Discovering **Your** Company's **Unique** Risk Posture

Quest TECHNOLOGY GROUP

Table of Contents

1. Introduction: Risk is About Business Not Technology

In today's ever-changing, hyperconnected world, company leaders are being continually bombarded with cybersecurity advice and warnings. As the leader of your company, protecting your company and customers is a responsibility you take seriously. The challenge isn't knowing, it's having a clear, practical path that's right for your company.

As company leaders ourselves, we understand how too much information and well-intended advice can lead to doing nothing. So we created two short 20-question each risk assessments that will help you measure your unique risk posture. There are no right and wrong answers because every company has its own immediate needs, long term strategies, and attitude about risk and reward. The assessments will give you valuable insights into your current cybersecurity posture and risk profile.

This ebook is designed to introduce you, as a key decision-maker, and your team to these risk assessments. We'll start with the two types of risk and show you how they impact your company's goals. But we won't leave you with a bunch of vague, confusing technical talk and no clear actions.

As you read through these pages, you'll gain:

- A clear **understanding** of what risk means in plain business words and why it matters to your company
- Practical **guidance** for companies of all sizes because cybersecurity protection is essential
- **Action ideas** to involve the right team members in your risk management
- The **reassurance** that managing your risk can be woven into your existing business and technology foundations
- A **roadmap** for applying your risk posture to your business planning

Action Tips

- Your risk posture will likely change over time as your goals and priorities evolve.
- Revisiting your attitudes about risk should be a regular part of your company's strategic planning.
- Risk management isn't a one-size-fits-all solution.
- Cybersecurity protection isn't a done-once-and-forget-it solution.
- Risk management is a company-wide responsibility that you lead.
- There are no right and wrong risk answers. Your unique business needs, long-term strategic goals, industry regulations, and resources all influence your attitude about risk.

Let's start by discovering the two types of risk and how they impact your company's goals.

2. What is Cybersecurity Risk Tolerance?

Risk tolerance indicates how much you can afford to lose when a security event occurs.

Key elements of cybersecurity risk tolerance include:

1. Your company's acceptable threshold for financial or operational losses
2. Your ability to recover from a security incident
3. Your willingness to invest in preventative measures
4. Your company's level of acceptance with reputational loss

Let's organize your risk tolerance attitude into 3 levels:

☑ **Low Risk Tolerance**: Your company tends to be risk-averse when it comes to cybersecurity.

Security measures you might take include:

- You tend to prioritize minimizing loss, negative events, and damage to your company over convenience.
- You are willing to invest significantly in protective tools, technologies, and measures.
- This approach can provide robust protection, but it can adversely impact operational efficiency.
- Employees might give up more autonomy and control in their day-to-day work activities.

☑ **Moderate Risk Tolerance**: A score in this range suggests a balanced approach to cybersecurity risks.

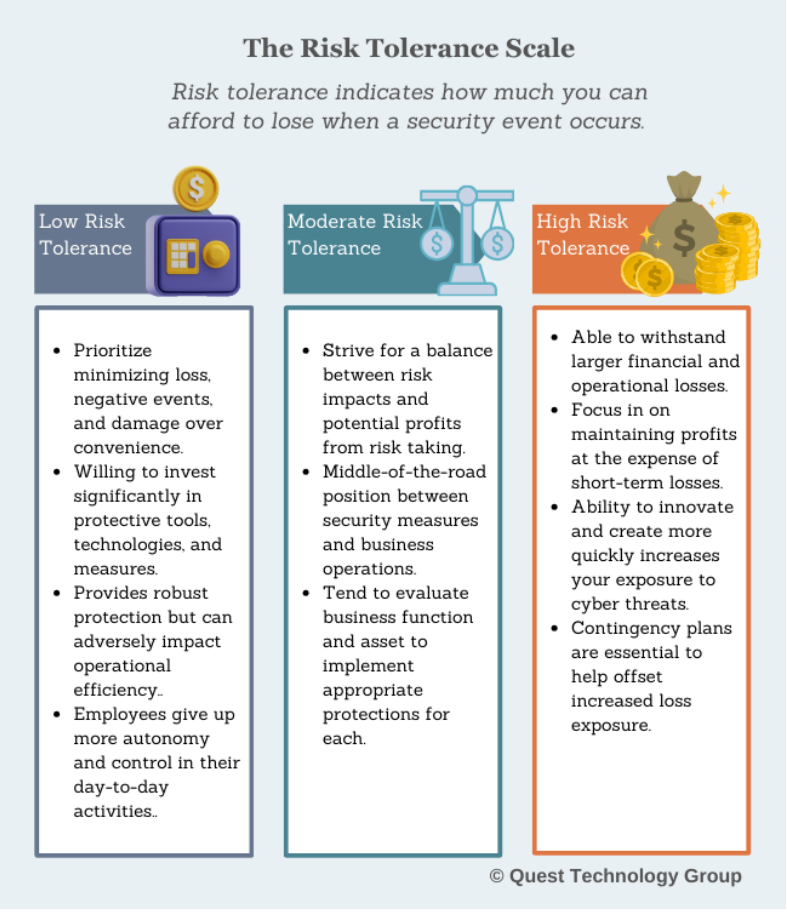
Security measures you might take include:

- You strive for a balance between risk impacts and potential profits from risk-taking.
- You're likely to stay in the middle of the road between security measures and business operations
- You evaluate each business function and asset to implement appropriate protections based on their overall risk exposure.

☑ **High Risk Tolerance**: This score indicates a more risk-tolerant position.

Security measures you might take include:

- You're able to withstand larger financial and operational losses.
- Your focus is on maximizing profits at the expense of short-term losses.
- While your ability to innovate and move quickly is greater, your exposure to cyber threats also increases
- Because you are exposed to significant loss, implementing contingency plans and controls is essential



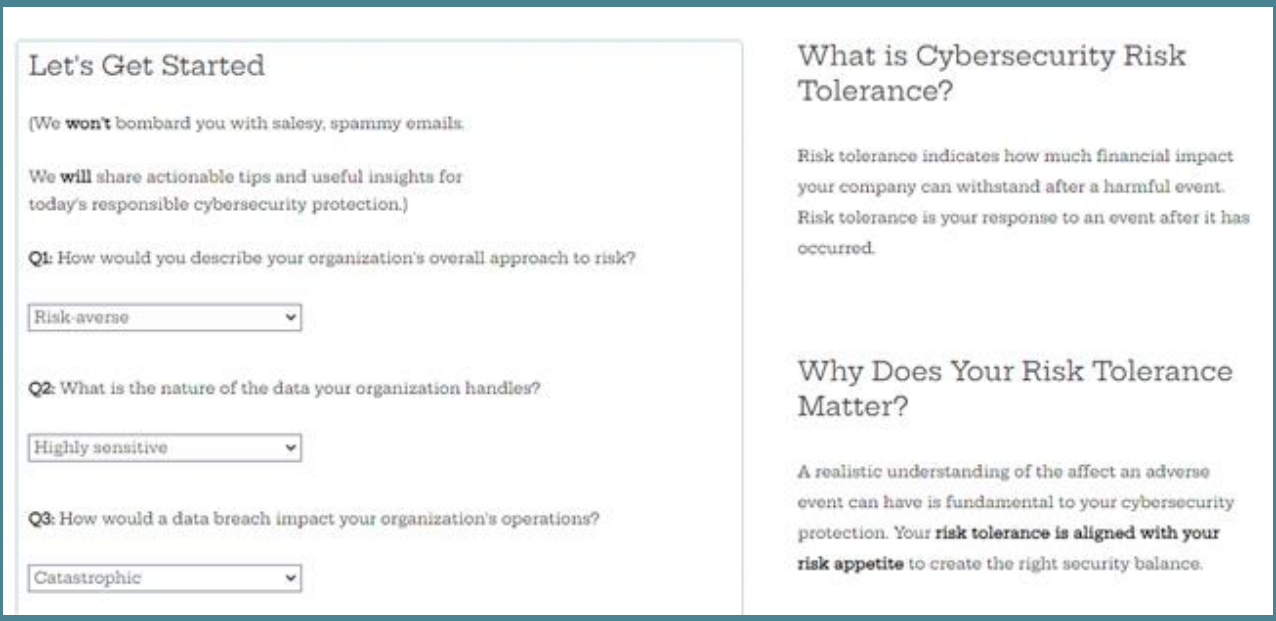
Regardless of where you are today, remember that there is no right and wrong risk position. You aren't being judged or measured against your competitors. It reflects your attitude and risk perception at a given point in time.

As your business changes and evolves, your risk tolerance will likely change as well.

For that reason, it's important to consider your risk score as a dynamic company factor that needs to be reexamined regularly.

Risk awareness is about understanding your current position. You can then make more informed decisions about aligning business strategy and plans with cyber threat realities.

Complete Your Short 20-Question Cybersecurity Risk Tolerance Assessment Now



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

3. What is Cybersecurity Risk Appetite?

Risk appetite indicates how much risk you're willing to assume to achieve your company's long-term goals and strategies. This is more proactive and positive than risk tolerance by focusing on the risks you're prepared to take in pursuit of success.

These are some key characteristics of cybersecurity risk appetite:

1. Willingness to collect and store sensitive customer data that will be used to deliver greater value
2. Comfortable adopting a work from anywhere culture with employee-owned devices part of the technology framework
3. Openness to expanding into new markets and regulatory environments
4. Embrace an early adopter mindset

Here's what your assessment will tell you:

☑ **Low Risk Appetite**: A score in this range indicates that you are risk averse.

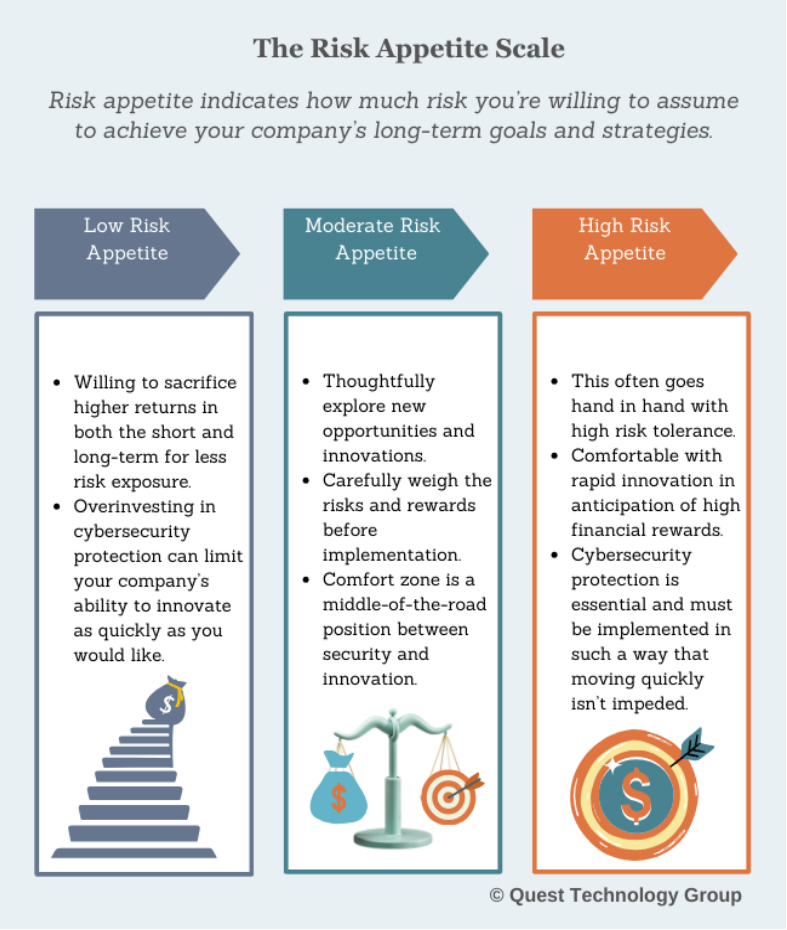
- You are willing to sacrifice higher returns in both the short and long term for less risk exposure.
- While you are willing to invest in cybersecurity protection, you might limit your company's ability to innovate as quickly as you would like.

☑ **Moderate Risk Appetite**: This score indicates a balanced approach to cybersecurity and innovation.

- You thoughtfully explore new opportunities and innovation.
- You carefully weigh the risks and rewards before implementation.
- Your comfort zone is a middle of the road position between security and innovation.

☑ **High Risk Appetite:** In this range, you are likely a high-risk taker.

- This often goes hand in hand with high risk tolerance.
- You are comfortable with rapid innovation in anticipation of high financial rewards.
- Cybersecurity protection needs to be implemented in such a way that moving quickly is not impeded.

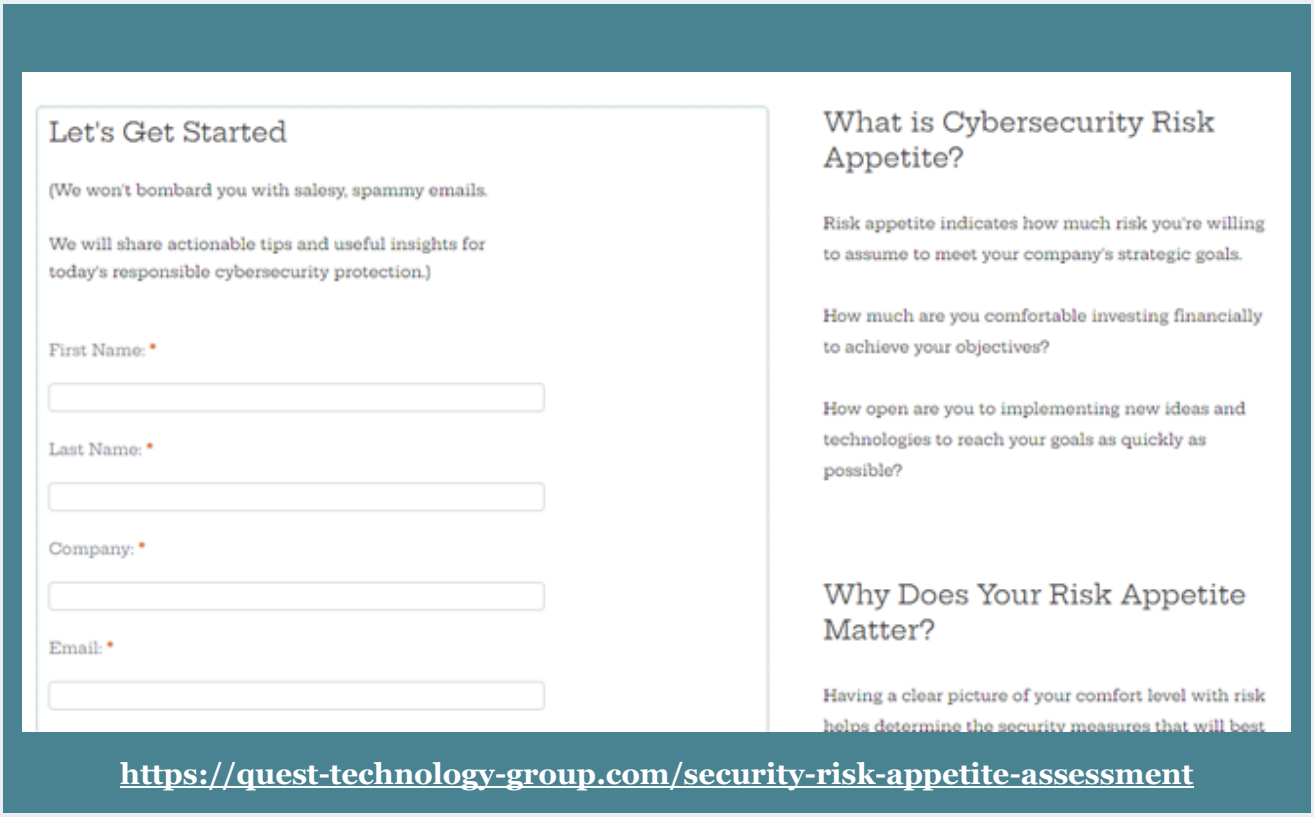


Your risk appetite score, combined with your risk tolerance, provides a comprehensive picture of your organization's cybersecurity posture at any given point in time.

It's crucial to ensure that this posture aligns with your actual threat environment and business needs.

Like your risk tolerance, risk appetite will change over time so it's important to make this measure a regular part of your strategic planning.

Complete Your Short 20-Question Cybersecurity Risk Appetite Assessment Now



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

4. Risk Assessments Create Clarity and Focus on the Right Cybersecurity Goals for Your Company

As your company's leader, you're continually faced with making critical decisions that shape your company's future. One of the most impactful – and often least confident – direction you need to set is your approach to cybersecurity. Starting with a business-first mindset helps clarify your choices and reduce the unnecessary, irrelevant considerations.

Our cybersecurity risk tolerance and risk appetite assessments provide a unique opportunity to clarify your position on digital threats and proactive security steps. These insights will guide your cybersecurity protection that is realistic, practical, and aligns with your company's unique business goals.

Each assessment is 20 questions intended to start your cybersecurity thinking. Invite your leadership team to participate in completing both of these. There are no right or wrong answers because there is no one-size-fits-all business strategy.

Keep in mind that your risk posture will change over time as your business goals and needs change. The approach you take toward cybersecurity protection today might not look like what you've done in the past or where you will be in the future. These questions are simply the starting point for continuous cybersecurity awareness and targeted protection.

Our Promise Before You Get Started

We're customers of products and services just like you are. When we're curious about an offer that looks intriguing – and then asked to hand over our name and an email address – we hit pause. It feels like we've just created one more unwanted spammy flood of sales emails.

We do ask for your name, company, and email address for one reason: to deliver useful, actionable information that will help you move your cybersecurity protection along when you're ready.

☑ As soon as you complete your assessment, we'll email the report to you.

☑ You'll also receive the free ebook After Your Cybersecurity Risk Assessments: Next Steps

☑ We understand that taking time to complete the assessments is an investment. Your time is valuable. You have a business to run. We will share information with you that we would want to receive ourselves. It will be short, actionable, and relevant to building the cybersecurity foundation that's right for your company.

☑ We promise not to annoy, abuse, or send you endless salesy emails that you don't want.

☑ We never share your contact information with anyone. Period.

You're Ready to Start Your Assessments

Risk Appetite **Risk Tolerance**

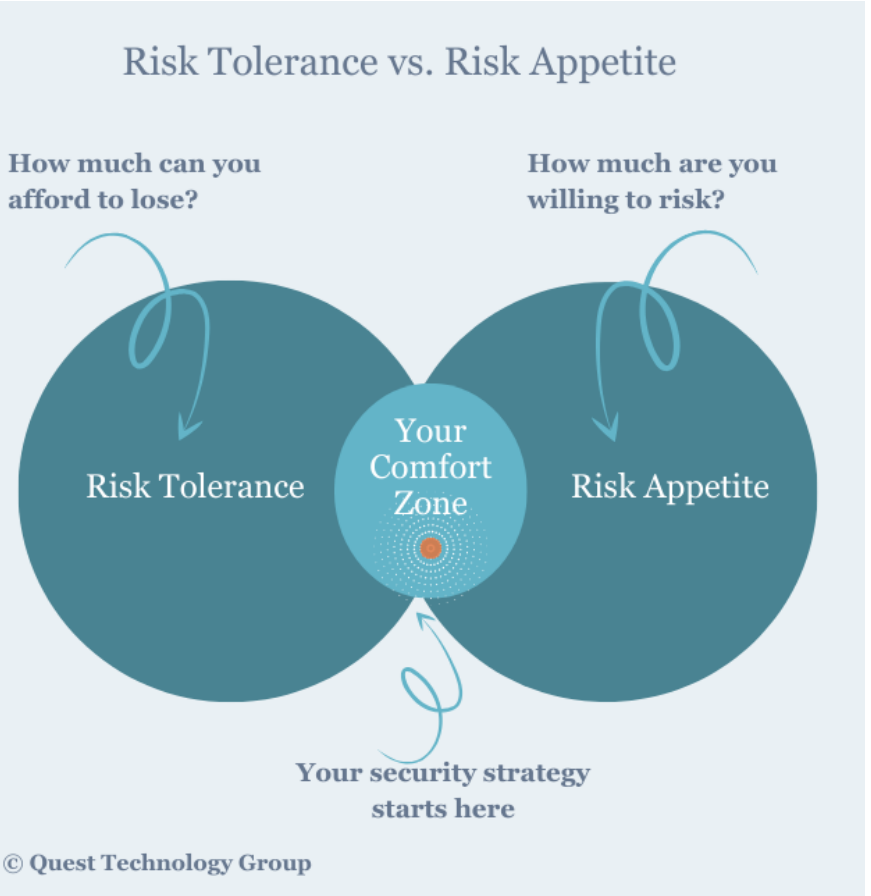
5. What's Next: Putting Your Risk Discovery to Work

Remember we started this conversation with the need to clarify and uncomplicate your cybersecurity protection decisions. When you understand your risk tolerance and risk appetite, you'll find that the implementation steps you take will align with your overall business strategy.

After you complete your assessments, you'll receive the free ebook After Your Cybersecurity Risk Assessments: Next Steps. We encourage you to include your leadership team in reviewing, discussing, building consensus, and planning your next steps.

Action Tips for Getting Started

- ☑ Review the risk scores with your leadership team
- ☑ Approach your cybersecurity protection as a business, not technology, initiative
- ☑ Remember, this isn't a one-and-done project so approach it with a strategic mindset
- ☑ Cybersecurity is complex and requires specialized skills beyond your reliable IT support folks
- ☑ Don't feel like you have to do everything at once. Take the time to carefully consider where the greatest ROI is now and start there.



Start With a No-Salesy No-Obligation Conversation Today

Sometimes you just have a quick question. Maybe taking an assessment feels like a commitment that you're not ready for yet. We get it. After 34 years working hand-in-hand with companies of all sizes and industries, we understand how complicated, time consuming, and costly dealing with technology can feel. We're not here to sell you stuff you don't want. Our goal is to simply share our knowledge and desire to help your business succeed.

Call us: 407.843.6603
Email us: support@quest-technology-group.com