Q&A Key Conversations

Interview with Justin Bradley, Account Executive with VTC Insurance Group

Q: Cybercrime has been called one of the fastest growing crimes in the world. Why is that?

Justin: Criminals have found a way to work more efficiently and effectively through cybercrime. Why take the time to burglarize an actual property when you can steal millions of data points in less time and with less effort? Technology has brought us to an unprecedented level of interconnectedness. Cybercriminals have found a way to locate, steal, and even hold ransom our valuables more quickly and easily than ever before. Whether it's banking info, employee social security numbers, or any of the important data you store, they can follow the path of least resistance through your network and right to what they want.

Q: What are some types of cybercrime and why are manufacturers and businesses a leading target for these crimes?

Justin: There are many ways for a criminal to infiltrate your network and steal or cause problems, but recently we've seen a lot of one popular method: Spear Phishing. This is a sophisticated crime in which a fake email is sent to an employee impersonating a supplier or company executive asking for a money transfer or payment. The emails look incredibly authentic, utilizing the impersonated sender's actual email address, email signature, and text they've used in previous emails; much different than Phishing scams of the past. Manufacturers are sometimes targeted because they tend to work with high volumes, high value product/stock, and a complex network of vendors and clients. It's a lucrative target for cybercriminals.

Justin Bradley
VTC Insurance Group

- Has worked in an account management role for businesses across Michigan for over 15 years
- Is a Certified Professional Insurance Agent (CPIA) and helps businesses of all sizes protect themselves and manage their risk with safety programs, risk transfer, mitigation, insurance programs, and more

Q: Where is the biggest exposure for a traditional manufacturing business?

Justin: One of the largest exposures a manufacturer has is their own employees. Computer networks are becoming more integrated with production lines, suppliers, and clients; the cyber supply chains are growing and some employees have digital access to every link of that chain. Whether it's disgruntled employees looking to cause problems or a well-intentioned employee making a bad decision by clicking a link they shouldn't have, the exposure is there. Employees play a critical role in both causing and preventing cybercrime for manufacturers.

Q: What steps should a manufacturer go through to ensure they are as secure as they can be?

Justin: Even if you have a security policy in place and have reviewed it, it's time to review it again. Your security policy should be adaptable, testable, and allow for quick responses to threats. Work with your IT department to add hard controls, such as antivirus software and system restrictions, as well as soft controls like enforcing stricter password protection for employees. Remember, having a stellar security policy in place won't keep the hackers from improving. New threats emerge, more entry points to your network open up, and preventative controls become outdated. You'll need to be proactive to stay ahead of the change.

Q: What are the resources available for a small manufacturer looking to combat cybercrime?

Justin: If you're a small manufacturer looking for help, your best bet is to partner with an outside firm that is an expert. Your commercial insurance agent should be able to advise on mitigating risk with insurance as well as helping implement policies and procedures to prevent losses. An outside IT firm can help with some of those soft controls, as well as implementing system restrictions and offering monitoring services to detect breaches early on.