proofpoint.

E-BOOK

Metrics That Matter:

The CISO's Guide to Assessing, Prioritizing and Justifying Cybersecurity Budgets That Make Business Sense

SECTION 1

From scapegoat to strategist

To understand just how much the role of the CISO has evolved in recent the years, consider the account of one executive at a recent Proofpoint roundtable.

"When I started in the industry, the role of the CISO tended to be the role of a scapegoat," he recalled. Executive leadership needed someone to blame if things went wrong. But often, they prioritized umbrella insurance policies over investments in security teams and solutions. In other words, he said, CISOs were technologists with limited resources.

But the tide is turning. Threats have grown more complex and can affect more than just a few limited systems within a business. And when cyber attacks grow into full-scale data breaches, they can quickly tarnish or destroy a brand.

This has changed the way that executive leadership views investments in cybersecurity—and the role of the CISO. Boards are paying a lot more attention to what CISOs are doing. And, reflecting the "chief" in their title, CISOs are deeply involved in the overall business strategy. More and more, they help to shape digital transformation in a way that manages risk, optimizes business processes and reduces avoidable losses.

> "When I started in the industry, the role of the CISO tended to be the role of a scapegoat."

Growing challenges bring new costs

With this evolution come new budgetary needs. According to a recent Forrester study, 60% of senior enterprise security decision makers increased their security budgets in 2020.[1]

And those who aren't spending more are trying to stretch their funds further. Today's cybersecurity budgets must contend with:

- Evolving regulations and requirements
- A continuing shift to the cloud
- An overnight shift to remote and hybrid work models
- An evolving threat landscape

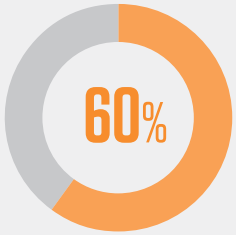
Preparing for the future

As CISOs adapt to these changes, many expect budgets to continue increasing (by 11% on average) to meet the challenges ahead. Nearly two-thirds (65%) think they will be better positioned to resist and recover from cyber attacks by 2023.[2]

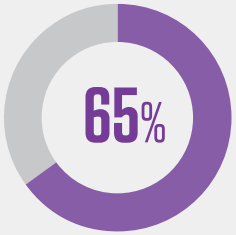
Nevertheless, preparedness is still a major concern. Although leaders express optimism about their ability to resist and recover in the future, they feel less confident in their position today. In our 2021 Voice of the CISO Report, 66% of CISOs reported feeling that their organization is currently unprepared to cope with a targeted cyber attack.[3]

People, not network technologies, are the new perimeter. And the move to hybrid work (from mostly or fully remote) only adds to security challenges and complexity.

As a security leader, you can direct your budget to cope with these changes. This e-book will give you best practices for assessing risk, establishing your company's risk tolerance, assessing your current solution, prioritizing spend and justifying your budget to the board.



of senior enterprise security decision makers increased their security budgets in 2020



of CISOs think they will be better positioned to resist and recover from cyber attacks by 2023

expected increase in budgets to meet the challenges ahead

1 Forrester. "Global Security Budgets in 2021." August 2021.
2 Proofpoint. "Voice of the CISO." May 2021.
3 Proofpoint. "Voice of the CISO." May 2021.

SECTION 2

Assessing risk tolerance

First, assess your risk exposure and establish your risk tolerance using a framework that makes sense for your business. There are many frameworks available. As you seek consensus on these topics with executives and board members, be sure to communicate which framework you're using and why.

Boiling it down to the numbers

Quantifying risk is not a perfect science, and it can get complicated. Yet taking the time to quantify risks and your risk tolerance will help you justify your budget later. You can also analyze risk in qualitative terms, but dollars-and-cents metrics will resonate with executives and board members.

And level-setting is critical. The risk tolerance that business leaders express during planning may not always match up with their actual risk tolerance. Consider mapping out realistic scenarios with executives and board members to ensure you arrive at your company's true risk appetite.

Major Cybersecurity Frameworks

National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

NIST, a division of the United States Department of Commerce, provides guidance on managing cybersecurity risk and improving internal and external cybersecurity communications.

NISTIR 8286: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management

This document focuses on addressing cybersecurity risk at the enterprise level within the context of the business mission and goals.

People-Centric Security Framework (PCSF)

Developed using a transparent, consensus-based process, including both private and public stakeholders, Proofpoint published this framework to enable better people-risk practices and help organizations protect confidentiality, integrity and availability of their environments.

SECTION 3

Mitigating risks

Once you pinpoint your risk exposure and your risk tolerance, you must evaluate your current protections against those risks.

Thinking beyond technologies

You may be tempted to think about this through the lens of your existing technology stack. Everyone is familiar with operational key performance indicators (KPIs), such as time to detect, time to respond and time to remediate.

These KPIs are useful for lower-level reporting and for understanding day-to-day performance of specific solutions that you have in place. But they are not as useful for evaluating and communicating your overall position against higher-level risks and business priorities.

Threat modeling

As you plan a budget and report upward, consider using a threat modeling approach to assess your organization's key risk indicators (KRIs) and your performance against them. Threat modeling is a process for identifying threats and how they occur, and then prioritizing mitigation measures accordingly. In contrast to solution-specific KPIs, threat modeling helps you see the bigger-picture risks to your organization and identify any gaps in your protection.

Threat modeling will help you identify what you are doing well, where you need more investment, and where you may be willing to accept residual risk. You can assess a variety of risks in this way. Here are just a few to consider.

Threat-modeling in practice

Here's an example of how threat modeling works in practice. Consider regulatory risk. One scenario that can lead to regulatory risk is data leakage. And data leakage can occur through a variety of threat vectors, such as:

- Email data loss
- Cloud-based transfer
- Saving data to a local disk
- Using removable media
- Transferring data to an insecure zone
- Using an external file sharing site
- Manual cut and paste
- Application vulnerabilities

As you lay out each of these vectors for data leakage, you can assess your level of protection and decide how to tackle gaps.

If you jump straight to assessing performance of specific technologies, such as a cloud access security broker (CASB), endpoint agent or virtual private network (VPN), you may overlook gaps in coverage for data leakage vectors that these products don't cover.

By using a threat modeling approach to assess your KRIs, you can draw a more comprehensive and strategic picture of your company's preparedness for various risks.

SECTION 4

Selecting solutions

Using your risk tolerance and your KRI analysis, you can identify the key areas of new investment for your business.

As you consider specific solutions to meet those needs, consider the following questions:

- Does it mitigate a risk?
- Does it solve a business problem?
- Does it help improve the business? (Enable new tools or processes)
- Does it help us simplify and streamline our security operations?
- Does it align with our business goals and risk tolerance?

You can and should ask the same for existing solutions. Before continuing to invest in a particular technology, be sure it still provides value.

Quantify the ROI

To justify your investments—and the budget needed to support them—to the board, quantify the return of each solution.

It's not always easy to quantify the return on security investment (ROSI) of solutions, but it can make getting buy-in from leadership much smoother. You can do this by weighing the benefits of the solution against its cost.

Be sure to investigate the hidden costs of a solution, such as:

Hardware

Implementation

Software

Ongoing Management

For each solution, compare the cost to the benefits, which may include risk reduction and workforce efficiency. You'll also want to outline the option of doing nothing by detailing potential exposure and providing some examples.

For example, if you were to choose not to mitigate the impact of ransomware or malware, the potential costs could include:

- Business disruption
- End-user productivity loss
- Time spent investigating threats and creating reports
- Time spent responding to or remediating a threat
- Time performing tasks manually, such as removing messages from a mailbox or responding to reported phishing messages

Document what's left over

Also be sure to identify your cyber insurance and your residual risk, which is the exposure that remains after your investments. It is nearly impossible to get your business to zero risk, and, if you could, it probably would not be worth the cost. But you should ensure that your residual risk falls within your organization's risk tolerance.

SECTION 5

Calculating and communicating budget requirements

Once you have determined your budget needs and areas of investment, you must communicate those needs and investments persuasively to executives and board members. You will likely have several different audiences, including:

- The board
- Operational leaders, such as the chief operating officer (COO) or chief information officer (CIO)
- Financial leaders, such as the chief financial officer (CFO)

Tailoring your message

It makes sense to tailor the business case for your security investments to each audience. Focus on the impact to the areas of the business that they oversee. Think of it like saying the same thing in three different languages:

- **The board.** As you address the board, emphasize how your plan meets the company's risk tolerance. And identify the residual risk the business will accept.
- **Operational leaders.** As you talk to the COO or CIO, operationalize your message. Focus on gaps, remaining vulnerabilities and how your plan will offset risks to business operations.
- **Financial leaders.** With the CFO, highlight how you've balanced the spend or how you plan to fix any unbalanced areas.

With all your audiences, communicate the ROI of solutions that you quantified during your planning phase. Help them understand what the organization gets for the money you spend.

Tapering ROI

Be prepared to explain the concept of "tapering ROI." You may have to spend the same amount on the big, obvious issues as you do on smaller, less obvious issues that are just as critical. A seemingly "small" threat can expose the business to a large risk, such as a data breach, justifying significant spending to offset it. Here you can refer again to your ROI calculations to put the cost of the solution in context with the risk it mitigates.

SECTION 6

Dealing with out-of-cycle needs

Your budgeting process happens annually or quarterly. Inevitably, issues will arise outside of the standard cycle, such as emerging threats or new threat actor tactics. Unexpected incidents are virtually impossible to avoid, but they can provide an opportunity to reassess your security posture and rethink your spending priorities.

Consider hidden costs

And don't forget to consider all the costs associated with each solution you implement. Most companies budget for licensing. But many forget to factor in the cost of maintenance or people resources needed for the solution. As you plan, consider those "hidden costs" to avoid getting blindsided out of cycle.

SECTION 7

Accelerating the process

Budgeting can easily turn into a cumbersome and slow process. But there are ways to accelerate and smooth out the process.

Think strategically

First, embrace your role as a strategic business partner and remember that the role of CISO is evolving. Determine what people are trying to achieve and help them get there with minimal risk.

Think beyond operations and technical leadership and consider how you can help the organization drive digital transformation and achieve business goals.

Balance risk and productivity

Remember also that you cannot eliminate risk altogether. As a security professional, you may prefer a conservative risk tolerance, but the board and other executives will want to balance risk exposure against business goals. For example, your email gateway efficacy may be 99.1%. But it takes just one email to result in ransomware, which leaves .9% residual risk. This residual risk is usually addressed by adding layered security such as isolation or data loss prevention (DLP). But all parties should have an understanding that zero risk is not possible.

Find common ground and try to avoid becoming the “Department of No.” Your budget and plans should balance risk against the company’s priorities and minimize exposure within the company’s risk tolerance.

Set the right expectations

Finally, temper expectations along the way. Most departments within a business operate on a production model, where output and higher returns are key performance indicators. Cybersecurity operates on a resilience model.

Just as firefighters get paid whether there’s a fire or not, cybersecurity requires a budget that doesn’t always translate to higher returns. No one would argue that firefighters are unnecessary. It is your role to help your business partners understand cybersecurity in the same way.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0500-000-01-01 03/22