COMPREHENSIVE GUIDE TO PREPARING YOUR 2025

Cybersecurity Budget

TECH 2020 SOLUTIONS

www.tech2020solutions.com
535 Broadhollow Road, Suite A28
Melville, NY 11747
516.876.8290 / 516.876.8761

Provided by
Tech 2020 Solutions

Cybersecurity
Making sound decisions.

In today's digital landscape, small to mid-sized businesses (SMBs) face escalating cyber threats that can have devastating financial and operational impacts. With cybercriminals increasingly targeting these organizations, it is crucial for businesses to develop a robust cybersecurity strategy, starting with a well-structured budget. A well-planned cybersecurity budget not only addresses immediate security needs but also lays the groundwork for long-term resilience against evolving threats.

This guide provides a comprehensive framework for creating a scalable cybersecurity budget tailored to the specific needs of SMBs. It covers essential steps such as assessing your current security landscape, defining objectives and KPIs, and prioritizing risks. Additionally, it highlights the importance of investing in technology, ongoing training, and maintaining a contingency fund. By following these guidelines, business owners and IT professionals can ensure their cybersecurity investments are strategic, effective, and aligned with their organization's goals.

Security First

Cybersecurity is a critical business investment.

Why Cybersecurity is Critical for SMB's

- **Increasing Threats:** The frequency and sophistication of cyberattacks are escalating. SMBs, often seen as easier targets, face risks from ransomware, phishing, and other malicious activities.

- **Financial and Reputational Impact:** Cyber incidents can lead to substantial financial losses and severe reputational damage. The average cost of a data breach for small businesses is approximately $3.86 million.

- **Regulatory Compliance:** Regulations such as GDPR, HIPAA, and CCPA impose stringent requirements on data protection, making compliance a financial and operational necessity.

- **The Human Element**: Employees often unwittingly contribute to security breaches through actions like clicking on phishing links or using weak passwords. Proper training is essential to mitigate this risk.

Your Small to Mid-Size Business is a Prime Target for Cybercrime

In today's digital landscape, small to mid-sized businesses (SMBs) are increasingly targeted by cybercriminals. According to recent statistics, **43% of cyberattacks are aimed at small businesses**, and nearly 60% of these businesses go out of business within six months of a significant breach.

These alarming figures underscore the critical need for a robust cybersecurity strategy, including a well-planned budget. This guide provides a comprehensive approach to crafting a scalable cybersecurity budget, tailored for the specific needs of SMBs.

Creating a Cybersecurity Budget

Step-by-Step Guide
Step 1

Assess and Analyze Your Current Cybersecurity Landscape

Objective:

Understand your existing cybersecurity posture, including current tools, policies, and vulnerabilities.

How Your IT Provider Can Help:

- Conduct a comprehensive security audit to identify existing vulnerabilities and gaps.
- Review current cybersecurity policies and tools in place.
- Evaluate the effectiveness of existing measures and recommend necessary improvements.

Your cybersecurity budget

Include in your budget planning measures that address your cybersecurity at present and provide scalability for the future

Prevention methods

Implementing advanced firewalls and intrusion prevention systems to block unauthorized access and malicious traffic before it can penetrate your network.

Detection methods

Utilizing sophisticated intrusion detection systems (IDS) and security information and event management (SIEM) tools to monitor and identify suspicious activity and potential threats in real-time.

Response

Developing and executing a detailed incident response plan to swiftly address and mitigate the effects of a cyber attack, including containment, eradication, and recovery procedures.

Cybersecurity Budget Steps

A Managed Secure Operations Center will ensure you Prevent, Detect, & Respond to threats in real time.

Step 2: Define Objectives & KPI’s

Objective: Establish clear cybersecurity objectives and Key Performance Indicators (KPIs) to guide budget allocation.

Considerations:

- Define specific security goals such as reducing incident response time or enhancing threat detection capabilities.
- Set KPIs to measure progress, such as the number of detected threats or the average time to resolve security incidents.

Step 3: Create an Inventory of IT Assets

Objective: Catalog all IT assets to prioritize budgeting based on their criticality and sensitivity.

Tasks:

- List all hardware, software, networks, and data.
- Categorize assets by their importance to business operations and potential impact if compromised.

Cybersecurity Budget Steps

The best defense is a strong offense when it comes to your cybersecurity. Having a Managed Service Agreement with a trusted IT Service Provider is the first step.

Step 4: Prioritize Risks

Objective: Identify and prioritize risks to allocate budget effectively.

How to Prioritize:

- Conduct a risk assessment to identify high-impact vulnerabilities.
- Focus budget on addressing the most critical risks first to ensure a higher return on investment.

Step 5: Allocate Budget for Various Resources

Objective: Distribute budget across different cybersecurity resources including infrastructure, personnel, training, and third-party services.

Allocations:

- Prevention: Invest in firewalls, secure network design, and other preventive measures.
- Detection: Budget for intrusion detection systems and monitoring tools.
- Response: Allocate funds for incident response and recovery efforts.

Step 6: Estimate Costs for Technology & Tools

Objective: Calculate costs for acquiring and maintaining cybersecurity tools and technologies.

Considerations:

- Software Subscriptions: Include costs for antivirus software, intrusion detection systems, and encryption tools.
- Hardware Upgrades: Factor in costs for upgrading servers and network infrastructure.
- Third-Party Services: Budget for Secure Operations Center (SOC) support and other external services.
- Cyber Liability Insurance: Allocate funds for insurance to mitigate financial impacts of a breach.

Cybersecurity Budget Steps

According to a study by the Ponemon Institute, 95% of cybersecurity breaches are due to human error.

Step 7: Allocate Funds for Initial and Ongoing Training

Objective: Invest in employee training to reduce the risk of human error. Investing in training can significantly reduce these risks by educating employees on recognizing phishing attempts and maintaining strong passwords.

Training Areas:

- **Basic cybersecurity awareness**
- **Advanced threat detection and response**
- **Secure use of personal and corporate devices**

Step 8: Create a Contingency Fund

Objective: Set aside funds for unexpected cybersecurity incidents and emerging threats.

Importance:

- A contingency fund provides a financial cushion for rapid response to unforeseen incidents.
- It allows for quick intervention and recovery, minimizing downtime and operational disruption.

Step 9: Get Approval from Key Stakeholders

Objective: Present the budget proposal to stakeholders to secure necessary approvals.

Steps:

- Clearly articulate the budget's rationale and benefits.
- Highlight how the budget aligns with business objectives and mitigates potential risks.
- Provide data and insights to support your proposal.

Cybersecurity Budget Steps

The percentage of a company's budget allocated to cybersecurity can vary based on factors like industry, size, and risk profile. However, a common benchmark is to allocate between 5% to 10% of the IT budget specifically to cybersecurity.

For smaller organizations or those in highly regulated industries, this percentage might be higher to ensure adequate protection against evolving threats.

Step 10: Leverage Cloud Solutions

Objective: Utilize cloud solutions to enhance flexibility and scalability in your cybersecurity approach.

Benefits:

- Cloud platforms often offer cost-effective and scalable security solutions.
- They provide advanced features and real-time updates to address evolving threats.

Step 11: Regularly Review the Cybersecurity Budget

Objective: Ensure the budget remains aligned with evolving threats and business needs.

Actions:

- Schedule regular reviews to assess budget effectiveness and make necessary adjustments.
- Stay informed about new threats and adjust the budget to address emerging risks.

Call to Action: You Can Get Started Today

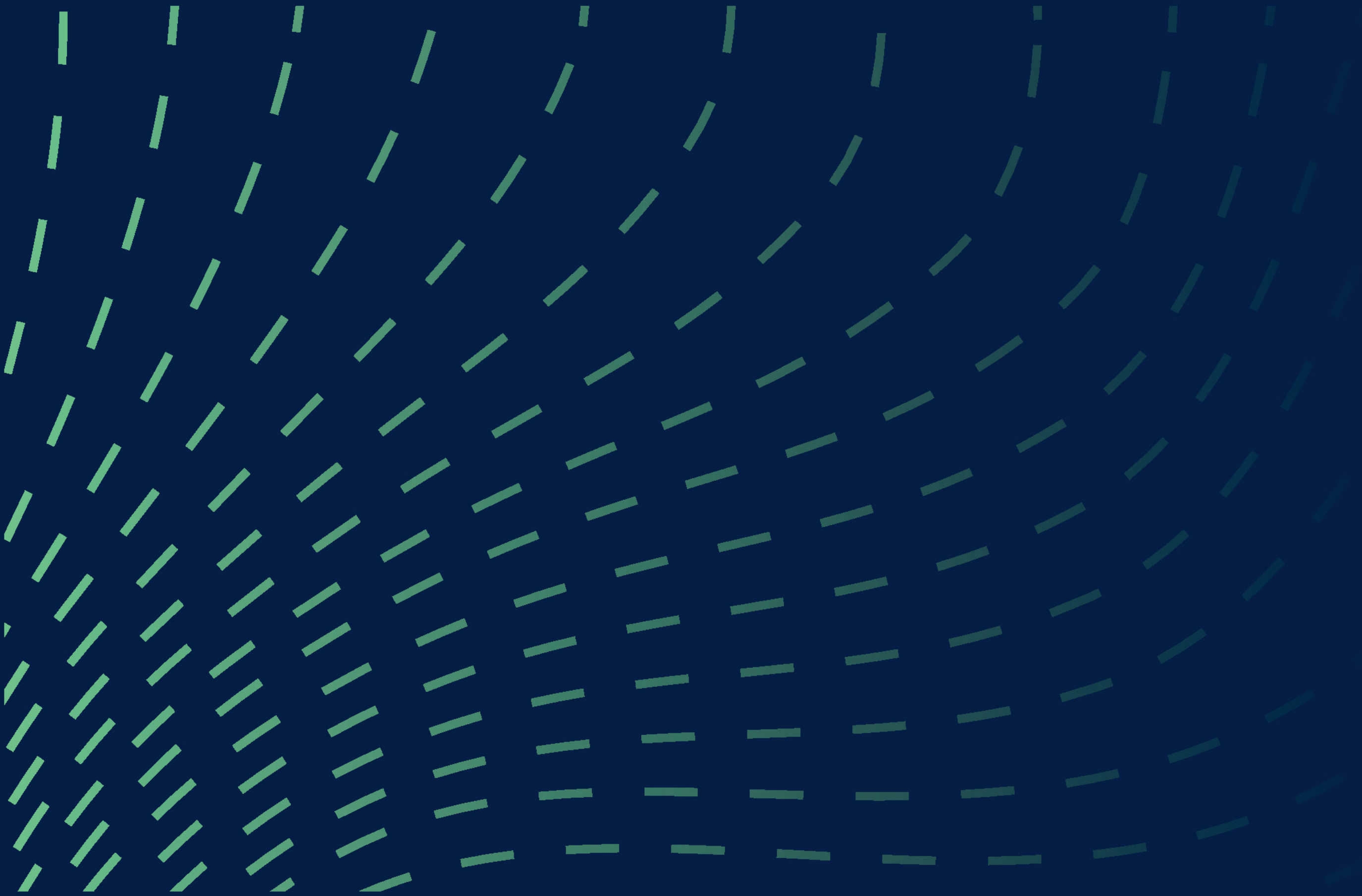
Creating a scalable cybersecurity budget is essential for protecting your business from cyber threats and ensuring compliance with regulatory requirements. As a business owner, you don’t have to navigate this complex process alone.

To take the next step in bolstering your cybersecurity, book your budget discussion with Tech 2020 Solutions to tailor a cybersecurity strategy that fits your needs.

Contact us at 516-876-8290 or email us at info@tech2020solutions.com to schedule a consultation. Let us help you safeguard your business with a comprehensive, future-proof cybersecurity budget.

CYBERSECURITY BUDGET WORKSHEET

#	ALLOCATION	BUDGET AMOUNT $
	PREVENTION	
	PREVENTION	
	PREVENTION	
	MISC	
	MISC	
	MISC	
	DETECTION	
	DETECTION	
	DETECTION	
	MISC	
	MISC	
	MISC	
	RESPONSE	
	RESPONSE	
	RESPONSE	
	MISC	
	MISC	
	MISC	
	OTHER	
	OTHER	
	OTHER	
	Total	



Contact us for further inquiries

www.tech2020solutions.com
info@tech2020solutions.com
516.876.8290 / 516.876.8761

TECH 2020 SOLUTIONS