How Much Should IT Really Cost?

PREPARED BY SUURV TECHNOLOGIES
San Antonio, TX
SUURV.COM | (210) 874-5900

↘ A BUSINESS LEADER'S GUIDE TO

Smarter IT & *CYBERSECURITY SPENDING*

EXECUTIVE

Summary

Most SMBs typically spend 3–7% of revenue on IT and 10–15% of that IT budget on cybersecurity. Falling below these ranges often correlates with outages, inefficiencies, and higher risk.

Key Takeaways for Business Leaders

IT Must Be Structured, Not Just Outsourced.

IT must be structured at multiple levels to account for communication with executives, day to day decision makers, and the ongoing support needs for everyone across your organization.

Cybersecurity Is a Non-Negotiable.

Proper investment in tools, redundancy, insurance, and people reduces the risk of costly breaches and downtime.

Costs Depend on Industry and Application Needs.

Different industries require different software solutions that can affect IT spend, cyber-security risk, and business continuity requirements. Choose your tools wisely for maximum efficiency.

IT Should Drive Business Outcomes.

The right provider aligns technology investments with goals for scalability, compliance, and operational efficiency.

WHY BUSINESS LEADERS ASK

How Much Should IT Cost?

Business leaders usually ask this when something feels off — rising costs, inconsistent support, or unclear value. There's no universal price tag for IT, but there are reliable benchmarks and cost factors that help determine whether your investment is on the right track.

What Does a Winning IT Department Look Like?

Structured from the Top Down

The strategy for any department must come from the executive in the organization. Whether internal or external, someone in the business must own the role for business strategy regarding how it is related to IT, cyber-security and risk mitigation.

Strategic IT Planning Sessions

Technology decisions should align with business goals. Without planning, you risk overspending or missing cost-saving opportunities.

Audits that Prevent Deviation

Strong IT environments rely on clearly defined standards — covering business continuity, MFA requirements, and consistent onboarding and offboarding processes. Assigning ownership for monitoring these standards reduces drift, even when human error occurs. Regular audits help maintain alignment, strengthen security, and support predictable operations.

Having the Right Business Tools for Your Industry

Different industries require different IT architectures. An engineering firm running heavy design tools like AutoCAD or SolidWorks may need local servers for performance, while smaller businesses often gain more value from cloud-based storage. The tools you choose — software, authentication methods, file locations, and recovery strategy — directly affect both your costs and long-term efficiency.

Hardware Lifecycle Management

Healthy IT budgets include a regular rotation of hardware — from laptops and servers to routers and firewalls. Aging systems slow down productivity and create unnecessary risk.

THE COST OF Cybersecurity

CYBER INSURANCE

Rates depend on industry, security posture, and incident history. A weak cybersecurity foundation can disqualify you from coverage — or make premiums skyrocket.

SECURITY TOOLS

Modern defenses include MFA, EDR, firewalls, phishing protection, and data loss prevention. These aren't "nice to have" — they're required to protect your business and meet compliance standards.

PEOPLE TO MANAGE THE TOOLS

Technology alone doesn't stop threats — people do. Skilled professionals are needed to monitor alerts, investigate incidents, and maintain compliance.

"If the cost of cybersecurity seems like a lot, consider the cost of a data breach.
— Shane Morris, CEO, SUURV Technologies

REDUNDANCY AND INCIDENT RESPONSE

Breaches and outages happen. Having reliable backups, recovery plans, and response protocols minimizes damage and downtime.

The High Cost of Getting IT Wrong

About Cutting Corners on IT

Reducing IT costs may seem harmless at first — but the fallout can be significant. When providers skip the dedicated roles for strategic planning, proactive auditing, or cyber security best practices, small issues quickly grow into larger operational problems:

- You may see recurring tickets, growing security vulnerabilities, and rising frustration among employees.
- What initially looked like savings often becomes far more expensive in the long run. Escepcially when a six to seven figure breach occurs.

> *IT isn't just fixing what breaks — it's about driving growth, lowering risk, and preparing your business for what's next.*
> ***— Shane Morris, CEO, SUURV Technologies***

Benchmarking Your IT Spend

Use these benchmarks to evaluate your investment:

- Total IT Spend: 3–7% of annual revenue (depending on size and industry)
- Cybersecurity Spend: 10–15% of the total IT budget, higher for regulated sectors

Final Thoughts — It's Not About the Lowest Price

Choosing an IT partner is less about price and more about a provider that purposefully allocates resources to core functions like Strategic Consulting, Auditing, and ongoing support, protecting and enabling your business. At SUURV Technologies, we integrate Managed IT Services and Managed Cybersecurity to build predictable budgets, strengthen security, reduce downtime, and align your technology with long-term goals.

The Real-World Impact of Getting IT Wrong

Beyond technical risks, poor IT choices create real emotional and financial consequences:

- A serious incident leads to exposed customer information, shaken employee confidence, and growing anxiety for leadership
- After a breach, companies can face delayed payroll, damaged reputation, customer attrition, and costly legal challenges.

A strong cybersecurity strategy helps prevent these executive-level problems.

GET IN TOUCH WITH US!

Don't wait until IT problems slow down **your business**.

Take control of your technology decisions today.

EMAIL
sales@suurv.com

VISIT US
www.suurv.com

PHONE
(210) 874-5900