SolCyber

# How to Persuade Your Executive Team to Prioritize Security

SolCyber

According to a survey conducted by Forbes, business owners and executives rank cyberattacks as one of the top risks their businesses face today. And yet, a similar survey of CEOs and small business owners showed that only half feel they are ready to handle a cyberattack.

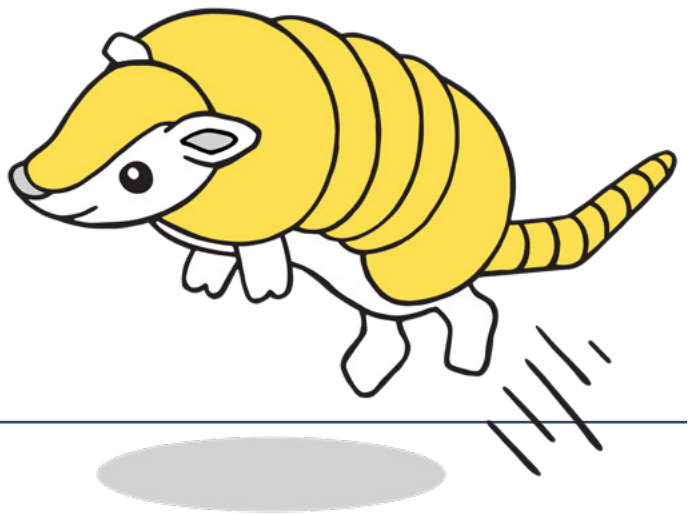
As a security advocate, you're no doubt familiar with the gaps in your company's security posture, and might even feel frustrated at the lack of forward momentum in implementing your security strategy. You know that most attackers prey on human error, so securing endpoints or installing email protection software, while important, won't stop someone in your organization from clicking on a malicious link or choosing to skip their MFA setup.

A strong security posture requires an effective tech stack and a concerted effort from every employee in your organization to remain safe. Despite your best efforts, teams will only be swayed if the messaging comes from the top.

But how can you convince your C-suite to implement the security technology you're recommending and enlist their help to build a culture that values security?

*You need to speak their language.*

This guide will help you deliver your message in a way that resonates with each member of the C-suite, so you can persuade them to up the ante when it comes to security.



# The CEO

When charged with developing a business strategy, sharing their vision, and keeping the board, partners, investors, and employees happy, your CEO has a pretty full plate. But cybersecurity affects nearly every aspect of a CEO's role, and a breach could put a real damper on their future plans. Investor and customer trust is at risk. Worse, the headaches that often come with data breaches can not only slow an organization down but virtually bring it to a halt. To secure company and customer data — and prevent a reputation-shattering breach — CEOs need to make cybersecurity a priority.

## Top priorities and concerns

- Corporate strategy and alignment
- Growth and scalability
- Finding and cultivating talent
- Fundraising
- Keeping external stakeholders happy
- Economy and inflation
- Regulatory changes

## How cybersecurity affects CEOs

60% of SMEs go out of business within six months of being hacked.

A weak security posture can scare off investors or get in the way of an acquisition.

A data breach can destroy relationships with business partners.

A security breach puts a CEO in defense mode and slows down a company's momentum for months or even years.

More than half of employees say they would consider jumping ship if their company experienced a cybersecurity incident.

As company leaders, the buck stops with the CEOs. A breach could lead to their termination and would almost certainly be a hit to their professional reputation.

## How to frame the conversation

**Make it personal:** Focus on how a data breach could affect the CEO. As the leaders of their companies, they're going to take the biggest hit in the case of a breach. Make sure they understand why cybersecurity should matter to them personally and specifically.

**Emphasize their role in the process:** Many attacks rely on social engineering, so securing the organization requires effort from each employee, but they'll only make security a priority if the directive comes from the top. Help your CEO understand that building a security culture within the company relies on leadership buy-in.

**Communicate the value of immediate action:** CEOs often move fast and focus on opportunities for growth. Acknowledge the CEO's need for speed but explain why cybersecurity can't be put on the back burner. The longer a company waits to implement security best practices, the more its cyber debt grows and the more vulnerable it becomes.

**Present solutions:** CEOs have a lot on their plates and don't want to be burdened with more problems, so bring solutions for the risks you present. Also, highlight areas for growth to make it easier for your CEO to say yes to your requests.

**Highlight the real risks:** No one wants to be the gray cloud on a sunny day, but CEOs need to understand the real dangers of a weak security strategy. Explain that it's not a question of if a breach will occur, but when. Arm yourself with as much data as possible about the risks your company is facing, the strategies attackers are using, and what your competitors are doing to protect themselves.

# The CFO

The CFO has always been part of the cybersecurity decision-making process. But as concerns around security grow, and because those concerns are affecting more aspects of the CFO's job, CFOs are becoming more involved than ever before. Because breaches can be so costly, security should be woven into every department. It's essential that CFOs make educated decisions around security.

## Top priorities and concerns

- Cutting operational costs
- Growing profit margins
- Enabling growth
- Securing funding
- Budgeting and forecasting

## How cybersecurity affects CFOs

In 2021, data breaches cost companies an average of $4.24 million, and that number is expected to rise. Final costs of a data breach include the investigation, remediation, legal fees and settlements, fines, lost business, and even reputational damage.

The larger your organization becomes, the harder and more expensive it is to address security concerns if an appropriate defense isn't put in place on day one.

CFOs are responsible for making their company look appealing to investors. But an investor won't want to work with a company that's taken on a lot of cyber risk, whether it's due to a poor internal defense system or because your company is working with third-party vendors that aren't secure.

Finance teams are prime targets for cyberattacks. According to a Deloitte survey, 34.5% of participants claimed their accounting and financial data was targeted by cyber adversaries in 2022.

## How to frame the conversation

**Speak their language:** CFOs look at things through an opportunity cost lens, so make sure you're crafting an argument with that in mind. How much will your security efforts cost? What's the risk cost (in dollars) if your plan isn't implemented? What are the real dollar costs of a security breach?

**Show the long-term savings:** At first glance, security technology, vendors, and cyber insurance look like significant costs. But these should be seen as investments that will save your company in the long run. By securing your company's data, you reduce cyber debt, the risk of a breach, and your overall attack surface. It will also set you up to scale your operation and attract potential investors.

**Be honest:** Many CFOs are focused on minimizing risk, so make sure they understand that security threats and your defense strategy will change over time and will minimize risk, not necessarily eliminate it. Anticipate that they will want to cut your proposed budget, and be honest about what partial coverage means for your organization.

# The CRO

A relatively new role, CROs are vital to the success of an organization. They're pulling segmented departments together to boost revenue. They focus on people, processes, and technology — all of which play a big role in your organization's security posture. One poorly configured application or a process that doesn't include security and your entire business is disrupted. It's important that your CRO understands what a breach looks like for his or her team and that it will likely end the business and customer relationships they've worked so hard to establish and maintain.

## Top priorities and concerns

- Growing revenue
- Organizational alignment
- Improving the customer experience
- Implementing technology that breaks down silos
- Managing and growing internal and external relationships

## How cybersecurity affects CROs

A data breach could drive customers away. Roughly 62% of Americans claim they would stop buying from a brand for several months following an attack.

It's estimated that lost business represents the largest share of breach costs, averaging $1.59M or 38% of the total costs.

Better security practices can help you win customers. In fact, 41% of business leaders say that closing deals depends on maintaining security and 57% are asked by prospective customers to prove their security measures.

A weak security posture could keep potential business partners at bay because they don't want to absorb the risks your security gaps present.

## How to frame the conversation

**Align your goals:** The CRO wants more deals to come through, faster. You want to secure the organization. Show them how security and risk management is a way to reduce friction in the sales process, allowing them to close deals faster.

**Communicate how security benefits them:** By ensuring processes are secure, you're actually making the CRO's job easier. As they invest in technology and rework processes that break down silos, you're reducing risk that can jeopardize their initiatives.

**Think of the customer:** Today's customers have high expectations when it comes to protecting their data. Show your CRO that a comprehensive security strategy gives your company a competitive advantage.

**Mention the three Ps (Process, Policies, and Procedures):** Throughout your conversation, make sure to mention that a strong defense system keeps employees around longer, makes processes more sustainable (because they won't be disrupted down the line when teams need to chip away at cyber debt), and ensures that technology purchases are implemented well.

# The CTO

As people rely on more applications and devices to do their job, an organization's attack surface grows. Company and customer data is moving through dozens or even hundreds of devices — some more secure than others — especially with a portion of the workforce working from home. So as your team builds products, integrates third-party applications, and updates servers and operating systems, security needs to be considered at every step in the process. Although CTOs are typically responsible for security, they don't often have the security expertise needed to ensure it happens.

## Top priorities and concerns

- Develop a technology strategy and vision
- Create a better customer experience
- Data security and governance
- Remove friction and focus on agility
- Integrate emerging technologies into the business

## How cybersecurity affects CTOs

At the end of the day, CTOs are responsible for security. If a breach or security incident occurs, their job might be at stake.

Customer privacy is more important than ever with 84% of consumers saying they want more control over how their data is being used. And CTOs are ultimately responsible for securing your product — and your customers' data.

CTOs are typically expected to make the final decision on security and software purchases. Failure to choose a secure application or software (or failure to secure it once implemented) could result in massive costs.

Taking a hodge-podge approach to security leads to significant cyber debt. Devices, products, and applications eventually need to be secured. Waiting only increases the time, resources, and dollars needed to make those repairs.

## How to frame the conversation

**Present the long-term benefits:** Your CTO might view security as a hassle or even a bottleneck, but investing in security early actually saves money and effort down the line. As your company grows, so does your cyber debt, making an early investment a cost-effective choice.

**Highlight the risks of not investing:** Security is all about minimizing risk. Communicate the risks of not implementing a strong security strategy. Highlight the costs of a breach as well as the costs of compliance or misconfiguration issues caused by a failure to implement the proper security protocols.

**Relate risk to the role:** As the individuals responsible for securing the organization, their job is on the line if a breach occurs. Considering that 50% of small and mid-sized businesses reported suffering at least one cyberattack in 2022, security is worth the investment!

**Build a smart budget:** Reassure your CTO that while security is a necessary expense, you don't need to spend the entire department's budget. Emphasize that there are smart ways to achieve cyber resilience on a lean budget.

**Approach it as a team effort:** You know security and can whip up a sound strategy with clear action items. But you need the CTO to help build a culture that values security. To get buy-in on your plan across the organization, ask the CTO to be your megaphone.

# BECOME CYBER RESILIENT WITH SOLCYBER

To convince your C-suite that security should be a top priority, you need to determine what they care about, tie that to security, and highlight the real dangers of a weak security infrastructure. Help them see that security incidents can not only affect a company for months or even years and have real reputational, legal, and business costs, they can put that company out of business.

Most importantly, explain that becoming cyber resilient doesn't require massive effort or an exorbitant budget. SolCyber helps SMEs secure their organization fast and arms them with a comprehensive security program, delivered as a service. With our Foundational Coverage, you'll get support from a dedicated team of security experts who can implement all the technology and tools you need, and get you up and running in days. This results in fewer decisions for your C-suite and assurance that all your bases are covered.

Reach out to learn more about SolCyber's Foundational Coverage or to set up an exploratory call.