7 Things to Consider in Your Business Technology Roadmap

You've been growing your business for years. You're geared to take it to the next level. But do you have a technology plan in place that can get you there?

These days, cybersecurity is more complicated than ever before—just ask any dazed CIO or CTO. With the increasing volume, sophistication, and scale of cyberattacks, every firm must prioritize security and compliance in its IT strategy.

Simply put, the stakes are high, folks. A single data breach can be downright devastating to an organization's bottom line and reputation—and, as the saying still goes, an ounce of prevention is worth a pound of cure.

However, organizations can minimize their risk by investing in a comprehensive approach to protecting systems and data before an incident occurs.

Now, What Exactly is a Technology Roadmap?

This might surprise you, but your technology roadmap isn't really about IT at all—it's about your business, your goals, and where you want to go. It's about what you need for your systems to work for you, not against you—and how to ensure those things are properly in place.

Your priorities will undoubtedly vary as your company grows and new possibilities or challenges arise. Consequently, your IT strategy will likewise need to evolve. Creating your technology plan is not a one-time thing. It is a living document that should be updated, reconsidered, and altered as required.

Need help getting started? No worries. Here are seven things to keep in mind when developing your technology roadmap:

1. Optimize Remote Employees

Remote work has become a new way of life for many organizations. In fact, according to the Remote Work Report by Owl Labs, a full 70% of companies are now permanently adopting hybrid and flexible roles.

As a significant part of the modern workforce, remote personnel can make your business more adaptable and efficient. However, with remote working becoming more common, cyberattacks on corporate networks have also increased.

Dealing with these cybersecurity concerns requires teaching and enforcing policies as well as equipping staff with the best tools, tech, and training they need to follow them (such as VPN access, speedy connectivity, and awareness training).

This raises issues around company-owned versus employee-owned devices. At the pandemic's start, several organizations required employees to use their personal laptops. But is the security of those laptops up to par? And if you send computers that belonged to the firm home with employees—are they being adequately managed? Proper technology planning responds to these crucial questions and more.

2. Comply with NIST and CMMC Cybersecurity Regulations

If you work in the government supply chain, you should be familiar with NIST or CMMC compliance. These rules are regularly revised by the National Institute of Standards and Technology to promote cyber security among federal contractors.

Even though most sensitive government data is classified, contractors rely on unclassified data to meet their contractual commitments. NIST 800-171 observance preserves both this and your proprietary data. CMMC is for institutions that interact with the Pentagon or the DOD. This three-year certification certifies your capacity to safeguard unclassified federal data.

Over time, the requirements and certification levels have changed. According to the latest CMMC 2.0 guidelines, there are now three certification levels depending on your firm's cyber security competence: foundational, advanced, and expert. In the end, it funnels down to proper cyber security and data hygiene policies. Since not all controls are technical, meeting compliance can take a significant amount of added labor in many circumstances.

3. Enable Multi-factor Authentication (MFA)

It's no secret that hackers utilize social engineering to target users' identities and passwords. According to the 2020 Verizon Data Breach Investigations Report, lost or stolen credentials—including weak passwords—caused 80% of data breaches. That's right: further proof that humans are cyber security's weakest link.

Although cybercriminals are cunning, multi-factor authentication can halt many attacks. Bypassing MFA requires users to validate their identities. In addition to your usual login data, you must verify your identity using a one-time code or push notification.

MFA works because the hacker cannot replicate the authenticator. On the contrary, if you have MFA available but do not utilize it, a hacker may enable it after gaining control of your account, making it much more difficult, if not impossible, to regain access.

4. Train your Team on Cybersecurity Responsibility

Next up: training! We are living in a time when cybercrime is rampant. The number of malicious actors and their efforts to hack your business, steal your data, and commit fraud has never been higher.

Threats to your company's cybersecurity are no longer just theoretical—they're real and happening every day. In fact, it's estimated that over 1 billion compromised records are floating around the Dark Web alone—and that's just one of many places where sensitive information can be found by those who want to harm your business. It begs the question: Is your team up to speed with the latest security awareness training?

Security Awareness Training: Cybersecurity awareness training is a prominent part of any company's security efforts. It's the only way to make sure your team is educated about cybersecurity's best practices and risks.

It makes sense then why so many businesses are turning to security awareness training as a way to protect themselves against these threats. Security awareness training teaches management and staff how to spot potential hazards and how they can help mitigate them through good practices such as password management and security hygiene at home or on the go.

You should provide ongoing training on topics like phishing scams and social engineering attacks so that your employees continue working towards better security awareness at all times.

5. Prepare for M365 Price Increases Already Taking Place

As the world changes, so does Microsoft. Microsoft 365 is modifying to meet the needs of today's corporate environment. As leaders worldwide seek to prepare their staff for a more flexible, hybrid work environment, it's clear that each business will require a new operating model that transcends people, places, and processes. As such, Microsoft is committed to fostering innovation that helps customers prosper and thrive today and in the future—building on the value they've contributed over the last decade.

With this in mind, Microsoft has increased the price of Microsoft 365 as of March 1, 2022. This move aligns with their vision to help customers become digital-first organizations by making it possible to transform how they connect with people and information, build software solutions, and protect data across their businesses at scale through an integrated set of cloud services.

6. Review Your Backup Strategy

We know you can never be too cautious when it comes to safeguarding your business. That's why we recommend reviewing your backup strategy annually. A recent copy of your data is essential to the success of any business, and ensuring that you are prepped for the unexpected should be a priority.

In today's world, it's necessary to make sure that mission-critical data is being backed up. Many businesses tend to focus on what data is most valuable or which is most costly to reproduce. But given the frequency and sophistication of today's cyberattacks, it's time to revisit that approach and ensure that you're protecting yourself against the worst-case scenario.

If you haven't reviewed your backup strategy in a while or don't even remember what yours looks like, now is a perfect time! Pause and reflect on what would happen if your systems were compromised. Consider how valuable your data truly is, and then make adjustments accordingly. The better and faster you back up your data, the quicker you'll be able to recover from an attack—and in many cases, this can mean saving your business from failure or financial ruin.

7. Replace On-Premises Microsoft Exchange Server

You may think that keeping an Exchange Server in-house is a simple, cost-effective way to manage your company's email, but in reality, it's becoming riskier and riskier.

In reality, many cyber insurance providers refuse to cover companies with an on-premises Exchange Server (or charge exorbitant premiums). Furthermore, according to some IT specialists, Microsoft may not release another version of on-premises Exchange for small and mid-market organizations.

Planning ahead of time for that shift will save you time and money in the long run—and ensure that you're covered from a cybersecurity perspective.

Planning for the Future

Here at a COUPLE of GURUS, we understand that there are so many things clamoring for your attention when you're running a business. You've got sales and marketing to worry about, making sure your customers are happy, developing new products and services… The list goes on. And hey—we get it! We've been working with businesses since 2002. We know what it's like.

But in all of this busyness, don't forget about your technology plan! A good technology plan isn't just about buying the newest stuff or finding a consultant—it's about having an overarching strategy that allows all of your technology systems to work together seamlessly.

Via our cutting-edge Managed IT and Cybersecurity services, our gurus are here to help get your technology in order. No more losing sleep over your IT—we've got this.

Schedule Your Technology Roadmap Assessment

A Technology Roadmap Assessment is an essential part of any business's long-term strategy. Our assessment is designed to help you understand how your IT infrastructure can be improved so that it's more reliable, secure, and efficient—giving you a clear perspective of where your company currently stands in terms of technology, as well as where you wish it to go.

We'll work with you throughout this process to customize a business-aligned plan that meets all of your needs. We then get to work helping you execute it, providing support and coaching along the way! With our Technology Roadmap Assessment results in hand, you can start improving your IT infrastructure for the benefit of your entire company.

What to expect:

- **Full Review of Your IT Ecosystem:** we'll assess your servers, workstations, network (firewalls, etc.), server room, and backup/recovery plan

- **In-depth Diagnostics & Troubleshooting:** identifying and solving problems is what we do best, and we do it as fast and cost-effectively as possible by listening to your concerns and inquiries

- **Productivity Analysis:** gauging whether you have the ideal domain, file solution, cloud computing, and remote-work tools for your needs

- **Clarity & Strategy:** we'll give you a clear view of your IT ecosystem's current health and vulnerabilities, as well as top-notch solutions, options, and suggestions

Ready to take the next leap forward toward enhancing your IT infrastructure? Sign up online or give us a call today!