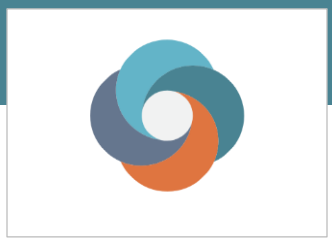


Let's Lay the Groundwork with These Three Key Points

1. Cybersecurity is a company-wide responsibility. It starts at the top with committed leaders who continually listen, learn, share their knowledge, and create a culture of shared security compliance.

2. Cybersecurity isn't a one-size-fits-all solution. Every company has different business needs, strategic goals, and security maturity.

3. Cybersecurity isn't a one-and-done checklist that can be handed off to IT to do. Instead, it's an ongoing process of planning, execution, monitoring, and adapting that involves the entire company.

Start with Two Short Risk Assessments

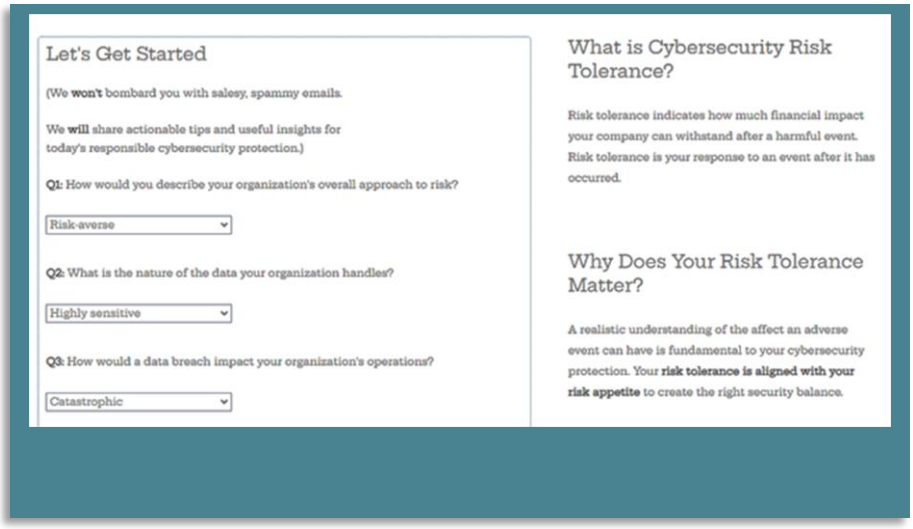
A great way to start the cybersecurity conversation with your clients is to learn more about their security attitude. They've all heard the usual breach warnings and predictions. Some clients will have taken them seriously and implemented rigorous safeguards. Some might have a wait-and-see attitude. Still others will fall somewhere in the middle with a degree of concern and action.

This comes back to the one-size-fits-all fallacy. It's all too common for an IT provider to sell the same collection of security monitoring tools and agents. They frame it as their magical tech stack.

But we're going to approach cybersecurity the way **security best serves your clients**, not a quick revenue generator for your MSP company. Don't worry – both you and your clients will see even greater financial and business benefits in the end.

Understanding Risk Tolerance and Risk Appetite Guides the Conversation

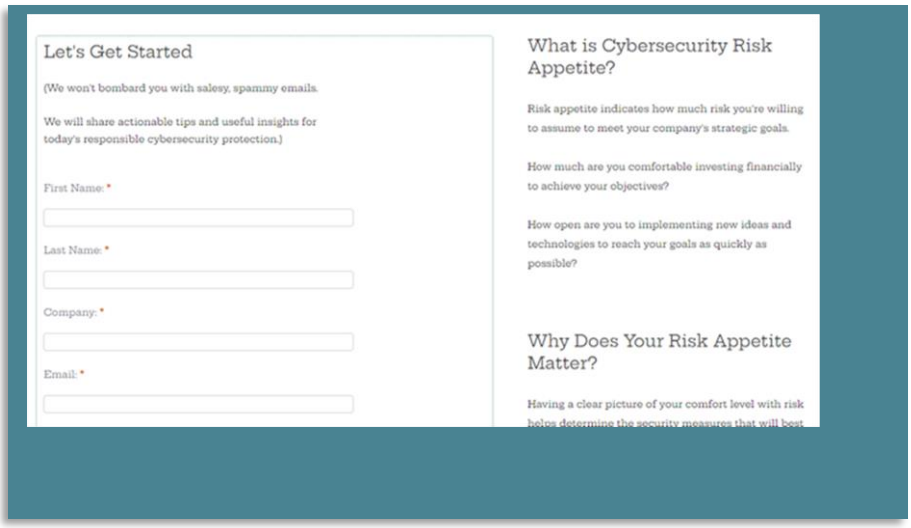
To support you responsibly recommending the right security solution for every client, you and they need a clear understanding of their risk tolerance and risk appetite. Before you go any farther down the cybersecurity solution path, ask your clients to complete these two short risk assessments.



Clarifying your client's **risk tolerance** means understanding how much they can afford to lose if a security event occurs.

Start the Assessment

(*https://quest-technology-group.com/security-risk-tolerance-assessment*)



Clarifying your client's **risk appetite** means understanding how much risk they're willing to assume to achieve long-term goals and strategies.

Start the Assessment

(*https://quest-technology-group.com/security-risk-appetite-assessment*)

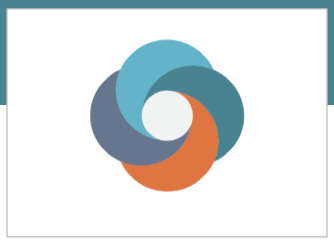
These are by no means an easy shortcut to the right cybersecurity solution. What you will gain are actionable insights that shape the conversation you and your client have next.

The value in completing these short, 20 question assessments is to help you and them have a clear, shared understanding of what risk means to them.

Tips Your Clients Will Appreciate

☑ Reassure them that there are no right and wrong answers.

☑ Clients feel that technology is expensive and complicated. Reassure them that you're not setting them up for IT purchases they don't think they want, need, or can afford.



☑ This is not the first step down a technology rabbit hole they can't escape from. Quite the opposite. The right information will help you identify gaps, potential risks, and the most effective way to address them.

☑ Suggest that your client use your email address instead of theirs on the assessment signup form. That way you will receive an email that their assessment is complete.

After the Assessments Are Complete

Ask your client to forward their completed assessment PDFs to you. Tell them that you will review their information and then schedule a time to discuss with them. Because they have invested their time to take these assessments, follow up within 1-2 business days to schedule your conversation. Their interest is high so don't let the opportunity slip away.

Their scores will give you an overall view of their current risk posture. Now you have a realistic starting point to dig into their actual risk exposure.

Gather all other relevant information you've acquired so far. This includes things like their technology roadmap, software inventory, and network discovery. The more information you have available the more focused your security solutions will become.

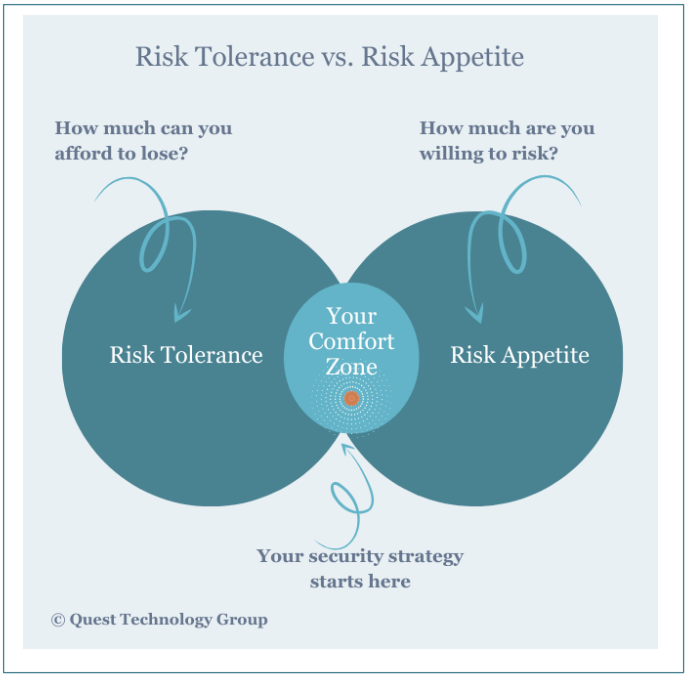
Resist the temptation to quickly suggest a solution based on these short assessments. This is just the beginning.

Wrapping It Up

The goal is for you and your client to have a common starting point for the cybersecurity conversation. This is the beginning, not a quick rush to problem solve. You don't have the foundation laid yet.

Encourage an open and conversational dialogue. Go deeper into any areas that your client is particularly concerned about.

Learn more about their strategic goals and how they align with their risk posture. This is where the right solutions happen.



A Friendly Reminder