Cybersecurity with Mark Spitz, Business Attorney

As the landscape of cybersecurity treats continues to evolve, businesses must stay vigilant to protect sensitive and proprietary information. To learn more, we spoke with Mark Spitz, a Colorado-based business attorney specializing in small to mid-sized companies with a focus on cybersecurity. With over 15 years of experience in the legal departments of companies, including eight years as a Senior Attorney at Luxottica, Mark understands business in a way many attorneys from traditional law firms do not. His first-hand experience with business principles and drivers builds into his belief that a good business attorney is part of the "team," and an invaluable resource for strategic advice.

Mark began his own practice, Spitz Legal Counsel LLC, to help companies and entrepreneurs maintain a proactive legal structure that allows them to focus on growing their business. Mark also works with companies to help them lower the chances of a cyberattack and reduce their legal exposure and liability in the event of a hack. Companies have become increasingly vulnerable to hackers trying to get company assets--customer data, trade secrets, bank account information and other valuable data required to do business.

"A lot of companies treat cybersecurity as just an IT matter," Mark said, "but it's a broader, company-wide issue. Most hacks come through actions taken by an employee or contractor who doesn't know any better." The biggest threat to cybersecurity isn't technology, but rather the human element. Phishing attacks and related scams (sending fraudulent emails with malicious attachments and links) have become the fastest-growing methods of attack.

While building a practice in this area, Mark found that many companies take a reactive rather than a preventive approach to cybersecurity. Companies often believe they're in lower risk industries or are too small to be of interest. "No one is too small to get hacked," Mark said. "Smaller companies are usually more vulnerable, as they don't invest up front. An ounce of prevention is much more economical than dealing with the cost of a cyberattack." Many don't take the initiative on improving

cybersecurity because they feel overwhelmed by the scope of the problem. They often they don't have the time or budget, or believe the risk is not high enough to take action.

For small to mid-sized businesses unsure where to begin, Mark advises a few key steps that don't require specialized consultants or large investments of capital.

- Make sure your firmware and software are up-to-date. Using out-of-date, unsupported operating systems increases your risk of attack.
- Require employees to set strong passwords and change them periodically.
- Back up sensitive information in secure locations.
- Avoid unsecured Wifi networks and consider investing in virtual private networks (VPNs) while traveling or working out of the office.
- Train employees on the signs of phishing and hacking attempts. They should not be clicking on attachments or links to emails from unknown or suspicious senders
- Explore your industry association resources (for example, supply chain or logistics). Trade groups often have experience with cybersecurity threats and can give recommendations that carry more weight.

Mark recommends a multi-pronged strategic approach to cybersecurity. After building a strong foundation, businesses can look to third party expertise for increased security, such as custom antivirus solutions and cyber-liability insurance policies. "There's a misconception that you can be one-hundred percent secure," Mark said. "You can't. For example, the FTC regulates companies with consumer customers, and requires you to take the right precautions depending on your size, industry, and data type. During an audit, they look at what you've done, and how reasonable the measures were that you took."

Beyond IT involvement, cybersecurity requires training, policies, and procedures reinforced across an organization. "It's not as simple as flipping a switch," he said. "Address the issue by making sure you have the right people in the room and create a culture of cybersecurity from the top down". "Everyone in the organization has to take responsibility, Mark said. "Not just mid- and lower- level employees. The right tone has to come from the top."

Mark believes a strong cybersecurity and legal foundation is important for business growth. To learn more about Mark's legal services and Spitz Legal Counsel, LLC, click here.