

IT Issues Business Owners Must Consider When Growing from 5 to 20 Employees



John Scroggins

Expanding a business from 5 to 20 employees is an exciting milestone. It reflects a healthy trajectory of growth and signals a shift in operational complexity. However, as the headcount rises, so does the strain on your technology infrastructure. For small business owners, understanding and addressing IT needs early on is crucial to ensuring smooth growing, maintaining productivity, and safeguarding the business against digital risks.

Here are the key IT issues that business owners should consider when growing their teams from 5 to 20 employees.

1. Scalability of Existing IT Infrastructure

Your current setup—likely a combination of basic hardware, shared drives, and consumer-level software—may have worked well with 5 employees but is unlikely to scale efficiently. As your team grows, so will the demands on your servers, network bandwidth, and storage.

What to consider:

- **Cloud services:** Transition to scalable cloud platforms like Microsoft 365 or Google Workspace to handle email, document sharing, and collaboration.
- **Server capacity:** If you're running in-house servers, evaluate whether they can handle increased load. Alternatively, consider moving to cloud infrastructure providers like AWS or Azure.
- **Network upgrades:** A slow internet connection or outdated routers and switches can throttle productivity. Invest in business-grade networking hardware and a high-speed internet connection.

2. Cybersecurity Threats Increase with Size

Cyber threats are not just a concern for large corporations. As you grow, your business becomes a more attractive target for cybercriminals. Each new employee is another potential entry point for attacks.

What to consider:

- **Endpoint protection:** Install antivirus, anti-malware, and firewall solutions on all devices.
- **Multi-factor authentication (MFA):** Require MFA for all logins to email, cloud platforms, and financial software.
- **Security policies:** Implement policies covering password requirements, acceptable use, and incident reporting. Train all employees regularly.
- **Data backup:** Regularly back up your data using both on-site and cloud-based solutions.

3. Access Control and User Management

With five employees, access control might have been informal—everyone could log in to everything. But as the team grows, that approach becomes risky.

What to consider:

- **Role-based access:** Assign access rights based on job functions. For instance, HR shouldn't access financial data, and junior staff don't need admin privileges.
- **User provisioning and deprovisioning:** Establish procedures for setting up and disabling user accounts when employees join or leave.
- **Directory services:** Use tools like Microsoft Active Directory or cloud alternatives to manage user permissions centrally.

4. Collaboration Tools and Communication Platforms

Internal communication becomes more complicated with growth. Email alone may no longer be sufficient.

What to consider:

- **Messaging platforms:** Adopt tools like Slack or Microsoft Teams for real-time communication.
- **Project management software:** Tools like Asana, Trello, or Monday.com can help manage tasks and projects more efficiently.
- **Document collaboration:** Move to cloud-based tools like Google Docs or Microsoft Office Online to allow for simultaneous editing and version control.

5. Device and Asset Management

When your business had five employees, tracking laptops and phones was easy. At 20 employees, it's critical to manage all hardware and software assets effectively.

What to consider:

- **Inventory management:** Keep detailed records of all devices, their specifications, warranty status, and assigned user.
- **Mobile device management (MDM):** Implement MDM solutions to manage and secure employee smartphones, tablets, and laptops remotely.
- **Standardization:** Standardize hardware and software purchases to simplify support and updates.

6. Compliance and Data Privacy

As your customer base and employee count grow, you're more likely to handle sensitive personal, financial, or medical data. This brings new legal and compliance obligations.

What to consider:

- **Data protection laws:** Understand and comply with regulations such as GDPR, HIPAA, or CCPA, depending on your industry and customer base.
 - **Employee data:** Securely store and handle employee personal data like social security numbers, payroll, and performance reviews.
 - **Auditing:** Implement systems that allow for tracking and auditing access to sensitive data.
-

7. IT Support and Helpdesk Services

In a very small team, your most tech-savvy employee might double as your IT department. As you scale, this becomes unsustainable.

What to consider:

- **In-house vs outsourced IT:** Decide whether to hire dedicated IT staff or use a managed service provider (MSP). Outsourced IT can provide round-the-clock support, predictable costs, and broad expertise.
 - **Ticketing systems:** Implement a helpdesk or ticketing system to streamline support requests and track issues.
-

8. Software Licensing and Subscription Management

Growing teams often outpace the original number of software licenses purchased, leading to compliance and productivity issues.

What to consider:

- **License tracking:** Keep records of all licenses and ensure you're compliant with terms.
 - **Cost optimization:** Regularly review usage to ensure you're not overpaying for underused software.
 - **Centralized procurement:** Assign software purchasing to one person or team to prevent redundancy and ensure compatibility.
-

9. IT Policy Development

Informal IT practices may work for five people, but they lead to inconsistency and risk as your team grows.

What to consider:

- **IT usage policies:** Document policies on acceptable use, BYOD (bring your own device), internet access, and social media.

- **Onboarding/offboarding processes:** Create checklists to ensure consistent setup and teardown of accounts, access, and equipment.
- **Incident response:** Develop a plan for responding to data breaches or technical failures.

10. Disaster Recovery and Business Continuity

At five employees, a computer crash might be an inconvenience. With 20 employees, the same issue could halt your operations.

What to consider:

- **Disaster recovery plan:** Identify critical systems and outline procedures for recovery in case of failure.
- **Redundancy:** Ensure your business-critical systems have backup options—whether it’s power supply, servers, or cloud systems.
- **Business continuity planning:** Define how your team can continue to operate during IT outages, natural disasters, or cyberattacks.

Conclusion

Growing a business from 5 to 20 employees is more than just a numbers game—it’s a strategic evolution that requires thoughtful planning, especially in the realm of IT. The right infrastructure and policies not only support growth but also protect your business from security threats, data loss, and operational inefficiencies.

Investing in IT as you grow isn’t just a cost—it’s a foundation for sustainable success.

ASK YOUR MENTOR

1. What if any I.T. infrastructure did you have to improve as you grew your business?
2. How did you decide when to do that?
3. Is there anything that you would have done differently? What would have you made a priority sooner?
4. Have you hired someone to specifically focus on I.T.? If so, what did that process look like?
5. What IT improvement provided “the biggest bang for your buck?” Why?
6. Can you think of any other big ideas about using tech to help a business grow that I should consider?

Reflect & Respond/Self-Rate- MENTEE

Rate the degree to which you are doing these things in your business. 5 = In place or doing it well

	1	2	3	4	5
Scalability of Existing IT Infrastructure					
Cybersecurity Threats Increase with Size					
Access Control and User Management					
Collaboration Tools and Communication Platforms					
Device and Asset Management					
Compliance and Data Privacy					

IT Support and Helpdesk Services					
Software Licensing and Subscription Management					
IT Policy Development					
Disaster Recovery and Business Continuity					

Go Do

1. Ask God, "What do you think I should prioritize the above?" Listen. What would it look like to trust God with this?
2. Practice. How I will practice or what I will do with this over the next month: