CYBERSECURITY STRONG STRATEGY

STEP BY STEP GUIDE

Collected by: Mohammad Alkhudari

2024

GREEN CIRCLE

be aware..be secure

This document is a comprehensive guide to cybersecurity strategy. It defines what a cybersecurity strategy is and why it's important, especially in light of the increasing number of cyberattacks. It also details the steps involved in creating and implementing a robust cybersecurity plan, including conducting risk assessments, setting security goals, evaluating technology, selecting a framework, reviewing security policies, and creating a risk management plan. The guide emphasizes the importance of continuous monitoring and evaluation of the strategy to ensure its effectiveness in the face of evolving threats. It also highlights common pitfalls to avoid and answers frequently asked questions about cybersecurity strategy.

The main topics in this document are:

- **Defining a cybersecurity strategy and its importance.**
- **Implementing defense in depth and zero trust security models.**
- **Comparing cybersecurity strategies for enterprises and small businesses.**
- **Understanding the importance of cybersecurity strategies.**
- **Recent increases in cyberattacks and their impact on various industries.**
- **Regulatory requirements, penalties, and the impact of the new mobile workforce.**
- **Data center and cloud transformations and their security implications.**
- **Developing a security strategy and the steps involved.**
- **Evaluating technology, security frameworks, and risk management plans.**
- **Implementing, evaluating, and maintaining a cybersecurity strategy.**
- **Common pitfalls to avoid and frequently asked questions about cybersecurity strategy.**

What Is A Cybersecurity Strategy?

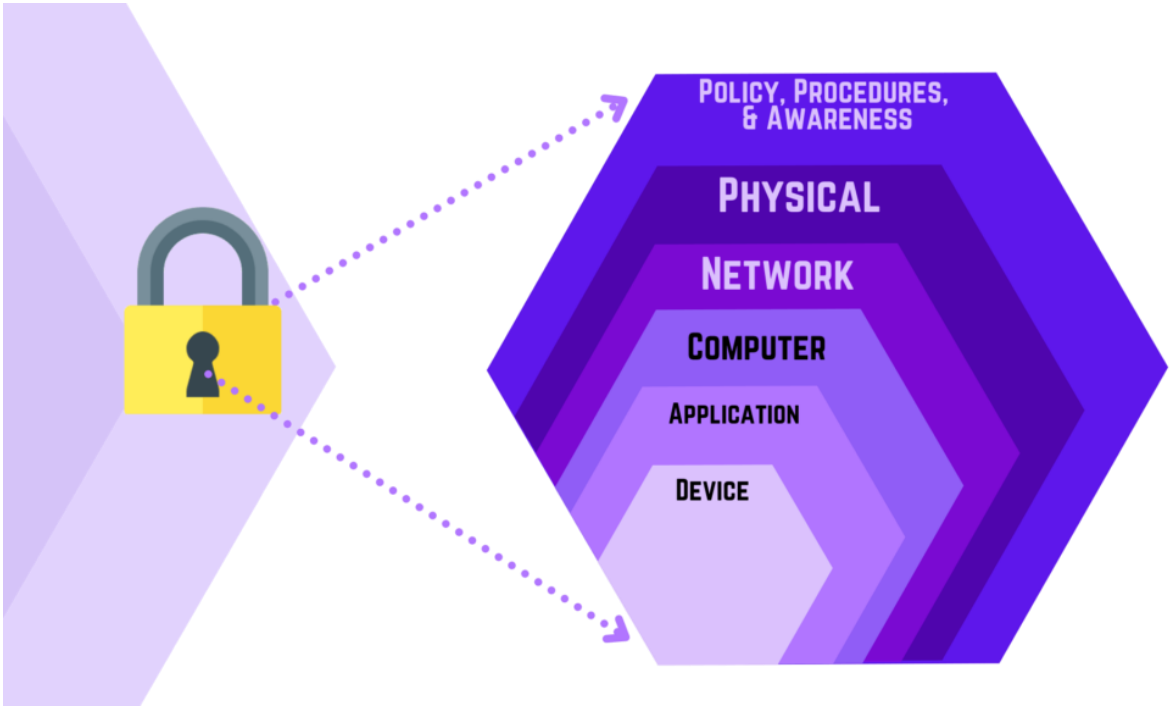
A cybersecurity strategy is a plan that involves selecting and implementing best practices to protect a business from internal and external threats.

This strategy also establishes a baseline for a company's security program which allows it to continuously adapt to emerging threats and risks.

Defense In Depth Strategy

To effectively manage emerging threats and risks today, the cybersecurity strategy should consider implementing defense in depth.

The goal of implementing this strategy encompasses the layering of security defenses.

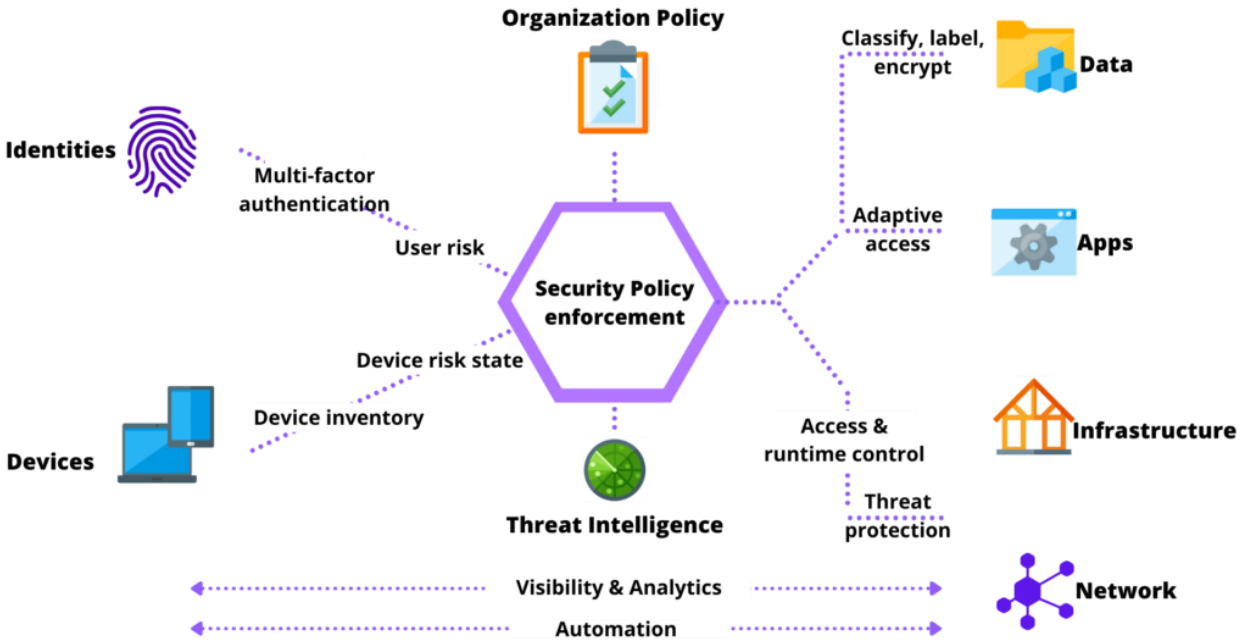


When applied correctly, this strategy increases an organization's ability to minimize and limit the damage caused by a threat actor.

A company may implement a combination of multiple tools to protect their endpoint devices, such as antivirus, anti-spam, VPN, and a host firewall.

Zero Trust Security + Defense In Depth

Layering multiple tools to create defense in depth is a solid approach towards laying the foundation for a sound security strategy, however, a company must have resources available to support and monitor the functionality of the tools.



This may introduce additional complexity.

To address this issue, a zero trust model should be implemented as well.

Zero trust implies, never trust, always verify.

Multifactor authentication and machine learning are components of zero trust, which provides the company with visibility on who and how the assets are being utilized within the network.

Cybersecurity Strategy For Enterprise VS Small Business

How is a security strategy different between enterprise and small business?

The primary difference between a large organization and a SMB (Small to Medium sized Business) is the number of employees and revenue.

Regardless of the size of the business, both types of companies can be targets of threat actors.

An SMB that handles HIPAA data is required to abide by the same regulations as a large enterprise.

A large enterprise has a larger footprint of data to secure and may require a larger investment in an IT budget to invest in the proper controls to secure the data, however, threat actors and email phishing do not discriminate based on the number of employees.

It is obvious that the larger revenue-generating organizations are prime targets for an attack.

The enterprise in most cases has insurance and may have funds available to pay up in a ransomware attack.

Read More: How To Prevent Ransomware: An Expert Guide

It is a general perception that a SMB has limited budgets and resources to fully secure their networks.

This makes them also susceptible to attacks.

Therefore, a cybersecurity strategy is just as essential to the large enterprise as the SMB.

The business model and assessed risk the organization has in its care determine the security needs of the business.

Affordable Security Options Available For SMBs

The challenge SMBs face have to deal with tight budgets, resource planning, staying current with technology, and staying competitive in their markets.

To meet the challenge, careful planning of where expenditures are needed is paramount, particularly when it involves the security of their business.

The good news is that many security vendors have adapted their large enterprise product suite to the SMB market.

Symantec/Broadcom, McAfee Small Business Edition, Microsoft Office 365 Business has subscriptions for less than 300 licenses.

Microsoft recently announced Microsoft Defendor for Business – an enterprise grade endpoint security designed for businesses with up to 300 employees.

At $3.00/mon per user, we predict this offering will attract a lot of attention in the SMB space to integrate into their existing Microsoft technology suite.

Why Are Cybersecurity Strategies Important?

Creating and implementing a cybersecurity strategy is more critical than ever as the number of security-related breaches during the pandemic increased by 600%.

Further, the average ransomware payment leaped 82% in 2021 to $572,000 from the previous year.

There's no sign of these attacks slowing down and evidence to support that threat actors will only continue to attack vulnerable systems.

Increase In Recent Cyber Attacks

Cyber attacks are growing and becoming more disruptive to businesses overnight, and it's only going from bad to worse with threat actors finding new methods of attack.

We've covered a number of the recent cyber attacks this year including:

- Microsoft Azure SSRF Vulnerabilities
- Slack GitHub Account Hack
- Data Of 228 Million Deezer Users Stolen
- Twitter Leaks Data On 200 Million Users
- Cisco Cyber Attack
- Twitter Zero-Day
- Starlink Dish Hacked
- Mantis Botnet
- Maui Ransomware Attack
- Conti Ransomware Attack
- The Kaseya Ransomware Attack
- Saudi Aramco's $50 Million Data Breach
- Accellion FTP Data Breach

Continue Reading: Top 10 Most Exploited Security Vulnerabilities In 2022

Attacks are prominently increasing in all industries, with a recent study establishing that the retail industry is at the most risk to cyber attacks through social engineering methods.

89% of healthcare organizations have also experienced a data breach in the past 2 years, even though security measures had been put in place.

This is due to web applications connected to critical healthcare information being vulnerable to cyber attacks.

The threat is just as high for small businesses in almost every industry.

43% of cyber attacks target small businesses, a problem too big for small business owners to ignore.

Therefore, it is important to address your company's cyber risk and define a strategy due to more organizations using online applications and cloud based applications.

With this being identified, the rapid increase in cyber attacks is inevitable and the effects can be simply, detrimental to your business.

The SolarWinds and Colonial gas pipeline ransomware attacks reveal how bad actors can uncover weaknesses in software code or poor security controls.

If these threat actors can pinpoint their attacks on systems that monitor the networks of the government and energy sources, hacking into your company unfortunately can be considered business as usual.

According to a 2021 security data breach report, there were 1,767 publicly reported breaches in the first six months of 2021, which exposed a total of 18.8 billion records.

Regulatory Requirement & Penalties

Different regulations and laws will levy fines against organizations if they are found to breach data or fail to comply with regulations, such as HIPAA, PCI, SOX, GBLA, or GDPR.

Due to the current growth of companies processing data, platforms such as storing data on the cloud and machines that supports the data has also increased.

The areas of attack and vulnerabilities to cyber attacks have increased due to more data being processed on premise or the cloud.

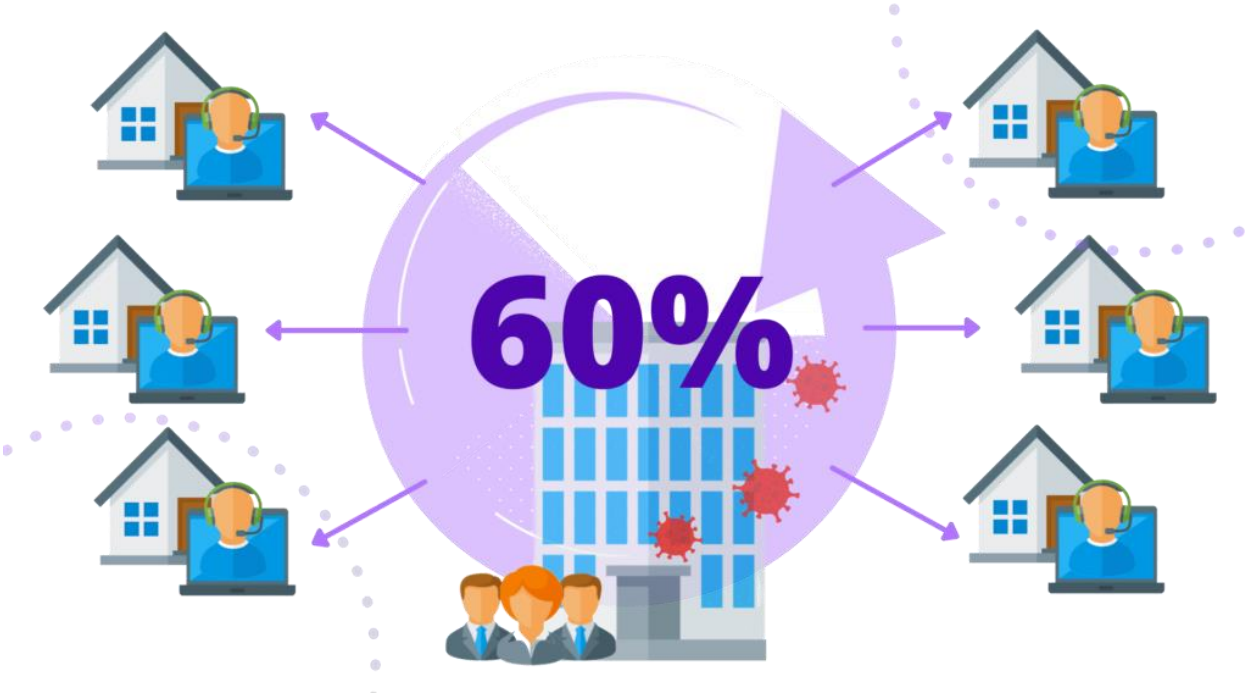
Recent worldwide data breach statistics indicate that many organizations are falling short on either the development or implementation of their cybersecurity strategy.

New Mobile Workforce

The COVID-19 pandemic has transformed the methods many people are working and will most likely continue to change how they work in the future.

VPN technology has been around for some time, however, this ability to remotely connect to the company's network from their home or away from the office is common practice today.

According to a new forecast from International Data Corporation, the U.S. mobile worker population will grow at a steady rate over the next four years, increasing from 78.5 million in 2020 to 93.5 million mobile workers in 2024.



By the end of the forecast period, IDC expects mobile workers will account for nearly 60% of the total U.S. workforce.

The ability to work remotely has allowed many businesses to remain profitable, especially if the role of the employee does not require face-to-face interaction or handling of equipment.

However, remote working does introduce risk, such as, stolen devices containing downloaded sensitive files, or weak passwords or out-of-date software or applications can provide an easy entry for bad actors into the corporate network.

Data Center & Cloud Transformations

Today, businesses are leveraging the power of the traditional data center along with the cloud.

Many companies today are developing business applications in cloud containers unknown to support staff.

A cloud research firm reported that breaches related to cloud misconfigurations in 2018 and 2019 exposed nearly 33.4 billion records in total.

On-premises server farms within the data center are either underutilized or unmanaged on the network.

In many cases, access to sensitive data is not secured properly, or there are blind spots in determining the data owner to resolve security issues.

These are a few problems when it comes to data protection and the cloud transformation facing many organizations today.

Policies To Consider When Developing A Security Strategy

An important element of an effective security strategy is the information security policy.

Security policies are a set of written practices and procedures that all employees must follow to ensure the confidentiality, integrity, and availability of data and resources.

The security policy provides what the expectations are for the business, how they are to be achieved, and describes the consequences for failure with the goal of protecting the organization.

In addition to a single Information Security Policy, many organizations opt to have specific policies instead of one large policy.

Breaking out the policies into smaller policies make it friendlier for the end user to digest.

Below are sample policies that can be written in addition to the main security policy.

Network Security Policies

These are a general set of security policy templates that set of standardized practices and procedures that outlines rules of network access, the architecture of the network, and security environments, as well as determine how policies are enforced.

Explore Resource

Data Security Policies

Data security policies are formal documents that describe an organization's data security goals and specific data security controls an organization has decided to put in place.

Data security policies may include different types of security controls depending on the business model and specific threats being mitigated.

Explore Resource

Workstation Policy

General security (use an antivirus, lock unattended, password usage, patching).

Download Template >>

Acceptable Use Policy

- Acceptable/unacceptable Internet browsing and use
- Acceptable/unacceptable email use
- Acceptable/unacceptable usage of social networking
- Electronic file transfer of confidential information

Download Template >>

Clean Desk Policy

Describes reasons for a clean, uncluttered desk that may have sensitive notes laying on a desk or taped to monitors.

Download Template >>

Remote Access Policy

- Definition of remote access
- Who is permitted (employees/vendors)
- Types of permitted devices/operating systems
- Methods permitted (SLVPN, site-to-site VPN)

Download Template >>

Steps To Creating A Cybersecurity Plan

There is no one size fits all approach when creating a cybersecurity strategy as every business need is unique.

In this section, we walk through 8 steps that your organization can use as a model to develop and implement a successful security strategy.

Step 1: Conduct A Security Risk Assessment

An IT enterprise security risk assessment is performed for organizations to assess, identify, and modify their overall security posture.

The risk assessment will require collaboration from multiple groups and data owners.

This process is required to obtain organizational management's commitment to allocate resources and implement the appropriate security solutions.

https://purplesec.us/learn/cybersecurity-strategy/

A comprehensive enterprise security risk assessment also helps determine the value of the various types of data generated and stored across the organization.

Without valuing the various types of data in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most.

To accurately assess risk, management must identify the data sources that are most valuable to the organization, where the storage is located, and their associated vulnerabilities.

A list of areas that are sources for the assessment are listed below:

Identify Assets

Leverage your current asset tracking systems (A repository containing all assets, i.e., workstations, laptops, operating systems, servers, corporate owned mobile devices).

Determine Your Data Classifications

- **Public** – Any data you publicly share such as website content, publicly available financial information, or any other information that would not impact the business negatively by being breached.
- **Confidential** – Data that should not be shared with the public. Confidential data may be used with 3rd parties or in limited cases made available to external legal entities, but would require a Non-Disclosure Agreement (NDA) or other protections to prevent the data being accessed by the public.
- **Internal Use Only** – Similar to Confidential data, but which should not or cannot be shared with 3rd parties.
- **Intellectual Property** – Data that is critical to the core business and would damage the company's competitiveness were it to be breached.
- **Compliance Restricted Data** – This is data that is required to be strictly controlled. Access to, and storage of this information must comply with the framework it falls under such as CMMC, HIPAA, HITRUST, NIST.

Map Your Assets

- **Software** – Maintain a repository for authorized corporate software.
- **Systems** – Leverage a Central Management Database (CMDB) for asset mapping back to a system or asset owner.
- **Users** – Catalog users into groups via role assignments, i.e., Active Directory.
- **Identity** – Ensure and regularly track user assignments to an asset/resource based on their current role or function.

Identify Your Threat Landscape

- **Assets + Vendors** – Work with Legal teams to identify contracts with 3rd parties, including NDA's or BAA list of business provides healthcare.
- **External vs internal infrastructure** – Identify all network egress and ingress points
- **Map where environments connect** – Ensure network diagrams are available and up to date. If conducting business in the cloud, ensure infrastructure diagrams are available as well.

Prioritize Risks

- Perform a Business Impact Analysis (BIA) to identify critical systems and data owners.

- Create and maintain a risk register to identify systems or assets that pose the highest risk to the Confidentiality, Integrity, and Availability of the organization's business systems.

Reduce Your Business's Attack Surface

- Implement Network Segmentation
- Conduct Penetration Testing
- Perform Vulnerability Management

Step 2: Set Your Security Goals

A key component of the cybersecurity strategy is to ensure that it aligns or is in step with the business goals of the company.

Once the business goals are established, the implementation of a proactive cybersecurity program for the entire organization can commence.

This section identifies various areas that can assist in creating the security goals.

Determine Your Security Maturity

- **Perform Assessment Of Your Security Program** – Review architecture, past and recent logged incidents, breaches, and review performance of Identity, Access, and Management system.

- **Determine Status Of Metrics** – Review Service Level Agreements (SLA's) or Key Performance Indicators (KPI's).
- **Benchmark Current State** – Use a self-assessment tool that measures the maturity of the organization's cybersecurity capabilities in a consistent manner.

Understand Your Company's Risk Appetite

Output from a risk register and impact analysis will help determine how and where cybersecurity should be prioritized.

Set Reasonable Expectations

- **Resources** – Does expertise exist to meet the cyber strategic goals? Does the budget exist to hire Managed Security Services Provider (MSSP)?
- **Timelines** – Set milestones for each strategic goal and regularly communicate status to stakeholders.
- **Budget** – Carefully review results of the cybersecurity risk assessment. The budget depends on the outcome of the assessment and determines if additional systems should be acquired to lower or mitigate risk.
- **Ability to execute** – Once expectations are known, review the state of resources to determine capability to make it happen.

Handle Low Hanging Fruit Immediately

The term 'Low hanging fruit is a business metaphor that refers to tasks that are simple and easily attainable, i.e., a quick win.

If executed in a timely manner, this will provide and exude confidence that you will continue to attain strategic goals as you address the more difficult challenges.

Step 3: Evaluate Your Technology

Another key component of the cybersecurity strategy is the evaluation of technology.

Once the assets have been identified, the next step(s) are to determine if these systems meet security best practices, understand how they function on the network, and who supports the technology within the business.

The items below will assist with the gathering of the information in this key area of the security strategy roadmap.

What Is Currently In Use?

Identify the current state of asset Operating Systems.

With End-of-Life technology, patches, bug fixes and security upgrades automatically stop.

As a result, your product security is at risk if there are business applications running on these systems and could potentially lead to compromise.

Are There Sufficient Resources To Manage These Platforms?

As listed in Step 2 of the plan, the expertise to support the technical platforms is critical.

Resources are required to patch these systems.

In the event of a zero-day attack, resources must be available and responsive to mitigate the threat, as well as recover from an incident.

Does Technology Bloat Exist?

Technical bloat is a known problem for large enterprise environments that have systems that perform duplicate services.

Poorly written code by developers may lead to 'technical debt' – basically, it will cost more, in the end, to rework and document the code properly compared to the initial release.

Unapproved installation of software can cause issues as well.

These systems are usually created by independent teams without the involvement of the support staff. This practice is referred to as Shadow IT.

How Does Data Flow In And Out Of Your Systems Because Of Using This Technology?

Documentation is essential to identifying security weaknesses in technology.

Best practices should be implemented with security engaged during the lifecycle of application development to production release.

Step 4: Select A Security Framework

There are multiple frameworks available today that can help you create and support the cybersecurity strategy; however, you can't secure what you can't see.

The results of the cybersecurity risk assessment, vulnerability assessment, and penetration test can help you determine which framework to select.

The security framework will provide guidance on the controls needed to continuously monitor and measure the security posture of your organization.

The items below can assist in the selection of a security framework.

Determine Your Current Security Maturity

Leverage the output from the results gathered in Step 2 related to the maturity model.

Identify What You're Legally Required To Protect

Depending on the vertical or sector of your organization, certain regulations exist that must be adhered to or be subject to stiff penalties, i.e., HIPAA, SOX, PCI, or GDPR.

There are frameworks that address a specific regulatory requirement of your organization.

Choose a framework that is feasible and aligns with your company's strategic business goals.

Once an understanding of the requirements of the business are known, you can then begin the selection process for a framework:

- PCI-DSS for consumer credit card industry
- CMMC for DoD suppliers
- NIST for healthcare
- CIS top 18 for SMBs

Step 5: Review Security Policies

The goal of security policies is to address security threats and implement cybersecurity strategies.

An organization may have one overarching security policy, along with specific sub policies to address various technologies in place at the organization.

To ensure security policies are up to date and address emerging threats, a thorough review of the policies is recommended.

Below are steps that can help you review the state of your security policies.

What Policies Are In Use Today?

A periodic review of the current policies should be conducted to ensure they align with the business model.

Are These Policies Enforced Or Just Written?

The policies should be enforceable.

Each person in the organization is accountable to how they adhere to the security policies.

The policies should be readily available for employees to view.

The policies should be mapped to security controls that monitors, logs, or prevents an activity that is documented in the policy.

Train Employees In Security Principles

Security awareness training is essential because it can be used to enforce security policies.

There are multiple options to achieve this goal:

- Select a platform that manages real time phishing campaigns through corporate email and provides immediate feedback to senior management.
- Invest in security awareness training applications
- Hire guest speakers to keep security education interesting, i.e., lunch and learns or annual awareness events.

Step 6: Create A Risk Management Plan

Creating a risk management plan is an essential component of the cybersecurity strategy.

This plan provides an analysis of potential risks that may impact the organization.

This proactive approach makes it possible for the business to identify and analyze risk that could potentially adversely the business before they occur.

The following policies below are examples of best practice policies that can be incorporated into your risk management plan.

- **Data Privacy Policy –** Provides governance around the handling of corporate data is handled and secured properly.
- **Retention Policy** – Describes how various types of corporate data should be stored or archived, where, and for how long.
- **Data Protection Policy** – This policy states how the business handles the personal data of its employees, customers, suppliers, and other third parties.
- **Incident Response Plan –** This plan outlines the responsibilities and procedures that should be followed to ensure a quick, effective and orderly response to Security Incidents.

Step 7: Implement Your Security Strategy

At this stage of the strategy, assessments are near completion along with policy plans.

It is now time to prioritize remediation efforts and assign tasks to teams.

Assign remediation items by priority to internal teams.

If your organization has a Project Management office, enlist this team to manage the project.

If there isn't a project team available, provide leadership and work with the internal teams and plan the efforts.

Set realistic remediation deadline goals

Setting deadlines that are too aggressive and unrealistic is a recipe for disaster.

Better to set a reasonable time frame and exceed expectations.

Step 8: Evaluate Your Security Strategy

This final step in the creation of the cybersecurity strategy is the start of an ongoing support of the security strategy.

Threat actors will continue to exploit vulnerabilities regardless of the size of the organization.

It is imperative that the security strategy be monitored and tested regularly to ensure the goals of the strategy align with the threat landscape.

The items below are key points to consider maintaining a continuous and comprehensive oversight.

Establish A Board Of Key Stakeholders Throughout The Organization

Stakeholders are critical to the success of the security strategy.

This group provides resources and ongoing support for the project and is accountable for enabling success.

Conduct Annual Risk Assessment

The goals of the security strategy typically do not change very often, since they should align closely with the goals of the business, however, the threat landscape changes quite often.

It is imperative that the strategy be revisited to determine if any gaps exist in the program. An annual review is a general accepted review period.

Obtain Feedback From Internal And External Stakeholder's

When stakeholders understand that you are making strategic decisions about the security of the business, they will accept and appreciate your actions.

The information you receive from internal and external stakeholders will help justify security budgets, processes, and overall business strategies.

Common Pitfalls To Avoid When Implementing Your Cybersecurity Strategy

The success of the cybersecurity strategy relies on careful planning with buy in from executive management.

Without leadership support, the strategy will falter and will ultimately fail.

Leadership from the senior team is the most significant factor in the success of the cybersecurity strategy.

There are pitfalls or roadblocks that may still be in the path that need to be recognized, avoided, or mitigated.

Technology Sprawl And Lack Of Documentation

Over time, new servers and applications are provisioned to accommodate a business requirement or development testing.

If there is a lack of change management and decommissioning processes, these systems may spread out and remain on the network indefinitely.

These systems may remain unpatched or can become sources of backdoors.

Legacy Systems

Legacy system that cannot be patched or no longer supported is a high risk.

Lack of continuous monitoring of the cybersecurity plan or weak application security management is a byproduct of this pitfall.

Insufficient Resources

When it comes to cybersecurity, time and the utilization of resources is what companies struggle with the most.

Many SMBs are lean on staff and one person wears all the hats.

It may be work, but failure to patched equipment leaves vulnerabilities in the network that may remain unmitigated for months or years.

Partnering with a Managed Security Provider can address this pitfall.

Frequently Asked Questions

What Should A Cyber Securitystrategy Include?

A cybersecurity strategy should include an objective that aligns with the goals of the business.

Once the objective is clear, various resources of information are needed to build out the strategy to establish the current state of the program.

The current state will identify risks and weaknesses within the organization. The strategy will provide the security controls and recommendations to remediate and reduce risk.

What Is a Cybersecurity Roadmap?

A cybersecurity roadmap is a strategic, risk-based approach plan.

The goal of a plan is to create a guide that includes an assessment of the current state of the program.

Once the current state is identified, the roadmap will include multiple strategic milestones designed to help the business monitor and immediately identify gaps in security controls within the environment.

What Is a Cybersecurity Framework?

The framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

In addition to helping organizations manage and reduce risks, it is designed to encourage risk and cybersecurity management communications to both internal and external organizational stakeholders.

Who Is Responsible For Your Business's Security Strategy?

Any strategy that addresses risk to the business starts at the top of the organization.

Leadership and IT teams do take responsibility for creating and deploying a strategy.

Employees also contribute to the strategy, but ultimately, the responsibility starts at the top of the organization.

How Long Does It Take to Prepare a Cybersecurity Strategy?

The length of time it takes to prepare a cybersecurity strategy can vary from one organization to the next.

There isn't a set time frame that fits all organizations, however, the plan should be treated as a project with milestones based on resources, risk assessment reviews, technology, and other factors related to the project.

How Do You Prepare Your Cybersecurity Strategy?

Preparation of the cybersecurity strategy starts with engaging all relevant stakeholders.

This communication will provide insight on the business goals and requirements to secure.

At this point, a roadmap strategy can be developed utilizing the 8 steps listed earlier in this article.

How Often Should You Evaluate Your Cybersecurity Strategy?

A typical time frame to evaluate a cybersecurity strategy at a minimum is annually.

However, the cybersecurity strategy may be re-evaluated sooner in case there is a security breach, company acquisitions, or change in business model.

How Much Does a Cybersecurity Strategy Cost to Develop & Implement?

The cost of developing and implementing a cybersecurity strategy has many dependencies. One dependency is resource availability.

Expertise will be needed to conduct risk assessments; however, the organization may not have internal resources to conduct the review.

The same principle applies to vulnerability and penetration testing, this level of testing is usually performed by a third-party company specializing in this area.

Organizations can expect to spend between $15,000 – $100,000+ for a cyber security strategy to be developed.

Implementation can range from tens of thousands to hundreds of thousands of dollars over a period of 2-3 years.

How Can Small Businesses Improve Their Cybersecurity?

Smaller businesses may be more prone to cyberattacks as they typically have fewer resources dedicated to cybersecurity.

However, there are a few simple, cost-effective practices to keeping data and devices secure without breaking the bank.

- Educate employees
- Multifactor identification
- Implement strong passwords
- Install Up-to-Date Antivirus Software
- Back up your data regularly

How do you build a cybersecurity strategy for your business?

Building a cybersecurity strategy for your business takes effort, but it could mean the difference between surpassing your competitors and going out of business. Here are the basic steps to follow in developing an effective security strategy.

Step 1. Understand your cyber threat landscape

Before you can understand your cyber threat landscape, you need to examine the types of cyber attacks that your organization faces today. Which types of cyber threats currently affect your organization the most often and most severely: ransomware, other forms of malware, phishing, insider threats or something else? Have your competitors had major incidents recently, and if so, what types of threats caused them?

This article is part of

The ultimate guide to cybersecurity planning for businesses

- Which also includes:
- **Top 8 in-demand cybersecurity jobs for 2024 and beyond**
- **Top 7 enterprise cybersecurity challenges in 2024**
- **How to develop a cybersecurity strategy: Step-by-step guide**

Next, get yourself up to speed with predicted cyber threat trends that could affect your organization. For example, many security researchers feel that ransomware is going to become an even bigger threat as ransomware gangs flourish and expand their attacks. There's also increasing concern about supply chain vulnerabilities caused by, for example, purchasing compromised components and either using them within your organization or building them into products you sell to customers. Understanding what cybersecurity threats you'll face in the future and the likely severity of each of them is key to building an effective cybersecurity strategy.

Step 2. Assess your cybersecurity maturity

Once you know what you're up against, you need to do an honest assessment of your organization's cybersecurity maturity. Select a cybersecurity framework, like the NIST Cybersecurity Framework developed by the National Institute of Standards and Technology. Use it first to assess how mature your organization is in dozens of different categories and subcategories, from policies and governance to security technologies and incident recovery capabilities. This assessment should include all of your technologies, from traditional IT to operational technology, IoT and cyber-physical systems.

Next, use the same cybersecurity framework to determine where your organization should be in the next three to five years in terms of maturity for each of those categories and subcategories. For example, if distributed denial-of-service attacks will be a major threat, you may want your network security capabilities to be particularly mature. If ransomware will be your biggest security issue, ensuring that your backup and recovery capabilities are highly mature may be key. If the remote work policies that were driven by COVID-19 have or

will become permanent at your company, temporary tools deployed during the pandemic need to be hardened. The maturity levels you're targeting are your new strategic objectives.

Step 3. Determine how to improve your cybersecurity program

Now that you've established a baseline and determined where you want to be going forward, you need to figure out the cybersecurity tools and cybersecurity capabilities that will help you reach your destination. In this step, you determine how to improve your cybersecurity program so that you achieve the strategic objectives you've defined. Every improvement will consume resources -- money, staff time, etc. You'll need to think about different options for achieving the objectives and the pros and cons of each option. It may be that you decide to outsource some or all of your security tasks.

Cybersecurity career advice

Looking to further your career in cybersecurity? These four articles provide timely information on how to build the technical and personal skills you'll need to be successful.

Cybersecurity career path: 5-step guide to success

10 cybersecurity certifications to boost your career

10 must-have cybersecurity skills for career success

Top 10 cybersecurity interview questions and answers

When you've selected a set of options, you'll want to present them to upper management at your organization for their review, feedback and -- hopefully -- support. Changing the cybersecurity program may affect how business is done, and executives need to understand that and accept it as being necessary in order to sufficiently safeguard the enterprise from cyber threats. Upper management may also be aware of other plans for the coming years that your efforts could take advantage of.

Step 4. Document your cybersecurity strategy

Once you have management approval, you need to ensure your cybersecurity strategy is documented thoroughly. This includes writing or updating risk assessments, as well as cybersecurity plans, policies, guidelines, procedures and anything else you need to define what's required or recommended in order to achieve the strategic objectives. Making it clear what each person's responsibilities are is key.

Be sure that, as you're writing and updating these documents, you're getting active participation and feedback from the people who will be doing the associated work. You also need to take the time to explain to them why these changes are being made and how

important the changes are so that, hopefully, people will be more accepting and supportive of them.

And don't forget that your cybersecurity strategy also necessitates updating your cybersecurity awareness and training efforts. Everyone in the organization has a role to play in mitigating security issues and improving your enterprise cybersecurity program. As your risk profile changes, so must your cybersecurity culture.

Karen Scarfone

These are the key steps to take in developing a cybersecurity strategy.

Monitor and reassess security threats and strategy

Developing and implementing a cybersecurity strategy is an ongoing process and will present many challenges. It's critically important that you monitor and reassess your organization's cybersecurity maturity periodically to measure the progress you're making -- or not making -- toward your objectives. The sooner you identify an area that's falling behind, the sooner you can address it and catch up. Measuring progress should include internal and external security audits plus tests and exercises that simulate what would happen under different circumstances, like a major ransomware incident.

Finally, be prepared to rethink your cybersecurity strategy if a major new threat arises. Agility in security is increasingly important. Don't be afraid to update your strategy as cyber

threats and security technologies change and as your organization acquires new types of assets that need safeguarding.

https://www.techtarget.com/searchsecurity/tip/How-to-develop-a-cybersecurity-strategy-Step-by-step-guide

How do you develop a strong cybersecurity strategy?

Below are seven key steps that can be used as a basis when building a strong cybersecurity strategy and why it is important to include an Incident Response plan:

Step 1: Perform a security risk assessment

A cybersecurity risk assessment is designed to get a detailed view of the possible cyber threats to your business, and your capabilities to manage the associated risks. The range of threats varies across businesses, so an in-depth risk assessment becomes the first and key step in understanding the gaps and vulnerabilities in your existing policies and procedures. Other than understanding your own risk profile, risk assessments can help in identifying third and fourth-party risks, which is a crucial part of the journey in getting secure.

Apart from understanding overall risk, a security risk assessment can help businesses identify, classify and map their data and information assets on the basis of their value. This allows businesses to prioritise and allocate resources accordingly to ensure the efficiency and effectiveness of cybersecurity measures implemented.

Without a thorough risk assessment in place, your business might not discover where the challenges lie, and what aspects of cybersecurity to prioritise and invest in, to prevent disruption.

Step 2: Define and establish security goals

An important step in building a cybersecurity strategy is to ensure that it is congruent with your larger business goals. The way this can be done is by defining security goals that align with and do not compromise the goals of your business. Creating security goals can be challenging however the process can be simplified if the following questions are asked.

Q1. What is your organisation's maturity level?

Understanding your current cybersecurity capability can help with defining security goals, by reviewing the current security architecture of your business and reviewing security incidents that have occurred in the past, you can gain an understanding of your current maturity level when it comes to cybersecurity. The Australian Cyber Security Centre has a framework called the Essential Eight Maturity Model that helps organisations identify a target maturity level that is suitable for their environment.

Q2. What is your organisation's risk appetite?

Security risk appetite is the expectations from the senior management of a business regarding their security risk tolerance. These criteria help an organisation identify security risks and prepare appropriate treatments and provide a benchmark against which the success of mitigations can be measured. Identifying security risk appetite can help determine how and where cyber security should be prioritised, thus making it easier to arrive at realistic and achievable security goals.

Q3. Are these goals realistic and achievable?

When defining security goals it is important to ensure that the goals are realistic and achievable. When setting goals factors like the following should be taken into consideration; your organisation's resources, the given timeline to achieve a certain level of cybersecurity maturity, the budget available and the skill and expertise available.

Step 3: Assess the level of your technology against Industry best practices

An essential part of developing a cybersecurity strategy is evaluating technology to see if it meets current best practices. With the rapid development of the tactics, techniques and procedures of malicious actors, the technology in an organisation is required to be up to date with the latest patches and security updates. Having technology that is outdated

leaves a business vulnerable to cyber attacks, for example, systems that are no longer receiving updates leave a network open to compromise as attackers find it easy to enter.

Once the technology is upgraded to match industry standards, it is important to ensure that there are resources available and dedicated to maintaining and supporting the technology within the business. For example, during a zero-day attack, it is essential that resources are ready and available to respond to the threat and mitigate any risks that arise.

Step 4: Choosing a cybersecurity framework

A cybersecurity framework is, essentially, a system of standards, guidelines, and best practices to manage risks that arise in the digital world. There are several cybersecurity frameworks a business can choose to help guide its overall cybersecurity strategy. Depending on the type of your business, some frameworks may require mandatory to comply e.g. the PCI DSS framework is essential for merchants that handle and store cardholder data and non-compliance may lead to legal repercussions.

Step 5: Review existing security policies and create new ones

A security policy is a document that states in writing how a company plans to protect its physical and information technology assets. They should be amended to reflect any changes in technology, vulnerabilities and security requirements. Part of this step is to review existing security policies and create new ones that were missing and are now needed. For example, one of the biggest cybersecurity risks is an organisation's own employees, negligent behaviour is a common cause of data breaches. For example, security policies that address appropriate password and privileged identity access management are essential to informing and upholding employees to a high information security standard.

These security policies need to be enforceable and every employee in an organisation needs to be held accountable for information security. Regularly scheduled and mandated security training and awareness programs can help enforce these policies.

Step 6: Risk management

An important part of creating a cybersecurity strategy is preparing for the worst, however strong your cybersecurity measures are, there is still a chance that your business falls prey to a cyber attack or data breach. Identifying the potential risks to your organisation's information security beforehand is a good way to mitigate the repercussions associated with an attack. As part of your risk management plan, the following policies can be implemented to ensure that your organisation is adopting a proactive approach toward their cybersecurity:

- Data privacy policy - outlines how corporate data should be handled and secured properly
- Data protection policy - covers how the sensitive data belonging to customers, employees, suppliers and other third/fourth parties should be handled
- Retention policy - details where data should be stored and for how long
- Incident response plan - outlines in detail the steps that need to be taken in the event of a security incident

Step 7: Implementation & Evaluation

Now that your cybersecurity strategy has been planned out and policies have been created, it is time for implementation. Once the cybersecurity strategy has been implemented by your information security or project management team, it is important to recognise the need for continued support and evaluation. Vulnerabilities will continue to evolve as threat actors discover new methods of attack, therefore your cybersecurity strategy needs to be continuously monitored and tested to make sure it matches the existing threat environment.

As upholding the cybersecurity strategy is the responsibility of the entire organisation it is important that key stakeholders are identified and held accountable for oversight. In addition to this, an annual risk assessment can help identify and fill in any gaps that may grow as threats evolve. Feedback received from both internal and external stakeholders can be a good way of receiving insight on how to best improve an existing cybersecurity strategy.

https://www.stickmancyber.com/cybersecurity-blog/how-to-develop-a-strong-cybersecurity-strategy

Collected by: Mohammad Alkhudari

https://www.linkedin.com/in/alkhudary/

2024