CYBER COMMAND

7 Technology Shifts Your Business Needs to Make in 2025

Solutions for a Rapidly Changing Business Environment

cybercommand.com

7 Technology Shifts Your Business Needs to Make in 2025

Technology is continuously changing, but 2020 marked the beginning of a new paradigm in modern computing which 2025 is refining and cementing. The world at large moved towards working remotely for most office jobs. That change necessitated large changes to infrastructure and threw gasoline on the fire for the already explosive expansion and growth of cloud platforms and other technology solutions.

Technology is ingrained at every step of the way for a successful (or even unsuccessful) business. It doesn't matter if you run a restaurant or a software development firm, you need computers and technology along the way. Whether it's the payment processor or the end product, modern computing technology is involved.

Neglecting the importance of technology utilization and security in your business is detrimental to your business long-term success.

In the past you only needed antivirus and a basic firewall to protect your devices. Today layers of protection, including extending outside of the office, is critical in defending against ever-changing threats. Besides, security utilizing technology is the way to grow and scale your business, but if not managed properly it can break processes and negatively impact your productivity. Whether technology enables your growth and success, or causes you to fail is up to you, you just need the right resources to leverage technology to support your business.

We'll dive into the 7 most important topics for you to look at right now. These trends impact your business's security (both from hackers and from accidents) as well as efficiency for both workflow and cost. Let's take a look at these trends and see what relevant questions you should be asking your Technology Resource to leverage your IT operational expense into a return on investment for scalable growth.

Technology and the New Decentralized Workplace

We are experiencing an accelerated massive shift in the traditional workplace. We have discovered that many jobs in today's economy can be performed remotely from almost anywhere. Whether your business requires a person onsite, or they can work remote this trend expands the technical options necessary and how much they cost. The more employees you allow to work remote, the more decentralized various office resources get.

Decentralizing the workplace requires a massive amount of work, but can pay dividends when done correctly, or cost your business if done wrong. A decentralized workplace can mean fewer expenses for physical space and on-premise solutions in exchange for a move to the cloud. If you have to make a change anyway, why not make one which provides the most benefit down the line? How are you turning this modern IT necessity into a business advantage?

The new workday has changed for many businesses. Since certain services and stores have changed their hours and availability, sometimes an employee's need for food conflicts with the traditional workday. School requirements have gotten more complex so employees are spending more time outside the old 9-to-5 workday filling in for missed time. While your employees aren't working 24/7, your business may be.

You have to take into account the development of the trust you have between your entire business's data and each employee's home. Every entry point into your organization expands the surface area for hackers or data theft. To provide a secure work from home scenario it takes expertise and management to implement technology that reduces your risk, detects potential issues, and responds to them before they become larger issues. Not to mention, any change to an employee's routines requires policy and training.

1. Cybersecurity

When people hear the term cybersecurity, they immediately think of cybersecurity portrayal in movies or news. This usually leads to anxiety and eventually the individual becomes overwhelmed with fear over their IT safety. Most of this comes from the over sensationalizing in the media and from IT service providers using fear, uncertainty, and doubt to paint a bleak future for the non-technical, small to medium business executive. This does not mean there is not a serious risk of business loss due to cyber criminals. Quite frankly, monetization of cyber-crime is a driving force behind it. According to Cybersecurity Ventures," global cybercrime will reach $10.5 trillion USD annually by 2025."

Obviously, accepting the inevitable by just giving up and ignoring the risks is not a good practice for any company. Having fundamental information allows you to make better decisions to institute the right resources to obtain the right balance for your business. This starts with a clear definition of cybersecurity.

According to CISA, "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information". The use of the term "art" is key here as it implies the requirement of skills and experience. Cybersecurity is not something that can be done alone anymore. The days of installing an antivirus and a basic firewall for complete protection are over. Now, more than ever, it is important that remote users be considered in your cybersecurity strategies. Preventing threats at each point of entry is an important consideration, especially if the device is not connected to your local network. This requires defense in layers and strong protocol to properly manage your organizations overall defense against cyber-attacks.

Having the right IT resources will dynamically evolve your cybersecurity posture through budgeting, management, and response. This will ensure that you are properly allocating and preparing for changes that may impact your organization as industry shifts happen. Cybersecurity is more than just tools such as a next generation firewall, advanced endpoint protection, and email filtering. Response and Remediation plans are also critical components of a good cybersecurity program to fully protect your business. It must also be culturally introduced into your organization. Employees, your most prized assets, are your first line of defense against cyber-attacks. Effective policies and employee training programs are critical aspects of a balanced line of defense to minimize cybersecurity threats.

Cybersecurity is complicated, but the right partner will provide you with peace of mind knowing they are asking the tough questions to proactively protect your organization.

2. Compliance

The increase in digital information storage and exchange has created numerous challenges for technology management. One of the most difficult challenges for IT Management is effectively ensuring regulatory compliance requirements are met. Regulatory compliance requirements are written by agencies to specifically protect information that can expose their constituents to risks such as fraud.

While you will find that there are a lot of common-sense items between the requirements, it is important to adhere to the specific recommendations of each to lower your risk. Not to mention, failure to meet these requirements can result in financial penalties, public disclosure of breaches, and other unanticipated adverse challenges to your business.

So, how does an organization properly accommodate these regulatory items? The first step is to identify what compliance requirements your organization needs to meet. For example, here are a few agencies/regulations have their own individual requirements:

- PCI DSS covers securing and handling the cardholder data environment (CDE).
- Sarbanes-Oxley Act (SOX) ensures the privacy of secure transfer of data to accountable parties.
- HIPAA and the HITECH act protects electronic health records and patient personal information.
- General Data Protections Regulation (GDPR) require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU states.
- Additional state regulations like the California Consumer Protection Act (CPAF) or California Privacy Rights Act (CPRA) further deepen the considerations.

There are some basic things that can be done to help you meet compliance along with adhering to the individual requirements of applicable agencies and/or regulations.

Finding the right technology partner is critical to avoiding compliance failures. They will be instrumental in helping you implement strong data protection/encryption and handling policies, addressing how new technologies like IoT increase your risk, understand ways to reduce risk through proper data sharing, and lastly, how to protect your staff devices regardless of their location.

3. Social Engineering

We all establish relationships and form bonds with others because we are relational beings. Within these relationships there is an inherent trust that takes place regardless of physical presence. This is the fabric that allows for cohesion and collaboration between co-workers within your organization. However, when it comes to technology, social trust can become your biggest risk.

Cybercriminals, also known as bad actors, use that social trust as a method to break-down the typical barriers to get a person to perform some action. This is especially true under remote work conditions as it is less likely two people will physically cross paths for an ad hoc confirmation of a request. Some typical scenarios are as follows:

- An executive asking for a transfer of funds from accounting to an outside vendor.
- Purchase of items like gift cards to "reward" staff.
- Requests by human resources department to fill out a form with personal information.
- Lastly, following a web link that requires entry of username and password for your email.

All these things seem innocent enough until you discover the actual recipient of these items was a bad actor pretending to be part of your organization. Our social nature brings our guard down and allows us to fall prey to these types of tactics.

Impersonation risk due to the increase of remote working is another looming threat with a similar risk to obtaining access to technical resources. Since most work performed by IT departments and providers is done remotely it increases exposure to impersonation. Technical personnel would be hard pressed to recognize all users' voices or identify any written or verbal tendencies of a user. Therefore, internal and external support (help) desks are now becoming a mechanism to gain access. By placing a simple call into support personnel, they can request administrative password changes, gain access to restricted data or obtain rights to critical applications.

All these scenarios can be handled with a simple rule of "trust but verify". However, when it comes to the support desk it is critical that you select an IT provider with a proven user verification process. The number of these exploits will only increase as providers outsource their support desks resulting in a further disassociation between them and the users.

4. Backup & Continuity

There is no question we are now in a digital age. The speed at which we can provide customer and employees access to information is now a perception of how well an organization operates. When this ability is hampered due to accidental deletions, hardware failure, or a cyber attack it can negatively impact productivity and possibly reputation. How you recover from these events is dependent on the technology used.

Backup is the process of taking a copy of data and storing it for a certain period. The cloud and local storage have replaced older technologies like tape, but the concept is the same. Data is saved to a location based on increments of time such as hourly or daily and then held for an extended amount. This extended time can be anything but most common are 14 days, 30 days, 6 months, 12 months, and infinite. Depending on the organization the time limits may be set based on the cost due to aggregate storage, staleness of the data, or regulatory compliance. Some organizations are unsure what their actual backup needs are, so they opt for the default of their service provider. Regardless of your current needs, your backup plans should be reviewed quarterly to check for any changes to the environment such as, newly created share drives, new applications, or a user removed that needs to be included. Besides understanding what is contained in a basic backup it is important to review data from a prioritization perspective in the event of failure.

In the event of a recovery, all data cannot be considered equal. A component of your backup strategy is defining what is known as Recovery Time Objective (RTO.) Identification of all critical restores required to meet immediate demands of the organization is important.

Revenue and payroll are usually the top two considerations. Along with this, a determination of who needs access and what is the elapsed time in which that data will be accessible is necessary. These are all things a technology service provider will help you address in your strategy planning.

The other area depending on the operational loss to consider is Continuity. Continuity uses your backup to leverage advances in technology such as cloud and virtualization to provide system access quickly -- even in the event of a hardware failure or malware attack. Although these solutions carry a larger cost of operating than a backup they are easily justified when compared against loss of income, loss of productivity, and loss of reputation. Understanding the benefits of continuity and how it fits within your technology budget and strategy is a crucial consideration.

Lastly, moving to the cloud does not remove the necessity of a backup. Some Line of business applications take responsibility for backing up your data. However, many cloud service providers have provisions such as, “Company is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you’ve stored.” Even in situations where a backup is completed by the Line of Business application, that process should always be validated. Understanding how to accommodate this with a backup solution or a contingency process should be part of your technology planning and budget.

5. Tech for Cost Reduction

Due to a lack of performance by many IT service providers many organizations have viewed IT as a necessary unpredictable cost of operations. To contain this expense, they filter work based on their crude estimate of time (hourly rate) and superficial technical understanding. This has caused an unhealthy relationship between an organization's cost of operations and its technical return on investment.

Organizations that spend the right amount of money on their technology partnership reduce their overall cost of operations. This may not seem possible since most things related to technology are viewed as a direct expense such as computers, software, and hourly labor. Yet even those things can be maximized for an improved return on investment.

Using IT to properly perform PC management can reduce costs. The consistent management of a PC may extend the life of a PC by as much as a year to benefit ROE. Planning to lifecycle a PC before a failure occurs or the system starts degrading in performance can reduce overall cost. Rebuilding and repurposing a PC to other areas such as manufacturing floor kiosk, customer courtesy kiosk, or to non-critical areas not only reduces cost, but may improve satisfaction of employees and customers.

Continuous patch management and validation also reduces the risk of an exploit, improve performance of the device, and ensure compatibility. Overall, these things reduce the cost of lost productivity.

Another area of cost reduction is process automation. When your IT provider helps you identify areas to automate workflows the reduction in labor costs can allow staff to be more effective on higher value activities. For instance, leveraging an automatic response to qualified inquiries to help schedule a meeting or provide additional information reduces cost of labor needed to perform these activities. In addition, the response is consistent with your brand and sales process messaging every time. Other areas of automation are as simple as creating awareness. Sending an email notification to the team when a new file is added is an example of being able to automate notifications on certain conditions to create awareness. This results in reduced labor and improved responsiveness especially when many of these types of notifications are only reviewed as time allows while managing workload for the day.

Lastly, technology further provides cost reduction when you can avoid tool sprawl. In today's technology landscape there is an abundance of applications available to everybody. In organizations, users are quick to implement and find their own solutions to their problems. This creates two problems. First, it creates process silos that may expose the organization to risk. Secondly, it may create a culmination of small incremental expenses that get overlooked. A good IT strategy works to take advantage of tools that are already in use. Then, most importantly, applying them at an organizational level to reduce cost and maximize utilization of the tool.

6. Cloud

The cloud can be confusing for many small to medium business owners. To put it simply, the cloud is just leveraging virtualization or web scaling on another third-party physical infrastructure.

Although there are many things that position themselves as a service, we will focus on the two most general categories. Infrastructure as a Service (IaaS) and Software as a Service (Saas).

Infrastructure as a Service allows organizations to eliminate their on-premises physical hardware and move it completely into the cloud. Two of the most common provider offerings in this space are Microsoft Azure and Amazon AWS. There are two main benefits to this type of offering.

First, you only pay for consumption of what you use. There is no longer a need to purchase onsite expensive physical equipment that needs to be replaced or modified when data aggregate exceeds existing space, or the CPU/memory is over utilized. The risk of physical hardware failure is also eliminated. In this model you can easily expand capacity just by paying for better instance or storage used.

Secondly, is availability of access. Moving to the cloud eliminates the restriction of having to be physically at your location. The reduction of your risk of loss of productivity due to things like temporary loss of power or internet is great. This type of solution still requires management and configuration of the servers themselves. This is mainly chosen by organizations that want to continue have control over their environment. The alternative to infrastructure as a service would be to give up control and go to a fully hosted application or service.

Software as a Service has gained popularity over the last few years. There is now a wide array of industry specific applications and utility services available for consumer use. These are the types of offerings lumped under this category.

- Email
- Productivity Applications like Microsoft Office
- VoIP
- Video Conferencing
- Integrations as a Service like Power Apps or Zapier
- Line of Business Applications – Industry Specific, CRM/SFA, or Accounting

The concept behind these cloud offerings is the same with regard to paying for consumption and losing physical hardware. However, with these offerings the updating is completely in control of the provider. They take responsibility for full maintenance of the platform. In this model, you also get the benefit of features being available as soon as the platform is updated. This can have huge productivity gains as you can take advantage of newly released time-saving features. These types of offerings really allow a company to scale and are the easiest to manage with a mobility strategy. Once you pay for a user, they can have access from anywhere.

As powerful of these offerings are, they still carry a large organizational responsibility. Unfortunately, too many businesses think that moving to the cloud passes certain responsibilities such as security, backup, and end-user training to the provider because you have given up “control” to access these things. However, the need for a great security minded IT provider does not go away when you move to the cloud. As a matter of fact, the need becomes even more critical as the implications of security for integrations, developing plans in case of loss of service, and developing the right security procedures to properly add/remove users from all services still needs to be managed. Lack of attention to these areas could decrease cost-savings as consumption exceeds true employee count or, worse expose your company to a data breach. The right provider will help you navigate the intricacies of the cloud offerings including maximizing available functionality.

7. Dedicated IT

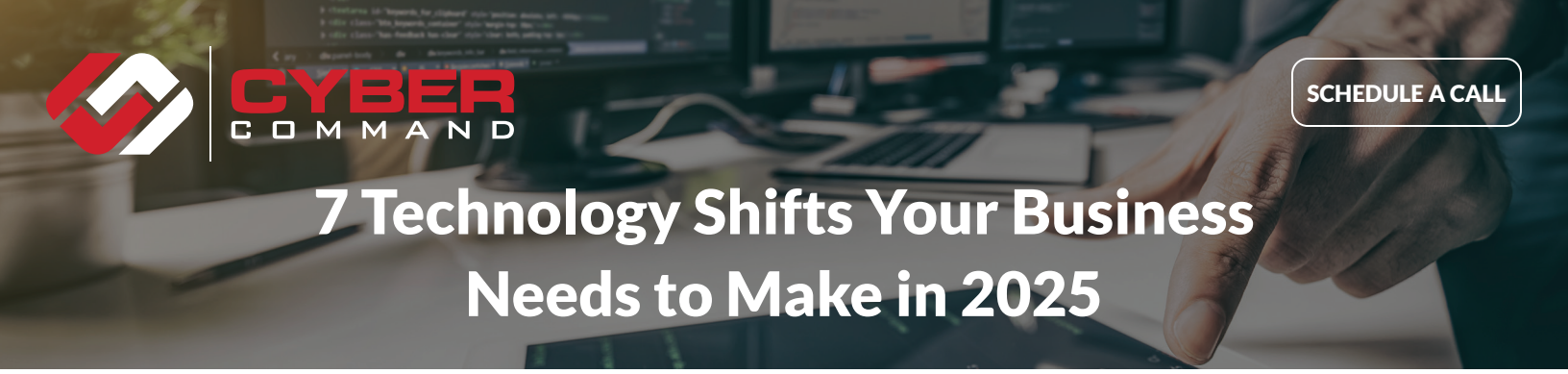
In the past, organizations could get by with paying for resources by the hour. Having an IT generalist and paying for the expertise was an acceptable way to temporarily bring in the skill needed to get the work done. This was especially true in the early days of technology when technology was less advanced. Things are much different today in our fast-paced work environments when access to information can be critical 24/7/365 and security has become more complicated, and technology boundaries are no longer constrained to one physical location.

This leads to the new reality of technology specialization. As technology advances, the number of exploits increase and the requirements to update often becomes critical. For example, having a specialization in the tools that allows you to centrally control and confirm is critical by today's standards. It would be insanity to grant every user the responsibility for updating and reporting on their status. A dedicated IT experience necessitates centralization of device management. Ultimately, this will limit the exposure to risks across the broader landscape of all devices under management. Regardless of where a need is discovered, a dedicated IT experience will apply necessary tools across all devices to protect. You do not gain this benefit of knowledge with a non-technical person acting as IT or with an ad hoc by the hour experience.

An obvious specialization in effective technology management is security. There are many different layers of protection and each requires training and experience to know how to maximize the tool for the greatest protection. This also means working with a security operations center (SOC). Every layer of security in the organization needs to be configured properly, reviewed frequently, and updated often. A dynamic approach is required and can only be delivered through experienced people on each layer such as server, network, firewall, and endpoint protection. This helps reduce your risk by properly managing all layers of your organization on an ongoing basis. Not to mention, security management must be an ongoing project to be successful.

Finally, a large benefit of having dedicated IT is having the right resource for project management. Poorly managed projects will almost always result in lost revenue. Even something as simple as a workstation set up is a micro project. An emergency is a critical fast track project. Having the experience to plan and gather the right resources, establish milestones, and estimate time is a practice that requires experience and established proven procedures. Dedicated IT not only performs these types of projects frequently, but constantly evolves their procedures to become proficient at them. Productivity is lost when personnel outside of dedicated IT try to manage the project themselves using Google or an ad hoc process. Time is wasted trying to find inexpensive labor that is immediately available. Under an emergency this can cause further emotional stress and incur increased losses of revenue and productivity.

Fast access and exchange of information are critical success factors needed to compete for today's successful modern business. This has resulted in technology that has evolved quickly and becoming more complex with high expectations on issue response time. Organizations that try to filter access to IT resources or do not have them aligned in their business will cause staff to lose confidence in technology strategies further creating data and operational silos. However, an organization that chooses a dedicated IT presence will have more accurate budgeting, more satisfied staff, optimal uptime, better project execution, improved insight into future strategies, and greater confidence in their overall approach to security. The right IT resources will provide you with a high-quality experience with better responsiveness at a price that scales with your organization.



7 Technology Shifts Your Business Needs to Make in 2025

Next Steps

Technology is more important now than ever. If you're not keeping up with it, you're falling behind, especially with the paradigm shift caused by the pandemic. The pandemic has exacerbated every hole in technology and has spread resources thin with the move to work from home and increasingly to the cloud. You can make yourself a target, or make the risk so high that you dodge the majority of attacks depending on your technical strategy. With the right expertise, the only difference you and your business notice is the calm.

2025 is just continuing to solidify the technical changes from 2020 and will continue to grow and evolve in new directions. As each trend becomes more commonplace, it becomes more essential to not just keep pace, but to make sure you understand what and why you're doing something. The cloud is a powerful tool, but you need to make sure you're using the right tool for the right job the right way.

Technology changes at a frenzied pace and you need to keep up for your business to stay relevant. It isn't just insecure to do things the old way, it's downright expensive. Modernizing your technology to keep up with the times can reduce the total cost of ownership by reducing risk of downtime or even just outright cut the costs. Sometimes it even gets you both.

With how complicated technology is, dedicated IT is a must. Gone are the days where a single person could instantiate, maintain, and service all of a business's technological needs. More decent technicians can be more efficient than one great technician due to the sheer magnitude of the knowledge required to just stay above water in modern technology.

What are you doing to address these issues and how can we help?

SCHEDULE A CALL