Guide

How to Sell the C-Suite on Greater Cybersecurity Investment

QOHASH

Good tech helps with the urgent business of cybersecurity, but good tech isn't enough for securing the funding for cybersecurity investment.

If it is a truism that cybersecurity never delivers full protection, it is equally true that corporate investment in cybersecurity never matches the actual need. Yes, 91 percent of companies have increased cybersecurity budgets in 2021, according to IDG research. But IDG also found that new cybersecurity hiring is flat, and many long-range security projects have been sidelined recently. Security professionals are having to do more with less.

Unless you sell executives on greater cybersecurity investment, that is.

Getting additional funding for cybersecurity initiatives is tricky. Defensive spending for the intangible benefit of enhanced security is always a hard sell, even in the age of digital transformation. But it isn't impossible. Getting the green light and additional funding for cybersecurity initiatives just requires a solid plan and executive buy-in. This guide shows you how.

Getting Executive Buy-In

The biggest reason that many security professionals fail at getting funding is because they don't approach the problem in the right way. When seeking greater cybersecurity investment, you don't want to think like a security professional. You want to think like a business leader.

Getting additional funding is essentially a sales activity. You're selling the C-suite on the need for a new technology, a new approach, or more resources. This requires understanding how your target thinks and looks at the world, and using language and motivation they understand and will respond positively to.

The problem is that many cybersecurity professionals approach the topic as if they were selling to another cybersecurity professional. The need for greater security is viewed as self-evident, the discussion is technical, and the language is precise but doesn't resonate with upper management.

So the first step toward winning more cybersecurity investment is changing how you think.

Link Cybersecurity to Corporate Goals

The impulse when selling cybersecurity initiatives often is the FUD approach, because obviously the cost of inaction is high with cybersecurity. While this might be an internal narrative within the cybersecurity community, it doesn't usually encourage security investment when talking with leadership. Management will pretty quickly tune out doom and gloom if it is not pressing.

A better approach is tying cybersecurity to business goals, as noted by Gartner research. Organizational objectives and ROI is the native language in the executive suite, so winning cybersecurity investment often comes down to the ability to connect the dots between security and business strategy.

Sometimes this can be as simple as repositioning something like "strengthening financial data security" to "enabling the business to build trust in financial products through enhanced data security." Sometimes it requires a little more.

Three areas to focus on include the connection between security and building trusted products and services, the role of better security in creating positive customer experiences, and the ways that security can drive financial goals instead of simply being a cost center.

Focus on Risk Mitigation Instead of Technology

A common mistake is focusing on the technical side of cybersecurity initiatives when pitching to company executives. Yes, cybersecurity is usually about technical solutions. But non-technical management doesn't understand the nuances of technical solutions, they understand business risk. Focusing on the technology also takes the conversation into the weeds instead of stressing the overall goal of minimizing risk through better cybersecurity.

When pitching a cybersecurity initiative, therefore, take a risk-based approach where the proposal is about offering solutions that mitigate overall risk. Lay out several options based on levels of risk mitigation, and let executives walk themselves toward the solution you champion through their decision to reduce company risk exposure in the best way possible.

Lean on Stats and Success Metrics

Abstract or technical threats that have not yet occurred are a hard sell, especially when coupled with an inability to measure the tangible business impact of a cybersecurity initiative. Selling cybersecurity investment requires concrete ideas that non-technical executives can grab onto, and metrics that will show the overall success of a project. Again, this is about positioning cybersecurity in a way that business leaders understand.

Statistics, ideally graphically represented, go a long way toward making the case because they are bite-sized, visual, and facts-based. Business leaders might not get the nuances of a technical what-if scenario, but a chart that shows the percentage of firms that leak sensitive data and the cost savings of avoiding a breach sure demonstrates the need for a given cybersecurity solution.

Similarly, proposals for cybersecurity initiatives that tangibly demonstrate progress and outcomes fit more closely with what executives like to see, and they make project greenlighting easier. The use of key risk indicators, security program maturity metrics and tangible goals make proposals more defined and measurable, which leads to greater understanding and approval.

Ride on the Back of Other Corporate Projects

Sometimes security analysts cannot get the ear of key corporate decision-makers, or improving security takes a back seat to business-driving initiatives that focus more naturally on company growth. Worthy cybersecurity proposals can get tabled or lost in this environment.

One of the most effective tricks for getting added cybersecurity investment is attaching a security component to another corporate project that already has widespread support among leadership. In this way, a cybersecurity initiative can boost its business case and gain additional exposure by riding along with a project that already has the ear of company executives.

Building security investment proposals around hot-button issues also drives added attention and interest from leadership. If there's a business trend or pressing issue that a security solution can help solve, the chance of approval goes way up.

Find a Corporate Sponsor for Better Politics

Cybersecurity is about technology, but investment in cybersecurity is politics. Often security professionals come in with a solid proposal that makes sound technical and financial sense only to lose the political game of human relationships.

That's why a critical aspect of getting buy-in for cybersecurity investment is getting support from others within the organization. A business champion outside the IT department goes a long way toward winning the political game of corporate investment, serving both as an indicator that the proposal has wider impact, and assisting with making the case for the investment.

Part of building support for cybersecurity investment also includes nurturing relationships and trust with senior executives both before and during new initiative proposals. When there is respect and a clear channel of communication between the security team and upper management, proposals have a greater chance of winning the political game and capturing support.

AUTOMATED CYBERSECURITY TECHNOLOGY

With more robust data management and security automation, institutions can speed up threat detection and protect against compliance violations, improve incident response, increase compliance visibility, and help standardize compliance processes.

Download the guide, How to Automate Financial Institution Data Compliance, which outlines the processes that should be automated, defines the steps for implementing data compliance automation, and suggests six best practices for a smoother compliance automation rollout.

Preparing Your Pitch

Second only to thinking like a business executive, the success or failure of your proposal will usually come down to preparation. After switching from a cybersecurity mindset to a business perspective, next it is time to craft your actual pitch.

There are six steps you'll want to follow as you get ready for pitching your proposal. These six steps will not ensure success, but they will give you the greatest chance for securing additional corporate funding.

Step 1: Research Your Audience and the State of the Business

Cybersecurity proposals are fundamentally about sales, as noted above; additional security funding comes from selling a vision to senior executives. So just like the sales team, the first step in securing additional cybersecurity funding is the due diligence of learning the interests and focus of the decision-maker—in this case, senior management. Every good sales pitch is tailored to a specific audience.

This means not only having a good understanding of what senior management wants, but also what the business needs. What are the current pain points within the business overall, what new products, markets or special projects are taking place? Where could additional cybersecurity investment advance company priorities and assist with company goals?

Know your target.

Step 2: Map Security Risks to KPIs and Business Goals

Most businesses have a wide range of key risk indicators and other security metrics. These are useful for the security team, but they have less direct value to the executives who will greenlight additional cybersecurity funding. As a result, map security metrics to overall KPIs and business goals so the connection between security and business objectives is clear for your non-technical audience.

Look to map all security outcomes back to overall business outcomes to reinforce the business case for additional security investment. Pay particular attention to the connection between security metrics and new company initiatives, as well as areas that have been identified as particularly important to those in the C-suite.

Step 3: Conduct a Security Assessment and Prepare Your Plan

The plan itself is of course the foundation of your proposal, so once you have a solid grasp of the needs of your audience and how security metrics translate into business outcomes, assess the specific cyber risks and both the possible and recommended solutions for addressing those risks. Include specific technologies and budgets, but always make sure they are tied to how they impact overall business goals.

Some components that might be of specific interest to executives include:

- Risk management. How additional funding will specifically reduce company risk, and by how much.
- Compliance management. How the proposal will strengthen compliance mandates and minimize the chance of regulatory violation around privacy and data security.
- Accountability by role. Who is responsible for each part of the security proposal in terms of both implementation and ongoing support.
- Costs. The specific costs for each part of the plan, why they are necessary, and how they impact the intended business outcomes.

Step 4: Develop an Elevator Pitch and Overall Narrative

Almost as important as plan specifics is an easy-to-understand narrative that quickly communicates the overall vision of the cybersecurity proposal. This narrative should be simple, easy to understand, relatively non-technical, and align with overall business goals. The plan contains the specifics, but the narrative is the simple idea that executives will remember and largely use to judge the relevance of the proposal.

Part of building this narrative is crafting an elevator pitch, a simple summary of the plan in a few short sentences. This elevator pitch serves as a short version of the overall plan, a clarifying agent for keeping the proposal focused, and a concise pitch that you can give verbally to prepare executives for the written proposal if the right opportunity presents itself.

Step 5: Gather Stats and Create Visuals

The story of why greater cybersecurity investment is needed must be simple, easy to grasp, and facts-based. Statistics and metrics that tell the story and show both the problem and the solution are critical for getting additional investment, so look for data that backs up every part of the plan.

Turn particularly key data into simple graphs and visual representations that further paint the obviousness of the proposed security investment. In preparing these visuals, challenge yourself to see if the graphs and visuals can communicate the essence of the proposal even without the written portion.

One excellent book for going deep on visual representation design is Edward Tufte's classic work, The Visual Display of Quantitative Information.

Step 6: Prepare a List of Objections to Overcome

Most likely there will be some pushback to the proposal, even if the objections are just testing the soundness of the plan.

No good salesman goes into a presentation without a clear sense of the objections that might be raised and how these objections will be addressed. So once the proposal is complete, go over it several times with an eye toward the issues and questions that could come up during the presentation.

Give substantial time to this part of the preparation, because it could be the difference between success and failure. Have several colleagues review the proposal prior to presentation with an eye toward possible objections, both readers who deeply understand cybersecurity and those who are more general in their understanding.

Later in this guide we list six common objections and how to overcome them. Make sure you prepare for overcoming all six, in addition to the objections you uncover during your preparation.

How to Overcome Objections: A Framework

Since overcoming objections is a foundational skill that is useful in almost all areas of life, there are numerous frameworks for how to overcome objections successfully. One of the most widely used frameworks goes by many names but basically revolves around five time-tested steps for getting to yes. Security professionals selling additional cybersecurity investment should internalize these steps before walking into a proposal meeting.

Actively Listen

Executives will have initial questions and concerns after hearing your security proposal. Pay close attention to what these executives say using active listening skills, because these comments and concerns provide the basis for overcoming the objections that lead to the sale.

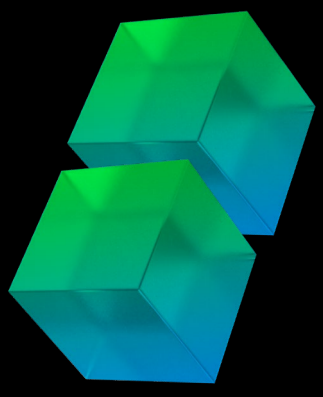
Specifically, make sure you truly understand what is said and don't interrupt or try to immediately answer the concerns until they have been fully voiced.

Repeat Back What You Hear

After an executive has voiced concerns and objections, verbally summarize what they just said so you get confirmation that you understand it correctly.

This is a communications checksum, basically, and it makes your audience feel heard and understood. That's important for trust, which improves your chance of overcoming the objections. It also helps ensure you understand what objections must be overcome.

Qohash finds, tracks, and safeguards the world's most sensitive data.



Validate Their Concerns and Show the Way Out

Show executives that you not only understand the concern, but their perspective is legitimate. Validating an objection does not reinforce its conclusions, it simply acknowledges the problem and further helps your audience trust that you're on the same team regarding the problem.

Once you acknowledge the concern, you then connect the dots between the problem and your solution.

If you're proposing automated data discovery technology, for instance, you might say something like, "I understand that implementing comprehensive data automation sounds complex and costly, but there actually are affordable turnkey vendor solutions for this task. So this isn't nearly as big or expensive as you would think."

Ask Follow-Up Questions

It is important to make the process a dialogue and not about divergent sides talking over each other. So keep the conversation interactive after validation by asking open-ended follow-up questions that lead the executive toward your solution.

By asking followup questions, you create the space for uncovering micro-objections to your solution and slowly working toward "yes" together.

Show Social Proof

Depending on the objection and your level of preparation, a final step in the process is highlighting the validity of your answers by marshalling data or examples that show that the objection can, in fact, be overcome. This could be a case study from another organization that had the same challenge, or statistics that prove your point.

Social proof in conjunction with an actual solution that overcomes the objections almost always seals the deal.

Common Cybersecurity Objections to Overcome

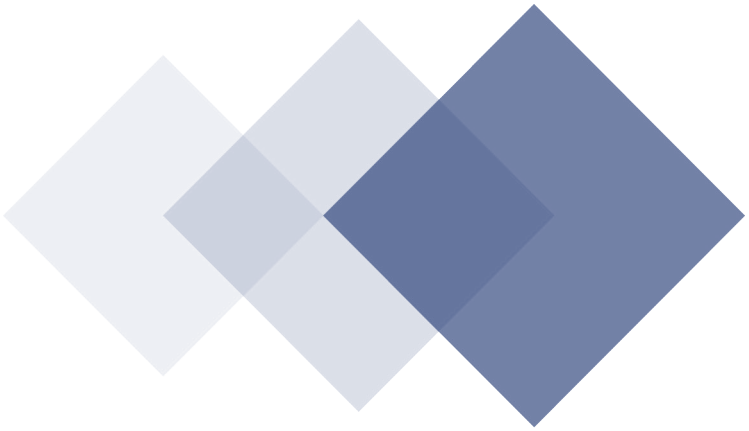
While the above framework can see you through virtually any objection you might encounter during your cybersecurity investment proposal, it helps to also come in prepared for some of the most common objections. By preparing for common objections, you can better formulate responses and gather the data needed for social proof.

Here are six of the most common objections you might encounter, and suggestions for how to overcome them.

Objection: "We don't have the budget for this."

How to respond:

- I understand that there are competing priorities for resources within the company. This should be at the top of the list, however, because…
- This proposal addresses key data compliance challenges that ultimately will save the company far more than the cost of investment. Here's the risk probability and how this solution will significantly reduce that risk…
- Let's do a thought experiment and budget for the cost of the likely cybersecurity breach that will occur if we do not find the budget for this initiative. This isn't eating budget, it is saving budget.



Objection: “Haven’t we already invested in this?”

How to respond:

- We did increase the cybersecurity budget last year, and let me show you how it benefited us. That said, cybersecurity is an ongoing expense, which is why I’m coming to you now with this proposal.

- Our organization took big steps last year toward cybersecurity preparedness, but it actually has been four years since we made a comprehensive investment. This proposal is part of the ongoing upgrade of our security position.

- Cybersecurity threats are constantly evolving, and our response must evolve with it. This is part of that needed evolution.

Objection: “This isn’t a pressing need, and there is a better use of resources.”

How to respond:

- We don’t actually know if we’re secure right now, so it might be more pressing than you realize. This proposal helps us uncover risk and deal with it.

- Just because we have been lucky in avoiding a data breach, that doesn’t mean it isn’t going to happen. We’re actually more likely to encounter a breach now because we’ve been lucky thus far.

- The cost of responding to a cybersecurity breach far outweighs the resources we will invest now. This small use of resources prevents a much larger use of resources after a breach.

Objection: “We’re focused on growth right now, so what’s the ROI?”

How to respond:

- The business disruption from a successful cyberattack will significantly harm the organization’s growth plans. This is not an ancillary project, it is a component of our growth plans.

- This proposal significantly reduces cybersecurity and compliance risk, so it is fuzzy but with clear ROI. If we look at the cost of failure, the ROI from this initiative is massive.

- We can get a clear picture of ROI by conducting a wargame to test our current state of cybersecurity preparedness and the cost of not implementing this proposal.

Objection: “Are there less expensive or ‘good enough’ solutions to this problem?”

How to respond:

- We’ve already applied this methodology and ruled out more expensive solutions. This is the “good enough” solution, and here are the other options we ruled out and why.

- I hear you. Let’s start with the objectives that must be achieved, and work backwards to see if there are less expensive options that still make sense.

- We cannot go with a lesser solution and still meet the needs, but we could implement it in bite-sized phases to spread out costs over time.

Objection: “I don’t understand the need for this.”

How to respond:

- This can be a technical topic, although the need is real. Let me try and explain this in a different way.
- Perhaps we need a special meeting so I can explain the need and the solution in more detail. When would be a good time for us to meet so I can show you why this is a pressing concern?
- Because there’s a clear need, can you help me understand why you feel this is an unnecessary project?

You’ve Got This!

Asking for more funding isn’t easy.

The good news is that cybersecurity is a pressing concern for many businesses today; roughly 90 percent of organizations report feeling vulnerable to data breaches, according to a recent study by Crowd Research Partners. The bad news is that gaining the necessary corporate resources is not a given, and getting there requires you to swap your technical chops for sales savvy.

Just as you learn new technologies on an ongoing basis as part of your job, however, you also can learn how to sell your next cybersecurity proposal. It just takes a different mindset, and a little preparation.

Make all your sensitive data secure

Identifying and classifying data is not instant. But at the same time, it is easier than many businesses realize. All it takes is awareness of a company's data landscape, a little structured planning, and the right automation technology in place. With a little work and the right data classification system, even businesses with small cybersecurity departments can ensure that sensitive data remains safe.

Qohash is a leader in data discovery and classification security software. It blends innovative and easy to understand security technologies, allowing businesses to gain visibility on sensitive data. Founded in 2018 with solutions available in the U.S. and Canada, Qohash provides customers with solutions tailored to meet today's hybrid and remote work environments in the financial services sector.

To learn more about Qohash products, schedule a demo.
Write us at info@qohash.com

© How to Sell the C-Suite on Greater Cybersecurity Investment