WIRED FOR GROWTH

THE SECURITY BLUEPRINT

One Step Secure IT

THE LATEST BYTE

2026 VOLUME 1

EXECUTIVE EDITION

In this Issue...

We're in an era where a single breach can erase years of progress. This Executive Edition delivers a battle-ready blueprint that turns cybersecurity into your sharpest competitive edge. You'll hear directly from our One Step Secure IT CEO on smart budgeting that shields SMBs without starving expansion, plus exclusive insights from our Director of IT and Security, a CISSP-certified expert who's stopped breaches cold.

We dive into AI's real risks and rewards, then show how strategic IT unlocks new revenue streams your competition hasn't seen. Along the way, our cybersecurity and business leaders will share actionable tactics to enhance your business security for 2026.

About Us

We are an outsourced IT company with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Our expertise includes Cybersecurity, Managed IT, Information Security, and Compliance Services. We understand that as business operations evolve, so do the security threats. Our expert team collaborates closely with you to create a customized IT strategy, identify vulnerabilities, and strengthen your IT infrastructure.

Our corporate headquarters are in Phoenix, AZ, and we proudly serve businesses nationwide. To learn more about how One Step Secure IT can enhance your technology, visit our website at www.onestepsecureit.com.

Whether you're a business owner, IT leader, or simply curious about staying safe in today's digital world, the *One Step Beyond Cyber* podcast is your go-to resource for practical cybersecurity insights.

Season 3, hosted by One Step Secure IT Founder and CEO Scott Kreisberg, delivered actionable advice, real-world stories, and expert tips to help you navigate evolving threats with confidence.

This season included 8 insight-packed episodes, 6 of which featured outstanding guests, from AI experts and insurance professionals to lawyers and product managers. Their fresh perspectives made the season truly unforgettable.

Dive into the full Season 3 library below and catch up on any episodes you missed. Stay tuned in 2026 for *One Step Beyond Cyber* Season 4!

ONE STEP BEYOND CYBER
PODCAST

That's a Wrap on Season 3!

S3 EP 01 *Hackers in the Driver's Seat: Cybersecurity Challenges in Auto Dealerships* with Kevin McAdam

S3 EP 02 *When Hackers Strike: Understanding the Legal Aftermath* with Attorney Andrew Garbarino

S3 EP 03 *Retail Under Attack: Lessons from the Largest Data Breach in History* with Tim Derrickson

S3 EP 04 *Cybersecurity & Compliance for Auto Dealers: A Conversation* with Nick Moyes from ComplyAuto

S3 EP 05 *Insured or Exposed? The Truth About Cyber Insurance in 2025* with Joseph Cook from The Arizona Group

S3 EP 06 *Rethinking Risk: A Framework for Businesses Below the Cybersecurity Poverty Line* with Tim Derrickson

S3 EP 07 *Stacks, Stats & AI: The Cybersecurity Playbook for Small and Mid-Sized Businesses* with Jim Peterson from ConnectWise

S3 EP 08 *AI for SMBs: Why Clean Data Matters: Unlocking the Power of AI for Businesses* with Chris Carte from Approyo

There's at least one episode this season made just for you. From AI and leadership to cybersecurity, pick the topic that speaks to you and hit play.

Scan QR Code to Start Listening!

Smart Cybersecurity Budgeting for SMBs

by Scott Kreisberg
One Step Secure IT's Founder and CEO

EXECUTIVE ARTICLE

I see too many business leaders treating their cybersecurity budget like a gamble.

They throw some money at it, hope for the best, and cross their fingers to avoid getting taken advantage of. A reactive, fear-based approach is a terrible way to run a business.

You wouldn't build a multi-million-dollar headquarters and just hope for no break-ins. You would install locks, cameras, and alarms. You would create a plan.

In the digital world, your most valuable assets are your data, reputation, and finances. Yet, many business leaders use tools they do not fully understand.

Stop gambling and start strategizing. Creating a cyber-resilient budget is not just about buying every new gadget or getting the latest AI tool that claims to prevent all unauthorized access. Instead, it's about developing a robust plan that safeguards your business while fostering its growth.

How do you build a cybersecurity budget that actually works?

Let's break it down.

1 Tie Cybersecurity to Business Objectives

Cybersecurity spending that lives in a vacuum won't survive the CFO's red pen. Instead, link security investments to business goals and KPIs. No business leader wants to walk into a boardroom full of tech jargon.

I read a Wall Street Journal article that said IT executives must repeatedly show boards how their spending helps the business. The most effective approach is to focus discussions on "business outcomes" rather than on technical specifications.

Planning a merger or acquisition?
That means IT integration and security.

Moving to a new SaaS platform?
Budget for securing that data and vetting the vendor.

Pursuing enterprise clients?
Be ready for a thick security questionnaire.

This is where metrics like dwell time (how long attackers lurk before detection) and vendor vetting speed come into play. Reduce dwell time, and you cut off attacks before they spread. Improve vetting speed, and you enable faster, safer business partnerships.

These operational metrics connect cybersecurity to business success. They show that security is not only about reducing risks but also about helping growth.

The distinction is simple: one choice is a reactive expense, like paying a ransom or buying a temporary fix after an incident. The other preserves operations by keeping systems and data available and recoverable, so the business keeps running.

2 Know What You Own (and Protect It)

Before spending, create a full inventory of IT assets:

Hardware: laptops, servers, phones, IoT devices
Software: applications, licensed and cloud-based
Data: where it lives, who has access, how sensitive it is
Networks: the links between everything

This isn't a one-time project. Keep refining. After identifying assets, classify them by importance.

Not every system needs equal protection. Retailers depend on POS systems, manufacturers on production lines, and auto dealers on dealership management software.

Prioritize these crown jewels with a Zero Trust framework, immutable backups, and segmented access.

3 Budget Across People, Tools, and Training

Your business isn't the same as the one down the street, so your security budget shouldn't be either. The old model of dedicating a fixed percentage of the IT budget to security is fading.

The Wall Street Journal emphasizes that "Cybersecurity spending varies by industry, a company's risk profile, and other factors."

A strong cybersecurity budget is balanced. This means not spending too much on tools and not enough on people, or the other way around.

Infrastructure & Tools- Firewalls, SIEM, MDR, intrusion detection. Renewal fees quickly add to expenses.

People- A cybersecurity analyst averages $120K annually. With benefits, building a team can exceed $1M. That's why SMBs turn to a Managed Security Service Provider (MSSP) or part-time Chief Information Security Officer (CISO).

Training- Most breaches start with human error: phishing, weak passwords, oversharing. Training isn't optional; it's a top ROI investment practice.

The "right" amount to spend depends entirely on your specific situation. How much to spend depends on:

Company Size- SMBs should focus on essentials and lean on partners, while enterprises need a full Security Operations Center (SOC).

Industry- Compliance is mandatory; HIPAA, PCI DSS, NIST.

Risk Profile- Remote workers and IoT devices raise risk. Higher risk demands a stronger posture.

4 Plan for the "When it Happens" Moment

Even the best defenses fail. An incident response plan helps you recover quickly from ransomware or outages. Without it, you could face weeks of downtime.

Boards now press CISOs on contingency budgets. If you don't have an answer, you're behind. Where does the money go?

Four main buckets:

Tech & Tools
Firewalls, antivirus, vulnerability scanners. Consider total ownership, not just sticker price. A managed security monitoring service often saves money in the long run.

People & Expertise
Hiring is costly. Managed Detection & Response (MDR) providers offer 24/7 protection at a lower cost, letting leaders focus on growth.

The Human Firewall (Training)
One phishing click can take you down. Training and phishing tests turn employees into defenders.

The "Oh Sh*t" Fund (Contingency)
A zero-day or advanced attack can hit anytime. Keep a fund ready to hire experts and contain damage fast.

Frame this as a trade-off: "If we skip installing Multi-Factor Authentication (MFA), we accept a 25% higher risk of credential theft, with a $2M potential impact." This example makes cybersecurity a governance decision.

5 Balance Short-Term Action with Long-Term Vision

Use your 2025 budget for essentials: security snapshot, MFA, and refreshed training. But don't stop there. Prepare your business's 2026 roadmap: Zero Trust adoption, AI security policies, advanced detection capabilities, and cloud posture management.

Track leading indicators that show whether policies are working:

- "500 critical vulnerabilities unpatched beyond 90 days" = red flag
- "Closing them reduces ransomware exposure by 40%."

When framed this way, even technical metrics become board-level insights. It's like training for a marathon. You need short sprints to build stamina, but the real win comes from sticking to the plan over time.

The Bottom Line

Strong security budgets come from knowing your assets, risks, and where to invest. Boards and CFOs don't care how many tools you bought; they care if the team in place reduced breach severity and sped up response times. Outcome metrics prove resilience, not just effort.

A Word of Caution

Don't get buried in dashboards. Too many numbers can create a false sense of security. Data should give you an idea of your business posture, but it's not the whole story. The companies that "get it" are the ones treating cybersecurity budgets as survival plans, not side projects.

Everyone else? They're just hoping the wolf doesn't show up at the door.

Make Cybersecurity a Strategic Advantage

Give us a call at 623-227-1997 and we'll help you build a cybersecurity roadmap and budget that protects your business and makes sense on your balance sheet.

AI in 2026

Profit Explosion or Total Exposure?

As artificial intelligence (AI) integrates deeper into business operations, leaders must balance its potential with emerging risks.

There are a few key areas every business leader should be aware of as we head into 2026: the precautions to take when using public AI tools, the ongoing value of email security training, and the professions that are poised for significant AI-driven change.

Here are some practical, actionable tips to help you stay ahead as AI becomes more and more integrated into the workplace.

Cautions When Using Public AI Tools

Public AI platforms like ChatGPT offer immense productivity boosts, from drafting reports to generating ideas. However, they come with significant risks, including data privacy breaches and cybersecurity vulnerabilities. Businesses have experienced leaks when sensitive information is entered, as these tools often store or use data for model training.

Additionally, AI can perpetuate biases from flawed training data, leading to discriminatory outputs or flawed decisions. Other concerns include generating malicious code, enabling phishing scams, and a lack of transparency in how models are built.

Tips for Business Leaders

Protect Sensitive Data
Never upload or share identifiable information, such as personal details, financial records, or proprietary business intel. This prevents unauthorized access or fraud.

Disable Tracking
Turn off any data-sharing or tracking options in AI interfaces to minimize exposure.

Opt for Privacy-Focused Services
Invest in paid AI tools that prioritize privacy and often provide better data controls and compliance features.

Conduct Risk Audits
Regularly review AI usage policies, ensuring teams avoid inputting confidential data and monitor for biases or inaccuracies.

Train on Security
Educate employees on AI-specific threats, such as intellectual property infringement, prompt injection attacks, data leakage through public models, and deepfake-enabled phishing, so they can use AI tools confidently without putting the company at risk.

The Importance of Continuous Email Education

In an era of sophisticated cyber threats, email remains a prime attack vector.

Clumsy phishing emails riddled with inconsistent grammar and glaring flaws are being replaced by polished, personalized messages crafted by AI.

Continuous education keeps teams vigilant, sharpening their ability to spot phishing, malware, or social engineering.

Regular training reinforces the fact that threats evolve and that AI-powered scams now mimic human writing styles, making detection harder. Without ongoing refreshers, complacency sets in, potentially costing businesses millions in breaches.

Key Indicators to Watch For:

- Unsolicited attachments or links from unknown senders.
- Urgent language pressuring for quick action, such as "immediate payment required."
- Mismatched email domains or slight misspellings in sender addresses.
- Requests for sensitive info, such as passwords or financial details.

Tips for Business Leaders

Mandate quarterly workshops, simulate phishing tests, and integrate email hygiene into performance reviews. This mitigates risk and fosters a culture of security awareness.

AI and the Future of Work

Which Roles Are at Risk and How Smart Leaders Are Turning Threat into an Advantage

AI is reshaping the workforce faster than most leaders expected. Roles are built on routine, repeatable tasks.

Entry-level customer service, basic data entry, standard content writing, junior paralegal research, straightforward translation, and boilerplate coding are already being automated or heavily reduced.

For business owners, the financial upside is undeniable: replacing an employee (plus benefits and overhead) with AI that costs pennies on the dollar can transform margins almost overnight. Many founders and CEOs are genuinely excited about finally escaping the endless challenges of scaling headcount.

That excitement is warranted, but it needs to be tempered with caution. Customers still notice and hate robotic, tone-deaf service or content that feels soulless. Companies that push low-quality AI output to clients can expect pushback.

Cut positions too aggressively, and you quietly erode the junior pipeline that feeds your future senior talent. Five years from now, you may have perfect automation, but no one left who deeply understands your customers, product, or culture.

The most successful leaders aren't asking "which jobs can we eliminate?" They're asking, "How do we redesign every role so a human & AI deliver more value?" They audit processes and fund serious reskilling in AI literacy.

Done thoughtfully, AI delivers both dramatic cost savings and higher quality. Done hastily, you risk short-term gains for long-term damage. The winners will be those who adapt people and processes with the same speed they adopt the tools.

AI offers the clearest path most leaders will ever see to both cut costs and raise quality at the same time. Get the balance right by reskilling people, redesigning roles, and adopting thoughtfully, and you'll come out stronger, more profitable, and ready for whatever comes next.

EXECUTIVE ARTICLE

TECH-DRIVEN GROWTH

Using IT to Unlock New Business Opportunities

by CISSP Tim Derrickson
One Step Secure IT Director of IT & Security Services

In a short timespan, we've seen technology shift from a supporting role to the primary driver of business innovation and growth. From artificial intelligence (AI) and big data analytics to cloud computing and automation, IT has become key in unlocking new business opportunities, enhancing customer experiences, and achieving operational excellence.

Businesses today are increasingly leveraging IT to transform their operations and strategies. According to McKinsey & Company (mckinsey.com), the economic value of generative AI could reach $4.4 trillion, with a significant portion stemming from marketing and sales enhancements. This underscores the immense potential of technology-driven initiatives in driving business growth.

Moreover, a report by CIO (cio.com) highlights that over 80% of C-suite executives anticipate improvements in productivity and revenue through data and AI integration. This sentiment reflects a broader recognition of IT's pivotal role in shaping business trajectories.

Real-World Applications: Case Studies of Tech-Driven Growth

Amazon's Personalization Engine *(forbes.com)*

Amazon has revolutionized the retail industry by utilizing AI-driven recommendation systems. By analyzing customer behavior and purchase history, Amazon delivers personalized product suggestions, enhancing user experience and boosting sales.

Walmart's Digital Transformation *(kerningcode.com)*

Walmart has embraced digital technologies to compete in the modern retail landscape. Initiatives such as acquiring e-commerce platforms, developing a robust mobile app, and integrating digital tools into physical stores have streamlined operations and improved customer service.

There are Key Technologies Driving Business Innovation, Artificial Intelligence and Machine Learning.

Artificial intelligence (AI) and machine learning empower businesses to process large amounts of data, identify trends, and make strategic decisions. A common application is AI-powered chatbots, which improve customer service by delivering real-time, tailored responses. While traditional chatbots based on closed large language models (LLMs) have limitations, those connected to open LLMs can engage in conversations and occasionally express viewpoints—typically reflecting the perspectives of the organizations that develop or deploy them.

Big data analytics allows companies to process and interpret large datasets to gain insights into customer behavior, market trends, and operational efficiency. This data-driven approach facilitates strategic planning and competitive advantage.

Cloud computing offers scalable and flexible IT resources, enabling businesses to innovate rapidly and cost-effectively. By leveraging cloud services, companies can deploy applications faster, enhance collaboration, and reduce infrastructure costs.

While the benefits of integrating IT into business strategies are substantial, organizations face challenges. Employees may be hesitant to adopt new technologies because of their fear of being displaced. With the increase of digitalization, there is a risk of data breaches and cyber threats. Implementing leading-edge technologies requires specialized skills that include employee training and development.

Addressing these challenges will take training, strong cybersecurity understanding, and cross-functional teams to handle support and development.

As technology continues to evolve, businesses must remain flexible and proactive in adopting solutions. Emerging technologies like quantum computing, blockchain, and advanced AI models will revolutionize industries. Organizations that embrace these advancements and integrate them into their strategic planning will be positioned to seize new opportunities and drive sustained growth.

Leveraging IT is no longer optional but essential for businesses aiming to thrive in the modern economy. By researching and adopting technological innovations, companies can unlock new avenues for growth, enhance customer experiences, and maintain a competitive edge in an increasingly digital world.

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

onestep
Secure IT Services

www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT