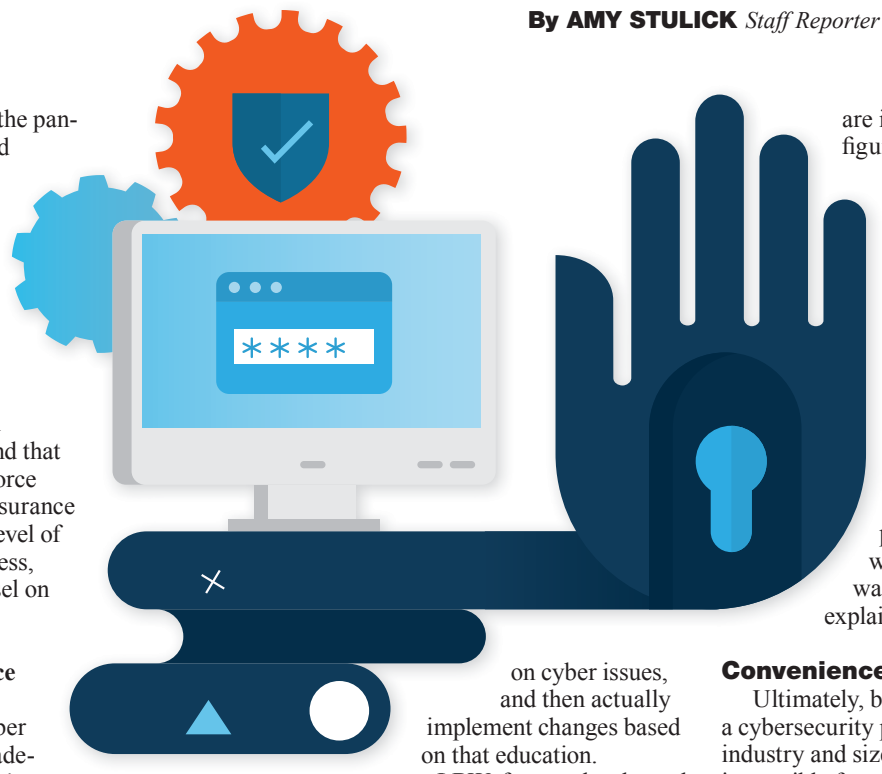
INVISIBLE RISKS

Insurance, legal and tech professionals can limit web liability.

By AMY STULICK *Staff Reporter*



Remote work during the pandemic has multiplied cybersecurity problems and increased liability for businesses, according to risk management professionals in the Valley region.

Companies need to be proactive when it comes to cybersecurity rather than reactionary, experts said, and that means educating the workforce on the threat, purchasing insurance coverage that matches the level of potential threats for a business, or even keeping legal counsel on retainer.

Howard Miller, vice president at **LBW Insurance and Financial Services** in Valencia, started selling cyber insurance in 2007; LBW trademarked his technology division, TechSecure, in 2011.

In its infancy, cyber coverage used to be "a little throw-in for privacy, identity theft" added **Mitzi Like**, chief executive of LBW. Now you can buy it in combination with client coverages or as a standalone policy.

Cost depends on the type of business, how large the business is, what type of data it has and how much data the company is responsible for, Miller said. Niche add-ons such as social engineering coverage were added to cyber insurance packages; it was a reactionary effort to combat hackers that preyed on social interactions.

Howard Miller

Miller said a scenario involving social engineering, or cyber deception in the workplace, could involve an emailed invoice from a supplier. The company pays the supplier only to find out later the supplier's email was hacked, the invoice fabricated and sent to the hacker's account.

"It's essentially getting tricked into giving a cybercriminal your money. The insurance industry, in the later part of 2014, responded with social engineering coverage to carve back that exclusion and provide financial protection, and that has continued into cyber policies so businesses can have a financial backstop," said Miller.

Building defenses

For websites, two-step authentication tools are helpful, or for more regulated industries, a virtual private network may be needed, according to **ITSupportLA**'s **Yuri Aberfeld**.

A VPN transmits data, using software and hardware, through a secure network only accessible by authorized users.

Aberfeld, chief executive of the Tarzana online risk management company, told the Business Journal that the best (and sometimes less expensive) defense businesses can have is an educated workforce from the top down on cyber issues, and then actually implement changes based on that education.

LBW, for one, has hosted webinars on business cybersecurity since 2011 and continued to do so throughout the pandemic.

John Gray, attorney at **Lewis Roca**, added that the strategy for building up a defense to cyber attacks is unique to the business; size, industry and type of content should be factored in.

Lewis Roca has an office in Glendale.

"Really, each organization is unique. What works well for one might not be sufficient for another. Even the most sophisticated cybersecurity practices and most sophisticated entities out there can't eliminate all risk. It's not a question of doing the same thing as everybody else," Gray said.

Aberfeld added that cybercriminals are opportunistic. He likened a cyber attack to a car break-in: if your car is unlocked the first time around, the criminal will try your car first the next time.

"This is a real pandemic that happens around us, and people just allow it to happen because they don't secure their devices, they don't invest into learning the subject," Aberfeld explained. "The best thing you can do is make it challenging. It's not worth their time to mess with you."

Brain Koegle, partner at **Poole & Shaffery** in Santa Clarita, said the law firm's main focus is on preventative maintenance, making sure policies and protocols are in place at client businesses.

John Gray

The firm also has a team of litigation specialists to handle cybersecurity breach claims, but added the payouts for such claims cost more to a business than it would have been to take precautionary measures.

"Our clients say, 'Well, we didn't know.' Ignorance of the law is not a defense. We have very difficult conversations with these clients because many times the cost to fix the breach, to provide monitoring for all those affected, are in the six and sometimes seven figures," said Koegle.

All these lawsuits drive up the cost of cyber insurance, Miller said. "An average ransomware loss is over $133,000, but you have to consider that, if you once get attacked by ransomware, that may not be the complete picture. It may be a diversion for (hackers) to extricate information from your system. Then you can be subject to a privacy lawsuit from the people or companies affected when their confidential info was given unauthorized access," explained Miller.

Convenience factor

Ultimately, businesses will need to find a cybersecurity plan that fits best with their industry and size, without making access impossible for employees and clients.

"The challenge is finding that line between security and convenience. If you need to verify 25 times before you can connect to the website, you'll never try to go to that website again. It's too much work," said Aberfeld.

The ITSupportLA executive expressed concern that employees working from the comfort of their own homes may be using their own WiFi network during the business day, then utilize the same network for Netflix or YouTube videos. There's no separate channel for work-related internet traffic, he said, and that can lead to compromised data.

"A less secure WiFi network generally doesn't exist in an office environment," Gray at Lewis Roca said. "(Remote work) exacerbates existing risk like phishing scams, for example, which might be more effective when employees are in less formal work environments."

Added Gray: "The shift to remote work has also accelerated the trend toward cloud computing, which requires much greater reliance on third-party vendors, and increases the number of avenues for potential risk or issues in cybersecurity."

Cloud computing allows workers to access a shared drive, or common documents, through a software service rather than at a business's physical location, Gray explained. Third parties that offer these services include **Google** and **Microsoft Corp.**, among others.

The Lewis Roca attorney said many of the firm's cybersecurity cases stem from vendor breaches, or attacks on subcontractors for these vendors. The vendor faces litigation or government investigation, and clients are notified their data may have been compromised.

"You rely on third-party providers. Those trusted providers, if they get compromised, can affect a lot of companies. The whole idea of trusting your supply chain has come into importance," added Miller at LBW. "It's a critical factor when you're looking at cybercrime."

Gray said these vendors are often targeted based on who their clients are, or what industries they service.

"If you have a cloud computing vendor that has a platform that is very popular among educational institutions or health care institutions and you're a cybercriminal, you may want to target those types of vendors precisely because you don't have to target each individual of that vendor," explained Gray. "You have arguably some access to all of those different entities which are clients of that particular vendor."

Brian Koegle

Miller added that social engineering scams are easier to pull off when everyone's separated.

Like has seen particular industries preyed on recently with this tactic – real estate and manufacturing.

"Someone goes to wire their deposit or put something into escrow, and all of a sudden it ends up in Russia. ... Real estate with big monies being moved around, that's one area we've seen hit. Escrow companies too," said Like.

Internet crime complaints, according to an FBI report, increased by 70 percent last year compared to 2019. In the first half of 2020, roughly 63 billion records were breached in the U.S.

Poole & Shaffery

HEADQUARTERS: Santa Clarita
BUSINESS: Law firm
SERVICES: Business litigation; business transactions; employment counseling; employment litigation; transportation and trucking; business succession planning; trust administration and disputes; cyber liability; intellectual property; trademarks; land use; governmental affairs.
LOCATIONS: 5
EMPLOYEES: 18

Lewis Roca

BUSINESS: Law firm
SERVICES: IP licensing; IP strategy; internet law and domain disputes; prosecution and litigation for patents; trademarks; and copyrights and trade secrets
LOCATIONS: 9 offices across 5 states
EMPLOYEES: 230-plus lawyers
NOTABLE: Rebranding initiative shortens name, changes logo, updated website

LBW Insurance and Financial Services

HEADQUARTERS: Valencia
CEO: Mitzi Like
BUSINESS: Insurance specializing in commercia, workers' compensation, group benefits, personal, financial and retirement.
NUMBER OF LOCATIONS: 1
EMPLOYEES: 36
NOTABLE: Trademarked TechSecure in 2011, an IT support and service provider for small businesses.