



THE CYBER SAVVY BROKER'S GUIDE

Addressing Client Objections



OBJECTION	REBUTTAL	DISCUSSION QUESTIONS
 <p>"I'm not a target of cyber attacks."</p>	<p>Everyone is a target</p> <ul style="list-style-type: none"> Automated attacks make small businesses easier to target Ransomware and funds transfer fraud (FTF) incidents increased by 54% and 40%, respectively* More businesses are becoming targets due to weak security controls 	<ul style="list-style-type: none"> Would your organization be able to operate entirely offline? What would be the revenue and reputational impact of a cyber incident? What security controls does your organization have in place to protect your critical systems and data?
 <p>"We don't rely on technology."</p>	<p>Every technology creates risks</p> <ul style="list-style-type: none"> Essential technology like email, online banking, and digital payments are easily exploited Email compromise can lead to phishing attacks (\$89K* average loss) and funds transfer fraud (\$118K* average loss) Remote collaboration tools and access are easily exploitable and can lead to ransomware (average loss cost of \$300K+*) 	<ul style="list-style-type: none"> Does your organization rely on email, online financial services, or remote collaboration tools? Do your employees and vendors know how to spot a phishing email? What controls do you have in place to secure invoicing and wire transfers?

*Statistics sourced from [Coalition's 2022 Cyber Claims Report](#).

OBJECTION**REBUTTAL****DISCUSSION QUESTIONS**

"I'm already protected from cyber threats."

Protections can (and do) fail

- Cyber security tools are only the first step in mitigating and managing cyber risk
- Security can fail, and your vendors, third parties, and employees can leave you exposed
- Organizations need security *and* insurance to be fully protected

- Do you rely on external third parties to maintain your IT and security?
- How often does that team implement security updates for outdated software?



"I have coverage in my existing insurance policy."

Not all cyber insurance is created equal

- Traditional package policies only cover third-party costs, leaving organizations with coverage gaps
- Cyber insurance now offers holistic coverage (including first-party expenses)
- Active risk management tools and services can help reduce the likelihood of loss

- Does your organization rely on email, online financial services, or remote collaboration tools?
- Do your employees and vendors know how to spot a phishing email?
- What controls do you have in place to secure invoicing and wire transfers?



"Cyber coverage costs too much."

You can't afford *not* to buy cyber insurance

- Recovery costs can multiply quickly, including legal, technical, forensics, and business interruption expenses
- The cost to remediate a ransomware claim has continued to rise over the last few years, increasing 10.5% to \$333K*
- Cyber insurance can be customized for an organization's risk

- Do you have the resources to recover from a cyber incident?
- Do you have vendor service level agreements (SLAs) or contracts defining obligations of each party in

*Statistics sourced from [Coalition's 2022 Cyber Claims Report](#).

Active Cyber Insurance from Coalition was designed to prevent digital risk before it strikes. [Login and start quoting today.](#)