BLOG

Ransomware & Business Email Compromise Webinar

By Robert H. Rosenzweig

Apr 24, 2019

On Wednesday, April 17th Risk Strategies, in partnership with cyber security experts The Crypsis Group, hosted a webinar looking at Ransomware & Business Email Compromise. We were joined on the webinar by Chris Salsberry, a Senior Director at Crypsis, who has over 20 years of digital and forensic investigative experience. There were a few main takeaways from the webinar:

- People are the greatest weakness in a company's cyber defense, with 52% of incidents resulting from employee negligence.
- The bad actors aren't just trying to steal personal identifiable information but are frequently monitoring email correspondence to manipulate invoices and/or to redirect payroll direct deposit to accounts they control.
- Ransomware has become prevalent.
- Ransomware is more destructive, causing significant downtime and leaving businesses with no choice but to pay.
- Ransomware extortion demands are typically in digital currency and in excess of $250K. Qualified forensic investigative firms such as Crypsis have bitcoin wallets and relationships with bitcoin brokers so that companies don't have to maintain their own bitcoin wallet.
- Employee training and multifactor authentication, are vital.
- Beyond its financial value, cyber insurance provides immediate access to necessary vendors including forensic firms at significantly discounted rates.

Those are the high points, but we covered a lot more important ground. Below you will find the webinar to learn more.

TAGS:
Cyber Liability