The Cybersecurity Guide for Company Leaders

2022 Edition

Quest
TECHNOLOGY
GROUP

Introduction

When company leaders hear the words “technology”, “IT”, and “cybersecurity”, your first thoughts are all too often:

- It’s complicated.
- It’s expensive.
- Our IT team will take care of it.
- We’re protected from breaches and threats because ______ (fill in the blank).
- We’re a small company so we’re not concerned.
- We have cyber insurance so we’re covered .

It’s no wonder you feel that way.

Technology has become a foundational tool for every company regardless of size, industry, or time in business. You rely on each piece of your technology framework to quietly deliver on its promise. You don’t give much thought to how it actually happens.

You shouldn’t have to. That’s what your IT team does for you.

Business Technology Has Changed

The reality is technology **has** become increasingly complex. The skills required to keep the wheels moving, to ensure that the parts serve your company and your customers have become more specialized.

Company leaders depend on their trusted IT employees and outsourced providers to understand, anticipate, and deliver the right services. The cybersecurity landscape has significantly changed who and how these services and support are delivered. Company leaders are too often left wondering if they have the right people, tools, and guardrails in place to meet today's needs.

Why This Guide Is For Company Leaders

This guide has been created for you, the company leader, to start the conversation with your C-suite and technology team.

Cybersecurity is a company-wide continuous commitment that is shared by everyone. It is no longer responsible to assume cybersecurity is something that IT alone does.

How To Use This Guide

The cybersecurity controls listed in this checklist are by no means all-inclusive. Every company is different, and the controls you decide to implement should be appropriate for you, your employees, and your customers.

Too Much Information Can Get in the Way

Having the right information to make the right decisions can be challenging. This guide lays the foundation for your information gathering. To include everything you need in a single guide would be exhausting. You would quickly quit reading. We certainly would.

Instead, let's start with a list of protections – the **Control** -- that make up a typical business cybersecurity protection plan. Then, we'll introduce links to relevant information. Each of these resources will provide more context to contribute to your decision making.

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top

Start With the Essentials

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top

There are, however, some protections that every company, regardless of size, should implement. These recommendations are based on continuous research and awareness of the cybersecurity exposures actively occurring. These are shown as (•) in the **Top** column.

Start with the Right Team

Your IT team is your first point of contact for day-to-day implementation and support. Their roles in your cybersecurity protection are indicated with (•) in the **Internal IT** column.

For the purposes of this guide, the team includes both your internal IT team as well as your outsourced IT provider.

As we mentioned above, the skills to design, implement, and support your company's

technology framework have changed. We recommend this Who Does What On Your Technology Team guide for the details.

If you have an outsourced IT provider, such as an MSP or MSSP, they should be actively involved in this plan.

We recommend you grab a copy of the free How to Have a Comfortable Cybersecurity Conversation with Your Technology Team. It includes Who Does What On Your Technology Team.

Quite a few of the ongoing services will be provided by established third parties. These are companies with specialized services you will add to your technology framework. These are (•) in the **3rd Party** and **Recurring Expense** columns.

Many of the controls will be implemented one time by your IT team and then regularly monitored for compliance. If these involve an outside partner, they will be shown in the **One-Time Expense** column.

Creating the Roadmap

Each of these controls requires additional step-by-step activities by one or more team members. Beginning with a detailed list of activities makes the implementation manageable and gives everyone in the company a shared roadmap.

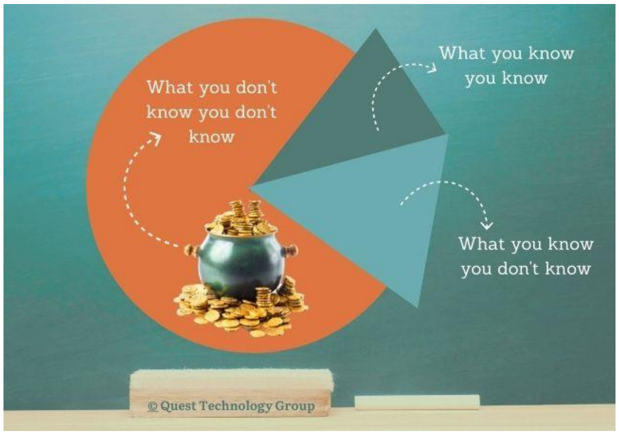
Bringing in an outside business technology partner to work with you on the implementation plan can be invaluable.

Your internal IT folks and outsourced IT provider may be uncomfortable telling you they haven't done some of these activities before. This is very common. It's their job, their partnership with you at stake.

Start by reassuring these valuable team members that saying "I don't know, but I'll learn" is not only acceptable but appreciated.

A Short Blog Post You Might Like

You Don't Know What You Don't Know. And It's OK.


What you don't know you don't know
What you know you know
What you know you don't know
© Quest Technology Group

One Final Note Before We Jump Into the Details

Documenting your cybersecurity program is essential for several reasons including

- Your cyber insurance company will look to this written documentation in the event of a claim. Simply saying you have implemented these controls without written supporting documentation might result in a denial.

- Your customers expect you to protect their valuable data. Clearly communicating this throughout your organization establishes clear expectations for employee behavior.

- Protecting company assets from internal misconduct or unintentional mistakes is reinforced with written policies everyone understands.

- As the company leader, you are ultimately responsible for the integrity, reputation, and protection of your company's assets. A living document serves as the foundation for your strategic planning and leadership throughout your organization.

- Create a sacred project management framework before you get started. This includes a trusted, experienced business technology leader to deal with the tech minutiae, craft working plans, and ensure your strategic needs are understood and met.

Your Cybersecurity Protection Outline

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top
□	Automate all operating system updates and security patches on all company devices		•				•
□	Review all user accounts for access privileges and disable all inactive accounts		•				•
□	Implement advanced endpoint security on all desktops, laptops, and servers		•	•		•	•
□	Implement web filtering to block all malicious and inappropriate websites		•	•		•	•
□	Disable user ability to change desktop, laptop, mobile device security settings.		•				•

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top
☐	Implement multi-factor authentication (MFA) for remote network access, web mail, all cloud applications, and admin user accounts		•	•		•	•
☐	Disable Remote Desktop Protocol (RDP) for external user network access		•				•
☐	Regularly perform full and incremental backups with local and offline remote storage		•	•		•	•
☐	Ensure all backups are infection-free		•	•		•	•
☐	Implement offline air-gapped backups and test regularly		•	•		•	•
☐	Ensure all user accounts are created with least privilege and do not operate as local administrator		•				•

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top
□	Implement and monitor a shadow IT policy	•	•		•		
□	Implement and manage a user-owned device policy	•	•		•		
□	Implement a formal employee onboarding program that includes security awareness training and review of all company technology policies	•	•		•		
□	Implement a standardized new equipment deployment procedures	•	•		•		•
□	Implement a standardized equipment decommissioning and destruction procedure	•	•		•		•
□	Conduct a review of all third-party applications and software for security risks, patch	•	•	•	•		

☑	Control	C-Suite	Internal IT	3rd Party	One-Time Expense	Recurring Expense	Top
	management, access to company data						
☐	Conduct a review of all third-party providers' access to company network, devices, and data.	•	•	•	•		
☐	Implement an Incident Response Plan	•	•		•		
☐	Implement a Disaster Recovery and Business Continuity plan	•	•		•		

Helpful Resources You Might Like

Building Your Business Technology Framework

Having a Comfortable Conversation with Your Technology Team

Every Company Deserves a Business Technology Team Leader

Why Discovering and Managing Shadow IT Matters

How to Build the Business Technology Partnership You Really Want

Uncomplicating Tech Jargon

The Questionary: Baffling Tech Words and Phrases in Simple English

We're Ready to Help You Get Started

Quest Technology Group is committed to helping companies like yours succeed and grow confidently and securely.. If you're ready to get started, just have questions about your current cyber protection or technology framework, we would love to learn more.

Quest Technology Group

407.843.6603

learning@quest-technology-group.com

www.quest-technology-group.com