
For Today's Tech
Savvy Leaders
Quest
TECHNOLOGY
GROUP
Cybersecurity Protection
Designed for Your Company's
Unique Goals

Table of Contents

1. Introduction: Cybersecurity Designed for Your Company

In today's hyperconnected world, cybersecurity isn't something that IT does while tucked away in a dark corner. It's a company-wide responsibility guided by committed leaders who continually listen, learn, share their knowledge, and create a culture of shared security compliance. The assessments you've completed offer valuable insights into your current cybersecurity posture and risk profile.

This ebook is designed to help you, as a key decision-maker, and your team understand the implications of your assessment results. We'll show you why a deeper dive into your cybersecurity needs is the important next step for your business's success and resilience. 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 your scores mean and why they matter to your company
- **Insights** into how your risk tolerance and appetite impact your strategic goals
- **Awareness** of the current threat landscape and how that impacts your company's risk position
- The **reassurance** that managing risk can be woven into your existing business and technology foundations
- An **overview** of the current threat landscape and its potential impact on your business
- Key areas where **strategic** cybersecurity investments can yield the highest returns for your business
- A **roadmap** for transforming these insights into actionable strategies

Remember, **cybersecurity isn't a one-size-fits-all solution**. There are no right and wrong risk scores. Your unique business needs, long-term strategic goals, industry regulations, and risk posture all influence the most effective cybersecurity protection for your company.

Your risk assessments are just the beginning of your cybersecurity plan. Every aspect of your business is impacted by the decisions you and your team make so the process needs to be thoughtful, thorough, and grounded by sound information.

Let's start by discovering what your assessment scores reveal about your company's approach to cybersecurity risk.

2. Understanding Your Risk Tolerance Score

Your Score: _____

Date: ____/_____/_____

Risk tolerance indicates how much you can afford to lose when a security event occurs. Let's break down what your score indicates:

☑ **Low Risk Tolerance (0-33)**: If your score falls in this range, 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 (34-66)**: A score in this range suggests a balanced approach to cybersecurity risks.

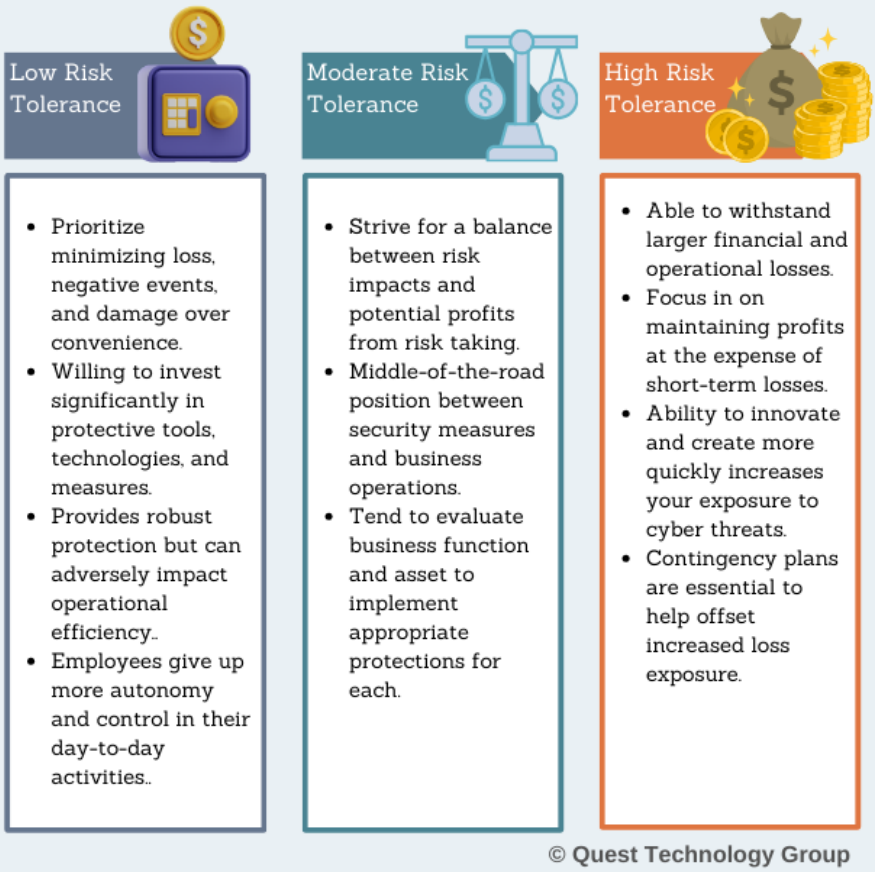
Security measures you might take include:

- 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 (67-100)**: This score indicates a more risk-tolerant position.

Security measures you might 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 your score falls, 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 this 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.

3. Interpreting Your Risk Appetite Results

Your Score: _____

Date: ____/_____/_____

Risk appetite indicates how much risk you're willing to assume to achieve your company's long-term goals and strategies.

Here's what your results might indicate:

☑ **Low Risk Appetite (0-33)**: A score in this range indicates that you are risk averse.

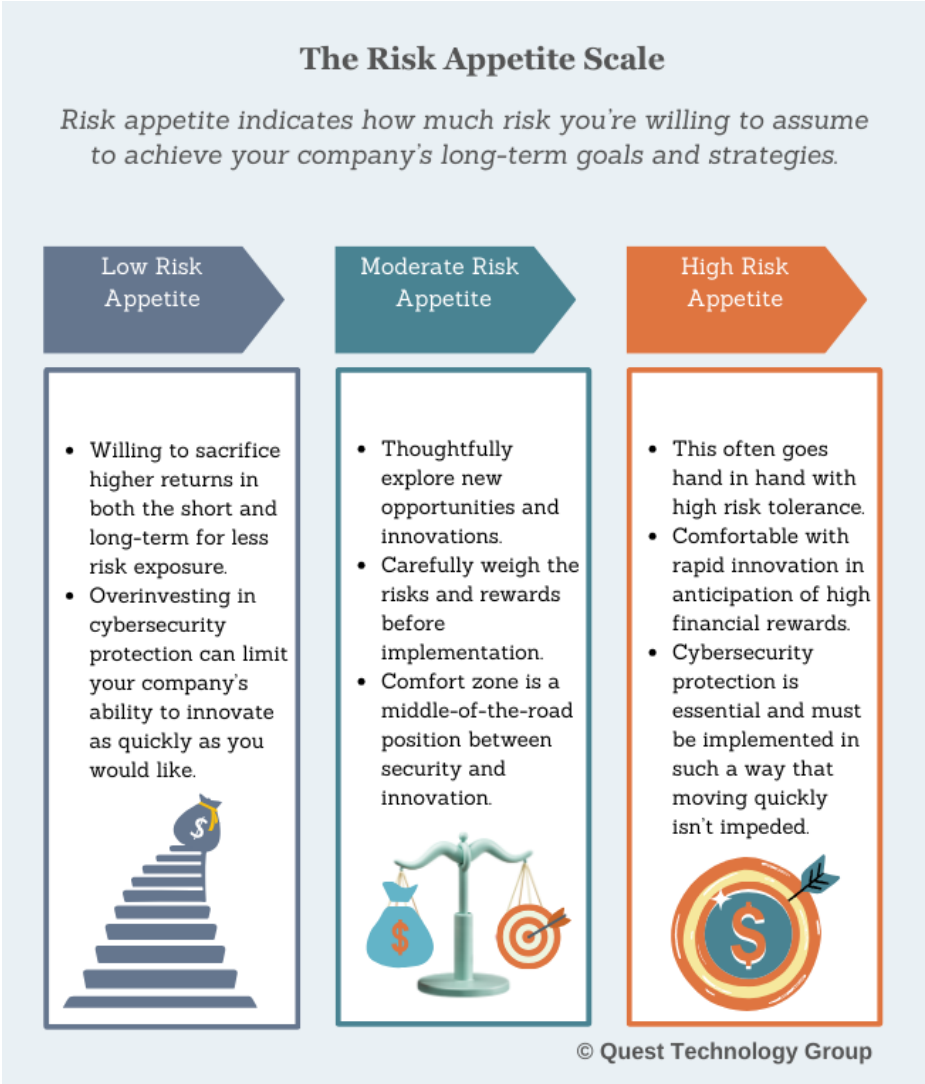
- You are willing to sacrifice higher returns in both the short and long term for less risk exposure.
- While you are willing to invest in cybersecurity protection, you might limit your company's ability to innovate as quickly as you would like.

☑ **Moderate Risk Appetite (34-66)**: 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 (67-100)**: 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.

4. The Ever-Evolving Threat Landscape: Where Are Your Company's Greatest Risks?

The cybersecurity threat landscape is constantly changing, with new vulnerabilities and attack vectors emerging regularly. Staying informed is an ongoing responsibility that company leaders don't' want to overlook. That doesn't mean you can or should become the cybersecurity master. Rather, expanding your knowledge will help you build the sound security foundation with the right skilled team for your company.

Your continued confidence in applying cybersecurity insights to your strategic goals will influence your risk posture over time as well.

Some key cybersecurity attack trends to be aware of include:

- **Ransomware Maturity**: Ransomware attacks are becoming more sophisticated. In addition to the more common data encryption tactic that hackers use to hold a company's data hostage, they are also employing data exfiltration. This fancy tech term, also called data exportation or data extrusion, refers to theft of an individual's or company's data.

- **Supply Chain Attacks**: Attackers are increasingly targeting supply chains to access and disrupt multiple organizations through a single point of entry. Software today typically involves a collection of third-party components, such as APIs, open source code, and proprietary code, instead of the built from the scratch model in the past. This means that every software provider in the chain is a potential target for a compromise. Maintaining security throughout your company is complex and messy.
- **AI-Powered Threats**: Artificial intelligence is being used to create more convincing phishing attempts and to automate attacks. Understanding and mitigating the risks of

AI, both inside and outside your company, is going to be increasingly important and complicated.

- **IoT Vulnerabilities**: As the use of personal devices, work from home, and new tech-enabled devices expands, the potential entry points for cyberattacks grows rapidly. It's important that you consider these often-overlooked access points when you weigh your company's risk exposure.

- **Cloud Security Challenges**: With increased cloud adoption, understanding how your company data is being accessed and protected in multi-cloud environments is crucial. There is a flawed assumption that these third-party cloud providers protect your company assets the way you expect them to. This is part of the conversation that we will have together.

- **Inside Threats:** Your company's and clients' data are among your most valuable assets. Implementing and managing access to this data is essential in today's work from anywhere environment.

- **Distributed Denial of Service (DDoS)Attacks**: Disruption of online services and downtime contribute to loss of revenue and lasting reputation damage.

- **Zero-Day Exploits**: Bad actors are becoming more aggressive and nimbler in waging their attacks. These vulnerabilities occur before patches are available.

Understanding these evolving threats is essential for considering your risk assessment results and designing your cybersecurity strategy.

10 Things You Can Do Now to Help Reduce Your Risks

1. Implement robust endpoint protection and detection (EDR) solutions.
2. Implement a process to validate, ensure timely updates.
3. Develop and regularly test an incident response plan.
4. Implement principle of least privilege.
5. Disable all terminated employee and vendor access immediately.
6. Setup alerts for suspicious activity.
7. Implement an AI use policy.
8. Implement a shadow IT policy.
9. Implement automated software inventory tools
10. Implement strong controls and limit vendor access to only necessary systems.

5. Key Areas of Focus for Modern Cybersecurity: It's Your Company So You Decide

Regardless of your assessment results and based on current threat trends, here are only some of the many critical areas that deserve attention:

Tech Savvy Leadership

The days of offloading technology responsibilities to the IT team are over. Today's strategic leaders understand the significance of technology to their continued success. They are adopting a comfortable relationship with technology and the people who are instrumental in building the right foundation for the company.

As your tech savviness increases, you'll discover that you dread dealing with IT people a lot less. It's likely that your risk tolerance and risk appetite will change as well.

Data Protection

Your company's and customer's data is one of your most valuable assets. Attackers know this, and they will quickly siphon it off every available device without your even being aware. Regardless of your risk posture, robust data protection is non-negotiable. This includes encryption, access controls, and data loss prevention strategies.

Asset Management

Regularly identifying the software, apps, applications, and devices with access to your company's assets is essential. Shadow IT, the use of technology not thoroughly vetted and approved by IT, poses a significant risk to your company, your data, and your customers.

Identity and Access Management

Implementing strong authentication methods and the principle of least privilege can significantly reduce your attack access points Internal housekeeping policies that include user management, strong password policies, and work from anywhere guardrails are today's business basics.

Cloud Security

With the increased reliance on cloud services, ensuring proper configuration and security measures in cloud environments is crucial.

Employee Training and Awareness

Your employees can be both your strongest defenses and weakest links so involve them in your cybersecurity program. Regular, engaging cybersecurity training is essential for companies of all sizes. Employees are eager to learn and feel a part of the company. Involving them not only in the "how" but the "why" will go a long way toward building a company of cyber conscious employees.

Incident Response and Business Continuity

Having a documented plan for responding to breaches, addressing customer impacts, and maintaining operations as the result of a cyber incident is critical for recovery.

Third-Party Risk Management

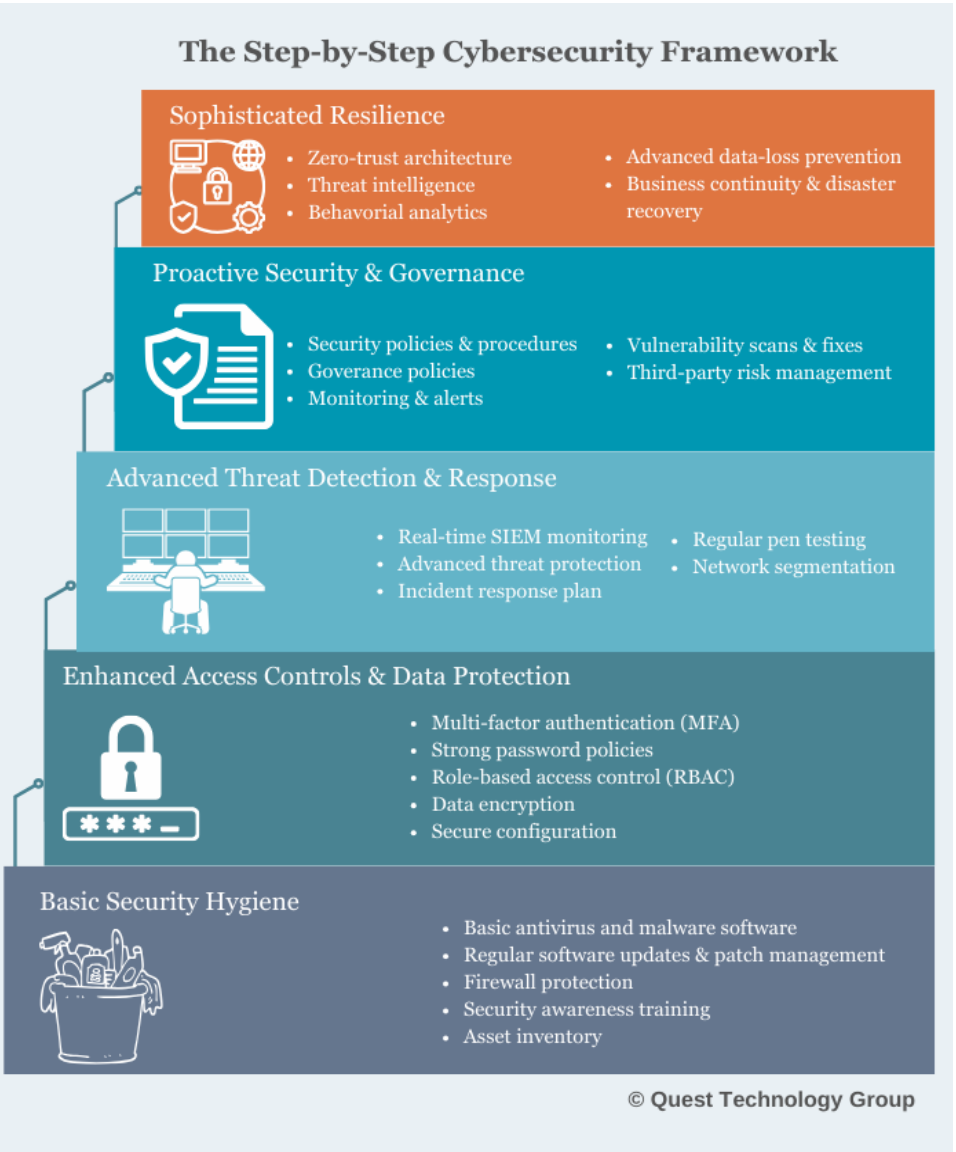
Your cybersecurity protection extends beyond your employees to include vendors and partners. Robust third-party assessment, access management, and monitoring processes are vital.

Cyber Insurance

While cyber insurance is not a defense against a cyber incident, it provides a potential degree of financial recovery in the event of a loss. Insurance companies are increasingly setting clear expectations for what a policyholder must do to participate in risk management. This rightly puts your company in the position to manage your risk, adopt a responsible cybersecurity program, and safeguard your customers as well.

Tips for Simplifying Your Cybersecurity Plan

- Start with the basics. What's essential for your company right now?
- Where are the gaps that create the greatest risk?
- Where are the opportunities that can be tackled with the proper security measures in place?
- Everyone doesn't know everything, and you don't have to become a cybersecurity expert.
- Build the right partnerships with the folks who have a proven track record to help with your priorities.
- Before you dive in, talk with the people who have done this before. You'll be surprised at how willing they are to share their knowledge and expertise with you.
- Measure, assess, adapt, and repeat often.



6. The Business Case for Robust Cybersecurity: Your Company Needs the Right Serving of Security

Investing in cybersecurity is no longer just about preventing losses; it's about creating business value:

- **Customer Trust:** Strong cybersecurity practices can become a competitive advantage, particularly in industries handling sensitive data. Show your customers how you are safeguarding their data.
- **Operational Efficiency:** It's common for employees to resist new, more restrictive, security measures. When efficiency and productivity are valued in the company, these additional workflow steps can feel like a roadblock. Reassure your employees that the short-term effects will quickly fade away, and they will be even more productive and efficient as a result.
- **Innovation Enabler:** Innovation is key to staying nimble and competitive. Moving into new areas involves a higher level of risk that must be anticipated and proactively managed. Planning for a continuous cycle of exploration with appropriate cyber protection is essential for today's strategic company.
- **Regulatory Compliance:** If your company operates under regulatory mandates, such as HIPAA, GDPR, or industry mandates, your cybersecurity measures must align with these.
- **Financial Protection:** The cost of a cyber breach goes far beyond the immediate financial losses. Recovering from reputational damage, losses that extend to your customers, and lost business opportunities can go on for much longer.

7. Next Steps: Tailoring the Cybersecurity Strategy That's Right for You

Your commitment to completing the risk assessments says that you understand the importance of cybersecurity. Now is the time to build on that momentum and take positive action to protect and strengthen your business.

You're invited to schedule a no-obligation conversation with our dedicated business and cybersecurity team. During this taking action session, we 'll:

1. Listen and ask a lot of questions before jumping to premature solutions
2. Explore your company's specific short term needs and long term goals
3. Provide a detailed analysis of your risk assessment results
4. Offer insights tailored to your industry and specific business challenges
5. Identify immediate areas to address and long-term strategic initiatives
6. Discuss how to align your cybersecurity strategy with your business goals
7. Answer any questions you have about enhancing your security posture

Don't wait for a cybersecurity incident to force you into action. No one wants to be in a reactive situation. You need to be in control of your decisions. Be proactive in safeguarding your business, your customers, and your future.

After 34 years working hand-in-hand with companies of all sizes and industries, we understand how complicated, time consuming, and costly this can feel. With the right step-by-step actions that are right for you, the complicated becomes doable.

The Right Cybersecurity Protection Starts with Your Company's Unique Risk Posture

Schedule Your No-Obligation Conversation Today

Your journey toward a more secure and resilient company starts with one conversation. After 34 years working hand-in-hand with companies of all sizes and industries, we understand how complicated, time consuming, and costly this can feel. With the right step-by-step actions that are right for you, the complicated becomes doable.

Call us: 407.843.6603

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