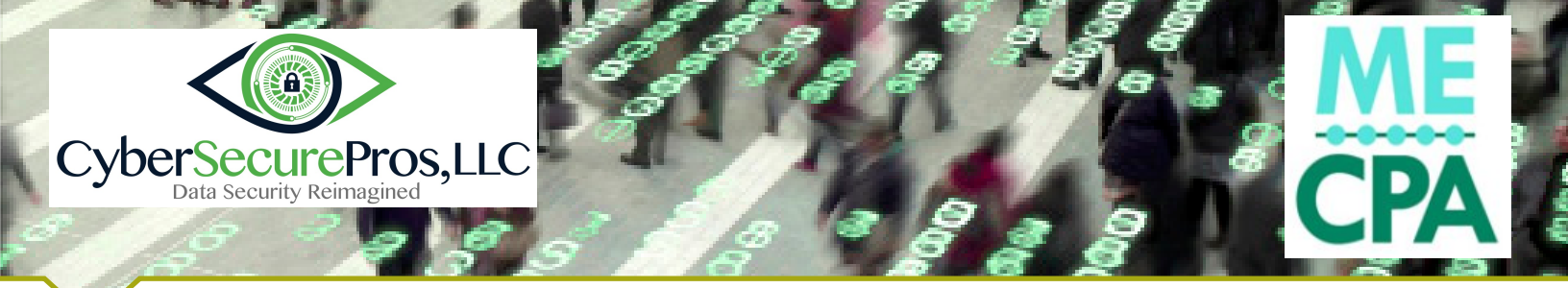

COMMON CYBER INSURANCE OBJECTIONS

Determining the importance of cyber insurance can be challenging. Below are common cyber insurance objections we have heard in the past and our detailed responses to them.

OBJECTION	RESPONSE
"I am not a target for hackers."	Many data breaches occur because of human error; a computer is stolen, left in a cab, or a user does not utilize proper security protocols. A study by *National Cyber Security Alliance* found that one in five small businesses fall victim to cyber crime each year and roughly 60 percent of those businesses go out of business within six months. A study by *PwC US* found that security incidents have increased 66 percent year over year since 2009 with an average of 117,339 cyberattacks and security incidents occurring per day. A study by *Trustwave* found that 98 percent of all computer applications are at risk of being hacked.
"We do not sell goods or services online so we are not a cyber risk."	If you capture and/or store customer and vendor data, you have cyber risk. Cyber policies are designed to address the risk of utilizing technology, computers and internet connectivity while conducting daily business including capturing, storing and using data every day.
"We use vendors for all our IT services."	Based on data regulations, the company that collects data and records from clients is held responsible if a data breach occurs. Legal liability cannot be transferred by contract, therefore, if a point of sale device (i.e. cash register) is comprised, the obligation to notify impacted parties will fall on the business owner, not the vendor who processes or stores payment information. Indemnification agreements typically limit recourse to the value of the contract. An average data breach involving personal financial records could cost a firm hundreds of thousands of dollars, well in excess of the value of most vendor contracts.
"We have top notch security in place."	There is no such thing as "perfect security." Agencies including the Central Intelligence Agency, White House and National Security Agency have been compromised by inside and outside parties, proving that no security solution is impenetrable. Cyber insurance augments even top notch security solutions.
"Our general liability policy will cover the loss."	General liability (GL) policies lack the flexibility to address new and emerging cyber perils. Several significant court decisions have ruled that a GL policy does not cover data privacy breach losses and the Insurance Services Organization released a data loss liability exclusion for GL policies in 2014.
"I don't collect a lot of data."	Every business with employees and/or vendors collects and stores private information including addresses, health information, marital status, bank account information, payment history, human resources records, etc. Additionally, if you sell goods/services, every financial transaction carries protected information including credit card and bank transfer information. The mishandling of such information can lead to a liability or public relations challenge.
"I don't see the value of cyber insurance."	Cyber insurance is more than a product to protect you from a data breach, it covers website media, cyber extortion, digital property replacement, cyber crime, business interruption, privacy liability and network security liability.

Visit **www.cybersecurepros.com** for more information or contact us today to learn more **(207) 536-8701**

Cyber Secure Pros, LLC | 425 Westbrook St | So, Portland ME 04106
Phone: 207-536-8701| www.cybersecurepros.com | info@cybersecurepros.com