BitLyft
Cybersecurity

CREATING AN ACHIEVABLE SECURITY BUDGET

A GUIDE TO THE COSTS OF CYBERSECURITY

OVERVIEW

The idea that cybercrime is a problem restricted to the financial industry or large conglomerates and Fortune 500 companies is a thing of the past. From manufacturing and utilities to education, healthcare, and small businesses, everyone is a target. Attacks are more frequent and severe, costing businesses more than ever before. According to IBM's Cost of a Data Breach Report, breaches during 2021 resulted in the highest average cost in 17 years. More findings from the report include:

- Compromised credentials caused the most breaches.
- Remote work increased data breach costs.
- Automation and security AI saved companies up to $3.81 million.
- A zero-trust approach reduced costs related to a data breach by up to $1.76 million.

National news regularly features stories of the impact of cyberattacks on all industries. If you think your business is too small to be a target, consider the fact that 43% of cyberattacks target small businesses. Cybersecurity is a crucial component of running any business. So, exactly how much will it cost you

The truth is, there's no set number that will adequately define the cost of cybersecurity. I know that seems like a cringe-worthy statement for a cybersecurity company to make, but it can actually provide certain benefits. Should a small company be forced to shoulder the same costs for cybersecurity as a multi-level corporation bringing in billions each year? Probably not, and the reason is simple. The cybersecurity needs of every business are unique. It's estimated that an organization should spend 7% to 10% of its IT budget on cybersecurity. However, certain factors could mean 15% doesn't provide adequate coverage.

Determining how much you need to spend on cybersecurity will depend on the size of your company, your employees, and exactly what you need your security stack to accomplish. This guide will help you determine the cost of cybersecurity, define what your security stack should accomplish, and find ways to prepare your budget to include cybersecurity costs.

It's estimated that an organization should spend 7% to 10% of its IT budget on cybersecurity.

TABLE OF CONTENTS

DEFINE SPECIFIC CYBERSECURITY GOALS

All companies are different. In the same way your cost for accounting software varies from other businesses in your community, your cybersecurity needs and other elements within your business will help you determine the amount you need to spend on cybersecurity. Before you investigate the specific factors that impact your cybersecurity costs, consider what jobs you want your security stack to accomplish. Your cybersecurity goals might include:

- Protection from direct attacks to your company
- Compliance with regulations such as CMMC, GDPR, HIPAA, etc.
- Additional security to meet third-party requirements (like vendors or other parties you work with)
- The ability to compete for large projects or government contracts
- Protection against weaknesses of third-party vendors

Before you investigate the specific factors that impact your cybersecurity costs, consider what jobs you want your security stack to accomplish.

WHAT FACTORS DETERMINE COSTS?

There is no one size fits all cybersecurity cost. In fact, it's important for companies to consider the types of data they need to protect and the security solutions that are within their unique budget. These are the most common factors most likely to affect your cybersecurity cost.

SIZE OF THE COMPANY

Larger companies house more data than smaller ones. More importantly, they have more employees. Since 95% of cybersecurity breaches are due to human error, and rarely come from the IT department, this is a pretty big deal. Besides cyberattacks that directly target employees, more employees mean more computers, devices, and workstations exist. Bigger companies simply have a larger attack surface than smaller ones.

TYPES OF DATA HANDLED AND STORED

Some types of data are protected by state and federal regulations. For instance, if your company handles or stores government-protected information, you have related cybersecurity requirements to uphold. Similarly, healthcare facilities are subject to HIPAA requirements, and businesses that store credit card information are compliant with the Payment Card Industry Data Security Standard (PCI).

The percentage of all cybersecurity breaches that are related to human error

To take it a step further, the type of sensitive data you store may mean different requirements exist beneath the same bill. The difference in the regulations for federal contract information (FCI) and controlled unclassified information (CUI) under the five levels of compliance for CMMC is a perfect illustration of this.

PRODUCTS AND SERVICES USED FOR CYBERSECURITY

The products and services you use will play a big part in how much you spend on your cybersecurity solution. Any effective cybersecurity solution combines the efforts of trained and experienced cybersecurity experts and highly specialized software. For companies with an in-house cybersecurity team, additional investments may only include the cost of software. Conversely, if you're starting from scratch, a bigger investment will be required. This could mean hiring additional employees or employing the services of a third-party security operations center. With these options, the cost difference between self or professional installation may still be a factor.

PROFESSIONAL AUDITS

Besides providing the security benefits of direct protection from cybersecurity attacks, your cybersecurity stack can be utilized to meet your compliance requirements. This may mean scheduling additional audits to prepare for annual compliance checks. Additionally, your cybersecurity provider may be able to help outline a plan to get your company ready to comply with upcoming regulations.

ADDED SERVICES

As the threat of cyberattacks continues to grow for every industry, regulations are being adopted to help protect businesses, government organizations, and citizens. Companies preparing for new certification may need additional services from a cybersecurity provider like readiness assessments and remediation plans.

THE ELEMENTS OF YOUR CYBERSECURITY SOLUTION

A truly effective security solution combines sophisticated tools and a human element. The right tools can speed up the search process and sift through large amounts of information in short periods of time. Cybersecurity professionals operate these tools and use intuition and growing knowledge to recognize and intercept threatening behavior. Cybersecurity requires a layered approach that is tailored to your needs and budget. Your cybersecurity solution may include the following elements.

CYBERSECURITY PRODUCTS

- Firewall
- Endpoint Security and Antivirus
- Endpoint Detection and Response
- Antivirus Software
- Email Protection
- Two Factor Authentication

CYBERSECURITY PROFESSIONALS

- Security Analysts
- Security Engineer
- SOC Manager
- CISO

CYBERSECURITY SERVICES

- Vulnerability Assessment
- Penetration Testing
- Compliance Auditing
- Security Program Development
- Security Architecture Review
- Monitoring Services

TYPES OF SECURITY OPERATIONS CENTERS

The headquarters that houses your security professionals and tools is called a security operations center (SOC). The type of SOC your company uses will have one of the biggest impacts on your cost for cybersecurity. The primary reason for this is that your SOC type dictates whether the cybersecurity professionals who take care of your company's security needs are employed by your company or by a third party.

IN-HOUSE SOC

A fully-staffed SOC located on the premises of your business property is referred to as in-house. For companies with an existing cybersecurity team, this is an opportunity to save money. However, if you don't already have cybersecurity experts on the payroll, adding the yearly salary of these experts into your cost will require a big investment.

- **Analyst: $53K - $116K**
- **Engineer: $73K - $130K**
- **Director: $105K - $198K**
- **CISO: $176K - $263K**
- **CIO: $100K - $263K**

Most companies need as many as 4 analysts and engineers, making the average cost for yearly cybersecurity staff salary $739,000 - $1,708,000. Unfortunately, these numbers don't include the cost of 24/7 monitoring and employee benefits.

With consistent rises in cybercrime and an ongoing talent shortage in this critical field, cybersecurity experts are difficult to find and carry a skill set that is absolutely necessary given the modern threat landscape. However, most companies lack the financial status to make these essential professionals part of their workforce. Outsourced SOC is becoming a popular solution.

OUTSOURCED SOC

Cybersecurity services from a third-party vendor are usually provided as-a-service. SOC as a service (SOCaaS) is typically the more affordable choice for small to medium businesses. SOCaaS provides companies with many of the same benefits as an in-house SOC. The up-front investment is minimal, and monthly payments cover the cost of ongoing service. Since your service provider already employs trained professionals, you can start with options that meet your current needs and scale your security solutions with your business growth.

THE COST OF A BREACH

You can't really discuss the costs of cybersecurity without including some information about the cost of inaction. In 2020, the average cost of a breach was $3.86 million, and the average time to discover a breach was 207 days. The impact is worse for smaller businesses because they're not large enough to absorb the costs as well. The overall cost of a breach is rarely felt right away. Instead, the expenses can be spread out over a year or longer. Some of the costs associated with a breach include:

DIRECT COSTS

- Monetary theft (86% of breaches were financially motivated in 2020.)
- Remediation and system repair
- Regulatory and compliance fines
- Legal and public relations fees
- Increased insurance premiums
- Costs of notifying affected parties, identity theft repair, and credit monitoring

INDIRECT COSTS

- Business disruption and downtime
- Lost customers
- Loss of intellectual property
- Damage to company credibility and reputation

CREATE AN ACHIEVABLE CYBERSECURITY BUDGET

There's no doubt that cybersecurity is an essential business expense for any business operating in today's advanced threat landscape. Unless you're operating a business completely off the grid, falling victim to a cyberattack is a when instead of if situation. When you consider the average cost of a breach results in losses that total over $3 million, even the cost of starting an in-house SOC from scratch would be cheaper. Still, noting the cost of a breach doesn't mean the average business has the funds to take care of the fall-out. Creating a cybersecurity budget doesn't mean you must afford the same security stack as Fortune 500 financial institutions. It means you should include the preventative security measures you need to protect the data within your organization. To form your ideal budget, look at these considerations.

YOUR COMPANY'S CURRENT POSITION

Where your company and employees currently stand in the fight against cybercrime will have a big impact on your upcoming security budget. Answer these questions to see where you stand.

- Does your organization have existing employees dedicated to cybersecurity? This could help you save on future investments.
- How security-conscious are your employees? Every employee within your company should understand and practice basic cybersecurity hygiene. If this isn't the case at your organization, additional training should be added to your budget.
- Are you facing new security hurdles in the near future? Assessing gaps, remediation plans, and certification costs will raise your cybersecurity costs.
- Is remote work a part of your organization? Remote work increased drastically during the pandemic and will remain at least partially present for many companies. Your security budget should reflect the additional risks these devices bring to the attack surface of your network.

OVERALL IT BUDGET

Cybersecurity is typically considered an IT cost. The total amount you spend on IT services can provide an accurate reflection of the cost of cybersecurity in relation to the size and the technological specifications of your business. Are you already spending the recommended 7% to 10% of your IT budget on cybersecurity? Are you satisfied with the results?

If your current budget isn't meeting your current risks, it's time to assess why. Your company may need to adjust spending to reflect new cybersecurity risks or explore different cybersecurity options for added protection.

COMPLIANCE REGULATIONS

While compliance with industry regulations doesn't necessarily equal adequate cybersecurity protection, it does factor into your security needs.

Regulations like GDPR, GBLA, HIPAA, NIST 171, and CMMC outline certain cybersecurity requirements you need to follow by law. Failing to add compliance costs into your budget can lead to expensive fines on top of other expenses associated with a cyber attack.

INDUSTRY-SPECIFIC CYBERSECURITY AVERAGES

For many companies with minimal cybersecurity measures in place, it can be difficult to determine exactly what risks exist and how much spending is required to defend against them. This is where industry-specific data can be helpful. Information that provides insight into what your competitors are spending can help you align your budget to industry risks. In the event that spending data isn't available, seek information about security costs specific to your industry

ORGANIZATIONAL NEEDS

While your industry norms can help you outline an average price range, your organization might have specific factors that should be addressed. For instance, if you need to invest in new hardware, this would be an added expense that isn't a part of typical cybersecurity spending. Other costs to consider include:

- Regulatory costs and certifications
- Employee turnover if you employ your own security professionals
- Protection for IoT devices
- Remote devices

ANTICIPATED ROI

While it's impossible to predict the future of cybercrime and your future cybersecurity needs, it's important to have a firm understanding of why you're spending the amount you settle on. Your cybersecurity goals help separate your spending needs from those of different organizations and industries. Factoring in historic data of your company and industry can help you address how much your cybersecurity spend will save over the cost of a breach. To avoid overspending on features you don't really need, identify where spending will result in diminished returns.

HOW CAN YOU CUT COSTS ON CYBERSECURITY?

No matter what type of security operations center you choose or how much you invest in the tools used in your cybersecurity stack, the actions that take place within your organization are a crucial part of your defense. While taking a proactive stance against cybercrime takes some effort and training, it can also help you avoid inflating your security budget with added costs. Implementing these practices can help you reduce cybersecurity costs and better protect your company.

REVIEW POLICIES REGARDING INTERNET AND DATA ACCESS

Your organization should have a policy in place that dictates which employees have access to sensitive data and procedures for all company-owned devices with internet access. If these policies don't exist, create some and set a date for annual review. Include a list of products, software, and employee devices on company property. Access to sensitive data should only be awarded to employees whose routine tasks require such access.

EDUCATE EMPLOYEES

Your security system is only as effective as its weakest link. If your employees are unaware of the potential risks and how to avoid them, you're setting them up to be weak links. If employees within the company unknowingly respond to phishing, malware, or other breaches, they render your firewall and other cybersecurity efforts useless because the attack is essentially coming from inside the organization. Whether you invest in professional training or the time to complete company training your investment will be rewarded. At a minimum, employee cybersecurity awareness training should include:

- Password strength and usage
- Links in attachments and emails
- Unverified requests for data or information
- How to use cybersecurity filters and tools at their disposal
- Actions to take during a potential security event

ASSIGN RESPONSIBILITIES

Even if you outsource your cybersecurity, you'll still need responsible employees within your company to make vital security decisions and create and enforce procedures. You'll need to assign a decision-maker to create and enforce company cybersecurity policies. Define all staff members' cybersecurity policies and note that this might vary due to the accessibility of sensitive data for different roles. Additionally, specific employees should be assigned to react in the event of a breach.

DESIGN AN EXIT STRATEGY

Not all employees leaving your company will be leaving on good terms. It's important to remember that these employees have access to information critical to your organization. Your device policy should include a log for all employees who own or lease company property. Similarly, sensitive passwords may need to be changed after employees are discharged.

PRACTICE DEFENSIVE BEHAVIOR

Integrating defensive behavior into every aspect of daily tasks helps basic cybersecurity hygiene become second nature for everyone within your organization. These are the behaviors that many individuals understand but resist because of time commitment or extra effort. Alongside the enforcement of other cybersecurity policies, encourage these behaviors.

ENABLE AUTOMATIC UPDATES

Device operating systems, endpoints, and servers should all be equipped with the ability to automatically update when new versions become available. Make sure these updates are enabled for all devices, including those for remote work and IoT devices.

ENFORCE STRICT PASSWORD POLICIES

Ensure that employees use complex, unique passwords for all devices and permissions. Never duplicate passwords for multiple uses, and ensure proper shut-down practices always require passwords for re-entry. Weak password policies make it easier for threat actors to move laterally within your network.

CREATE A SENSE OF RESPONSIBILITY

Most employees think it's not their job to take care of cybersecurity. If they haven't been educated otherwise, they're right. Create a company culture that prioritizes everyone's role in cybersecurity. Share the potential risks of poor behavior and how those risks can ripple throughout the organization and to individual employees.

ENABLE ACCESS MANAGEMENT CONTROLS

Employees within your company should only have access to the data they need to properly do their job. Creating levels of privilege within your access management controls can halt cyberattacks when a threat actor gains access from a lower-level employee or an individual server.

Stretching your business budget is never easy. It becomes even more difficult when navigating the complex territory of cybersecurity. Yet, there's no denying that the cost of a breach will quickly surpass that of your cybersecurity solution. Determining your company's unique costs of cybersecurity can be a confusing process, but taking the time to learn more can help you make informed decisions about your company's future. The consequences of a cyberattack can result in enormous direct costs and irreparable damage to your brand and company.

If you're unsure about the level of security you need for your organization, it's a good idea to consult a professional. Cybersecurity experts can examine your specific needs and help you assess your current cybersecurity posture. Don't wait around to pick up the pieces after disaster strikes. Talk to the cybersecurity experts at BitLyft to learn more about complete protection for your network with a platform that merges the best people and software to provide unparalleled protection for you.

HERE TO HELP

When you're looking to protect an entire organization on a limited budget you can have trouble prioritizing spending. The one certainty is that you need people. Whether you're an established company, or just getting started, BitLyft has a solution to help you protect your organization from cyber attacks. Our team of cybersecurity professionals can fully augment, or come along your existing team to help you illuminate and eliminate cyber threats.

Schedule a meeting with our BitLyft Success Team today to get started.

"In over a decade of helping businesses decide to build their own SOC or outsource to a SOCaaS provider, I have seen time and time again a much better ROI to subscribe to the right vendor than to build internally. Everyone's environment is different and the use cases can vary. However, there's never a bad reason to take a moment to review your current state and future needs with experts like those at BitLyft."

SECURONIX™

MIKE JOHNSON
CHANNEL SALES DIRECTOR
SECURONIX, INC.