DEFENDIFY®

A No BS 90-Day Plan to Get Your Cybersecurity Program Started

www.defendify.com

The cybersecurity platform for IT teams

INTRODUCTION

Cybersecurity
Let’s Talk Business

Imagine sitting down with the IT leaders in an organization with no dedicated security team, in a boardroom where a company’s leaders review long term strategies, or even in a room with regulators who have their eyes on the latest privacy rules. What’s the hot topic that keeps popping up? You guessed it - cybersecurity.

Security isn’t one person’s pet project anymore; it’s center stage, and everyone is paying attention. Boards fear a devastating cyber attack will negatively impact organization’s reputation and share prices. IT leaders are educating their teams and trading tips and tricks in their meetups. And regulators? They're rolling out new standards and rules to protect consumers’ personal data.

For small and midsize businesses, these conversations are extra important. Cybersecurity isn’t just something to keep your IT department busy; it’s a huge piece of the puzzle that makes up your overall business success. Plus, it’s all about keeping your customers' trust and staying on the right side of those tightening regulations.

Now, before you start worrying that this is going to be another tough, technical slog - it’s not. Think of this as your plain-speaking guide to what can often feel like a tricky subject. We're going to take all that big talk government regulations and security vendor tech-speak, break it down, and make it work for you and your business.

Together, we'll map out where you stand with your cybersecurity right now. No alarm bells, no jargon or BS - just a straight-up look at what's what. From there, we'll get into strategy and how you can beef up your defenses in a way that makes sense for your business. No off-the-rack solutions here; we're all about tailoring to fit.

And don't worry, we won't leave you to do the tech talk at company meetings. By the end of this, you're going to feel comfortable enough to join in on those discussions, steer them even; showing off and justifying a cybersecurity setup that works for you, and impresses everyone from your coworkers to the powers-that-be.

Getting cybersecurity right is like unlocking a new level in the business world. It's a solid foundation that supports everything else you're working on. Let's turn those high-level chats into real results for your business. Ready to dive in? Let's get to business - the cybersecurity business.

A Strategic Blueprint for Cybersecurity The First 30 Days

Chapter 1

Day 30

No scare tactics. Let’s push past the usual fear-inducing chatter about cyber doom and focus on empowerment. Yes, cybersecurity involves some serious threats. But today, we’re going to tackle them head-on, rationally, and effectively. Cybersecurity is, after all, a critical component of any modern business, and it’s well within your grasp to master it.

In the formative stage of protecting your business against cyber threats, you need to begin with a structured approach that examines the roots of your cybersecurity posture. The first 30 days will set the tone for your defensive strategy, as it’s crucial to align the organization’s cybersecurity approach with its broader objectives and constraints.

Align Goals

Before diving into the specifics of your program, it's essential to set the stage by aligning the cybersecurity strategy with the broader organizational goals and context. This alignment ensures that your efforts to bolster cybersecurity directly contribute to the overarching objectives of the organization.

Role Clarification

Whether you are newly appointed or looking to enhance an existing program, understand what prompted the creation of your role. Was it in response to a mandate from the C-suite or board, due to customer or partner requirements, compliance lapses, or following a significant incident?

Budget Analysis

Get a clear understanding of the current cybersecurity budget. Examine last year's expenditures to see how funds were allocated. Talk to leadership to understand how they arrived at this year's budget for both internal and external spending (covering technology and personnel).

Stakeholder Engagement

Start conversations with key leadership stakeholders to understand their concerns and ensure alignment on the cybersecurity goals. Securing buy-in at this stage is instrumental to smoothly executing your plan.

After aligning the fundamentals, the strategic blueprint can then delve into the specific actions and assessments needed to solidify the organization's cybersecurity defenses.

Reviewing Financial Constraints and Compliance Obligations

Financial Analysis

Every penny allocated towards cybersecurity should be scrutinized for its effective deployment and returns. Examine previous expenditures to understand which investments produced protective benefits and which, if any, underperformed. This analysis should establish a clear correlation between expenses and security outcomes.

Regulatory Compliance

Organizations often operate under various regulatory frameworks, from sector-specific ones like DOD regulations to privacy statutes like the EU's GDPR or the California Consumer Privacy Act. Failure to comply can result in fines and damage to your organization's reputation.
A thorough compliance audit should be undertaken to ensure that current security controls align with the relevant legal frameworks.

Execute a Comprehensive Asset Inventory

You need to know what assets you are managing in order to protect them. Therefore, a detailed catalog of your organization's digital and physical assets is vital to any cybersecurity strategy. This inventory should include all tangible hardware, the software that operates on it, and the critical data within your systems. Recognize the value and vulnerability of each asset, understanding not just what it does but also why it is a target.

Prioritize Using Risk-Ranking

Once your asset inventory is known, build consensus about which systems and data are most critical to the organization's goals so you can prioritize resources and defenses. Assign a risk value to each based on the likelihood of compromise and the potential impact it would have – critical, high, medium, and low are fine. By tiering your assets in terms of risk, you can allocate time, money, and personnel to areas where they will be most effective.

Understand Organizational Risk Appetite

Knowing your organization's risk appetite is crucial. Decision-makers should critically define the level of acceptable down-time, data loss, or system compromise that the enterprise could accommodate without significant disruption. This understanding will tailor your security measures to realistic and operationally acceptable levels.

Gather Insights through Stakeholder Interviews

Engage stakeholders from across the organization, including finance, end users, engineering, and executive leadership. An inclusive approach will provide a composite picture of the security requirements for the business as a whole. Your goal is to understand their concerns, dependencies on specific resources, and essential functions that need protection. Incorporating these insights will not only create a security approach that covers all bases but also fosters an organization-wide culture of security awareness.

Inventory your Cybersecurity Tools, Technologies & Consultants

Tools and Technologies Inventory

Careful inventory and assessment of your cybersecurity tools is as important as that of your physical assets. Determine what is in place, and redundancies in your arsenal. Evaluate your existing technologies and controls, including firewalls, antivirus software, vulnerability scanning tools, security awareness training assets, and detection and response capabilities.

Consultants and Personnel Review

Outsourcing cybersecurity can be a strategic move, bringing in specialized expertise and allowing for scalability. However, it is critical to assess the performance and alignment of any third-party consultants or cybersecurity firms with your business objectives. Look to see if you can lower costs and gain efficiencies by consolidating partners.

Charting the Course Ahead

At the conclusion of the first 30 days, your organization should have a broad yet detailed understanding of its existing cybersecurity capabilities and requirements. By getting alignment between cybersecurity initiatives and corporate goals, engaging stakeholders, understanding your risk profile, and prioritizing assets and resources, you can now design a flexible and effective cybersecurity program.

Remember, this plan is not static. It must be capable of evolving as new threats emerge and as your business grows and changes. Regular review and modification of plans, financial investments, compliance obligations, and security controls are critical. Ensure, too, that your staff remains well-informed of the latest cyber threats and best practices.

In summing up, the initial 30-day strategy is about proactive cybersecurity leadership. It calls for a combination of strategic foresight, operational reflection, and a culture committed to security. This multi-layered approach provides organizations with a framework capable of adapting to the creativity and innovation of criminals, paving the way continuously improving security.

Begin Assessing The Second 30 Days

Chapter 2

As you transition into the second 30-day phase of your cybersecurity program, your focus shifts from aligning goals to rigorously assessing the current state of your security landscape.

These weeks – five through eight – are dedicated to evaluating, benchmarking, and identifying areas where your cyber defense controls are sufficient or fall short.

Benchmark Organizational Security

The best way to start is by establishing a baseline for the organization's existing cybersecurity posture. Benchmarking against industry standards provides a clear view of your organization's security strengths and weaknesses. It is best to use a recognized control framework like ISO 27001, Center for Internet Security (CIS) Controls, or the NIST Cybersecurity Framework as yardsticks. These frameworks offer a structured approach, covering everything from asset management to data protection and incident response. Their widespread recognition and adoption mean that aligning with them not only boosts our cybersecurity resilience but also fosters trust among partners and clients.

Cybersecurity Control Assessment

The Deep Dive

Once a framework is selected, use it to conduct a thorough cybersecurity control assessment. This step is akin to an in-depth health check that scrutinizes existing controls against industry best practices for addressing potential threats.
This allows teams to systematically evaluate controls to identify areas where existing controls are robust as well as areas that require additional attention.

Policy and Privacy

The Framework of Trust

An essential component of your assessment phase is reviewing the organization's security and privacy policies. The existence, completeness, and relevance of these policies are fundamental to a sound cybersecurity strategy. Be sure they address all critical areas such as data privacy, access control, and incident response (IR) management.

Upon identifying gaps, add missing policies and update current policies and Incident Response plans. This documentation forms the backbone of our cybersecurity governance, ensuring that our practices are grounded in a proactive and planned approach.

Review Cybersecurity Testing Outcomes

A Look in the Mirror

The assessment period must include a detailed review of all cybersecurity testing results. Key questions at this stage include:

Is there a robust vulnerability management program in place? How is patching managed and prioritized? Unpatched systems and vulnerable software provide criminal hackers with a simple attack vector.

Do you have 24/7/365 Detection and Response capabilities? How many incidents were recorded in the previous year? Review whether you are responding quickly and appropriately to attacks.

Have network and application penetration tests been conducted recently? Analyzing these results can uncover weaknesses a skilled attacker can leverage to execute ransomware attacks or steal valuable data.

What other assessment and testing tools and programs are currently deployed? Evaluating these tools' effectiveness is vital for ensuring they meet our organizational needs and that you're not investing in redundancies.

Revisiting these areas not only helps in recognizing your current capability to identify and respond to threats but also in laying the groundwork for continuous improvement in your cybersecurity efforts.

Identify Immediate Vulnerabilities

Vulnerabilities in applications and systems are inevitable. Identifying critical vulnerabilities that require immediate remediation is crucial. A scan of infrastructure and devices for known vulnerabilities, such as outdated software or default passwords, can quickly improve your security profile. If resources allow, scheduling a penetration (pen) test can provide invaluable insights into our defenses' effectiveness from an attacker's perspective.

Move Forward with Informed Vigilance

By the end of the assessment phase, an clear picture of your cybersecurity strengths and areas for improvement emerges. This understanding forms the foundation for building targeted strategies to bolster your defenses.

Key to this phase is not just the identification of gaps but the prioritization of issues based on their potential impact on the organization. This risk-based approach ensures that resources are allocated efficiently, focusing efforts where they are needed most to mitigate significant threats.

In the final chapter, armed with the information gathered in our assessments, we will plot the course to improving your organization's cybersecurity posture. The aim is clear: to not just defend but to proactively adapt and stay ahead of cyber threats, ensuring the security and resilience of your systems and data and, by extension, the trust of your colleagues and customers.

The journey from aligning goals to assessing current state sets a solid foundation. The insights gathered will guide you in deploying stronger defenses, crafting strategic policies, and engaging in continuous improvement, elevating your cybersecurity readiness to new heights.

Plan, Budget and Implement The Final 30 Days

Day 90

Chapter 3

As we move into the third 30-day period of our cybersecurity journey, it's time to transition from preliminary assessments to strategic actions. This phase involves the creation of a well-defined plan, establishing a detailed budget, and beginning the formal implementation of controls. In short, we will take the findings from initial assessments and turn them into specific activities that meaningfully boost your cybersecurity posture.

Utilizing Assessments as a Benchmark

Our preliminary assessments guide our strategy, providing a clear picture of our current security posture and critical weaknesses to guide the prioritization of our efforts.

A Comprehensive Approach

Ongoing Assessments & Testing

No organization's secure posture is static. Changes in the environment and in the threat space can leave once secure systems open to attacks. This means ongoing assessments and regular testing are mandatory for maintaining a resilient security stance. It is important to integrate continuous vulnerability scans, penetration testing, and security assessments into your plan to ensure your defenses remain robust and proactive against emerging threats.

Policies & Employee Awareness Training

Unsafe data handling can result in loss of personal information and other regulated data. Phishing attacks exploit busy users and can lead to breaches and ransomware attacks. Crafting clear, applicable policies and investing in employee cybersecurity awareness form a dual approach to strengthening the human firewall. We recommend developing clear security policies and comprehensive training modules – including phishing simulations – tailored to educate end users on best practices and threat recognition.

Endpoint Detection & Response

Criminals work around the clock. Establishing advanced detection mechanisms and a swift, structured incident response plan is imperative. Your plan should include the deployment of state-of-the-art detection tools and the formulation of a 24/7/365 incident response by cyber experts to mitigate threats efficiently and minimize potential damage. In many organizations, establishing an internal SOC is not practical. If that is the case, consider a Managed Detection and Response solution partner.

Develop a Formal Budget

With your cybersecurity plan as the blueprint, the next step is to secure the financial investment required to bring this vision to fruition.

Conduct Discovery Calls with Vendors

Engaging with various cybersecurity solution providers through discovery calls helps teams understand the landscape of available tools and services. These interactions are crucial for identifying the solutions that best match your needs and budget constraints.

Prepare Detailed Cost and Budget Plans

A detailed budget is required to, provide a clear breakdown of costs associated with each component of your plan. This should cover everything from software subscriptions to hardware procurement and team training expenses.

Presenting the Budget

Articulating your budget requirements to non-technical decision-makers needs to be simple and clear. Your presentation should not only to inform but also persuade your audience on the necessity of each financial request. Avoid technical jargon and focus on the impact of each expenditure to the organization's goals and security posture.

Explaining the "Why"

Linking your budgetary needs directly to the findings from your assessments and the agreed to goals is crucial. This demonstrates the direct correlation between proposed spending and the enhancement of your cybersecurity defenses, emphasizing the value of each investment.

The Evolving Cybersecurity Landscape

Building and maturing a cybersecurity program takes time. Touch on longer term plans to prepare stakeholders for future needs. While your goal is approval of your initial proposal, you also need to prepare others for the potential need for flexibility and ongoing investment in your cybersecurity capabilities.

Implementation

With budget approval, we start the hands-on phase of deploying your cybersecurity strategy.

Deploy and Build Your Program

Map out and systematically implement the components of your cybersecurity plan, from technical defenses to policy rollouts and staff training sessions. This period is marked by careful coordination and meticulous execution to ensure comprehensive coverage.

Communicate Progress to Stakeholders

Regular updates to stakeholders about the implementation progress maintains transparency and fosters ongoing support. These communications underscore the positive impact of your initiatives and outline any adjustments or additional needs.

Outline the Long-Term Cybersecurity Strategy

While focused on immediate implementation, keep an eye on what's next and continue to communicate this to stakeholders. This includes future enhancements, evolving threat landscapes, and plans for the continuous improvement of cyber defenses.

In conclusion, the third 30-day phase is a linchpin in your cybersecurity journey, translating strategic planning into tangible outcomes. By meticulously planning, securing necessary funding, and executing your strategy with precision, you lay the groundwork for a resilient and robust cybersecurity posture that not only addresses present challenges but is also scalable for future needs.

Next Steps

The third 30-day phase translating strategic planning into tangible outcomes. By meticulously planning, securing necessary funding, and executing your strategy with precision, you lay the groundwork for a resilient and robust cybersecurity posture that not only addresses present challenges but is also scalable for future needs.

As you move forward, keep an eye on and continue to communicate with stakeholders. This includes future enhancements to your countermeasures, communicating on evolving threat landscapes, and plans for the continuous improvement of cyber defenses.

Remember, building and maturing a cybersecurity program is a process.
By regularly assessing your posture and responding to new threats, you can build a resilient cyber defense capable of maintaining sensitive assets and achieving organizational goals.

DEFENDIFY

A No BS 90 - Day Plan to get Your Cybersecurity Program Started