TESSIAN

Prove the Value of Cybersecurity Solutions: 16 Tips From Security Leaders

As a security or IT leader, researching and vetting security solutions is step one. What's step two, then? Convincing key stakeholders like the CEO, CFO, and the board that the product needs to be implemented, that it needs to be implemented *now*, and that it's worth the cost. This is easier said than done.

We talked to security leaders from the world's most trusted in innovate institutions to find out how they get buy–in from the c–suite. These are their tips.

01

Familiarize yourself with overall business objectives

TOP TIP

Start by reviewing annual reports and strategic roadmaps. Build your case by attaching cybersecurity initiatives to key business objectives.

While cybersecurity has historically been a siloed department, today, it's an absolutely *essential* function that supports and enables the overall business. Think about the consequences of a data breach beyond lost data. Organizations experience higher rates of customer churn, reputations are damaged, and, with regulatory fines and the cost of investigation and remediation, there can be significant revenue loss.

The key, then, is to attach cybersecurity initiatives to key business objectives. The security leaders we interviewed recommended starting by reviewing annual reports and strategic roadmaps. Then, build your business case.

If customer retention and growth are KPIs for the year, insist that cybersecurity builds customer trust and is a competitive differentiator. If the organization is looking for higher profits, make it clear how much a breach would impact the company's bottom line. (According to IBM's latest Cost of a Data Breach, the average cost of a data breach is $3.86 million.)

Create specific "what–if" scenarios

02

A lot of security solutions are bought reactively (after an incident occurs), but security leaders need to take a proactive approach. The problem is, it's more challenging for CxOs and the board to see the value of a solution when they haven't yet experienced any consequences without it.

As the saying goes, "If it ain't broke, don't fix it".

That's why security leaders have to preempt push–back to proactive pitches by outlining what the consequences would be if a solution *isn't* implemented so that stakeholders can understand both probability and impact.

For example, if you're trying to get buy–in for an outbound email security solution, focus on the "what–ifs" associated with sending misdirected emails which – by the way– are sent 800 times a year in organizations with 1,000 employees. Ask executives to imagine a situation in which their biggest clients' most sensitive data lands in the wrong inbox. What would happen?

Make sure you identify clear, probable consequences. That way, the situation seems possible (if not likely) instead of being an exaggerated "worst–case scenario".

What would happen if your biggest clients' most sensitive data landed in the wrong inbox?

03

Work closely with the security vendor

You know your business. Security vendors know their product. If you combine each of your expertise – and really lean on each other – you'll have a much better chance of making a compelling case for a particular solution.

Ask the vendor for specific resources (if they don't exist, ask them to create them!), ask for product training, ask if you can speak with an existing customer. Whatever you need to get buy-in, ask for it. Rest assured, they'll be happy to help.

04

Collaborate and align with other departments

It takes a village and cybersecurity is a "people problem". That means you should reach out to colleagues in different departments for advice and other input. Talk to the folks from Risk and Compliance, Legal, HR, Operations, and Finance early on.

Get their opinion on the product's value. Find out how it might be able to help them with *their* goals and initiatives. In doing so, you might even be able to pool money from other budgets. Win-win!

Ø5

Consider how much executives really know about security

To communicate effectively, you have to speak the same language. And, we don't just mean English versus French. We mean *really* getting on the same level as whomever you're in conversation with.

But, to do that, you have to first know how much your audience actually knows about the topic you're discussing.

For example, if you look into your CEO's background and find out that he or she studied computer science, you'll be able to get away with some technical jargon. But, if their background is limited to business studies, you'll want to keep it simple.

Avoid security–specific acronyms and – whatever you do – don't bury the point underneath complex explanations of processes.

In short: Don't succumb to the Curse of Knowledge.

What is the Curse of Knowledge?

It's a cognitive bias that causes one person to incorrectly assume that other people have the same background and/or information as they do.

Use analogies to put costs into perspective

06

One of the best ways to avoid the Curse of Knowledge and give abstract ideas a bit more context is to use analogies. It could be the ROI of a product or the potential cost of a breach. Either way, analogies can make big, somewhat meaningless numbers more tangible and impactful.

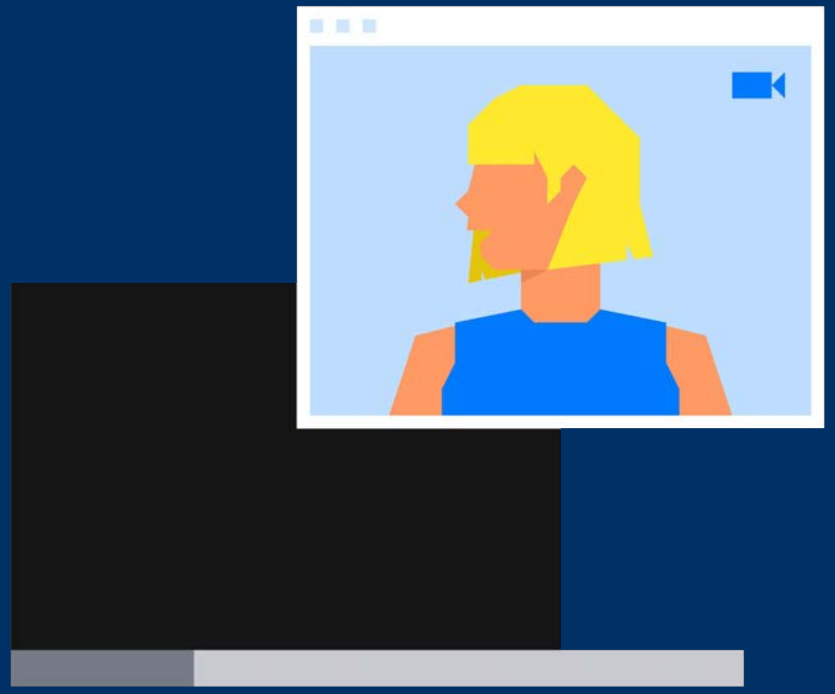
For example, imagine you're trying to convince your CFO that the cost of a solution is worth it. But, the 6-digit, one-time cost is a hard sell.

What do you do? Break the overall cost down by the product's lifespan. Then, divide that number by the number of employees it will protect during that same period.

Suddenly, the cost will seem more manageable and worth the investment.

(Cost of Product ÷ Product Lifespan) ÷ Nº Employees Protected

07



We’ve put together this list of 20 cybersecurity and business events perfect for inviting your non–technical colleagues to.

Invite key stakeholders to events or webinars

Before you even start pitching a particular solution, warm–up executives with educational webinars or events that aren’t product–specific. This will give CxOs a chance to better understand the problem, how it might apply to them, and how other people/organizations are finding solutions.

Bear in mind: most vendors will have at least 1 (generally 2+) webinars or events during the standard sales cycle. Looking for events to attend?

We’ve put together this list of 20 cybersecurity and business events perfect for inviting your non–technical colleagues to.

Do you want to find all the value of Tessian’s flagship event in one place? Become a Human Layer Security member and get instant access to sessions led by cybersecurity leaders at AWS, Salesforce, The FBI, Unilever, & many more. And it’s 100% free.

08

Prepare concise and personalized briefing materials

Individual stakeholders will be more likely to consider a particular solution if the problem it solves is *directly* relevant to them. How?

COMBINE TIPS:

1 Familiarize yourself with overall business objectives

2 Create specific "what-if" scenarios

3 Work closely with the security vendor

5 Consider how much executives really know about security

After taking some time to understand the business' overall objectives, take a closer look at individual peoples' roles and responsibilities in meeting those objectives. Then, dig a bit deeper into how much they know about cybersecurity.

Imagine you're meeting with a COO with some technical experience whose focus is on maintaining relationships with customers. Their briefing documents should contain minimal technical jargon and should focus on how a data breach affects customer churn.

The bottom line: make it about *them.*

09

Collaborate and align with other departments

While this may seem obvious, the security leaders we spoke to made it clear that this is an essential step in getting buy-in. No one wants to feel caught off guard, unprepared, or rushed.

To avoid all of the above, make sure you share any documents relevant to the solution well in advance of any formal meetings.

Build a strong security culture

Before we dive into why building a strong security culture can help you get buy–in, we want to make it clear that this isn't something that can happen overnight. This is a long–term goal that requires the help of the entire organization.

Yes, **everyone**.

So, how do you build a strong security culture? Start by ensuring that security and IT teams are committed to helping – not blaming – employees. There has to be a certain level of mutual trust and respect.

Beyond that, employees have to accept responsibility for the overall security of the organization.

They have to understand that their actions – whether it's clicking on a phishing email or using a weak password – have consequences.

If they *do* accept this responsibility, and if they genuinely care about following policies and procedures and helping secure data and networks, high–level executives will care, too. They'll therefore be more likely to sign–off on solutions.

10

Looking for tips on how to build a strong security culture?

CHECK OUT THESE ARTICLES:

Cybersecurity Awareness Should Be People–Centric, Too

Research Shows Employees Are Less Likely To Follow Safe Data Practices At Home

How to Adapt: 7 Tips from Upwork's Former CEO

11

Keep an eye on security trends outside of your industry

Some industries – specifically Healthcare, Financial Services, and Legal – are bound to compliance standards that formalize the need for effective security solutions. That means that, compared to other industries like Retail or Manufacturing, they'll be required to have more robust strategies in place. What they're doing now, the rest of us will be doing in 12 months. Keep this in mind.

If you notice that organizations operating in the most highly regulated industries are all taking data loss prevention (DLP) seriously, you'll be able to make a strong case that this is something that should be on your radar, too.

12

Approach non-executive stakeholders early on

While – yes – getting buy-in from CxOs and the board is important, security leaders also need to get buy-in from non-executive stakeholders working in IT, infrastructure, etc. After all, those are the people who will actually be responsible for deploying the solution and maintaining it. By approaching them early on (and assuming they're interested in the solution, too) you'll be able to paint a clear picture of the process *after* the solution has been signed off on.

How long will it take? Who's involved? Will employees' workflow be disrupted? These are all important questions to answer.

13

Match like-for-like people from both sides

If you're scheduling a meeting with executives from your side and key people from the vendor's side, make sure you're bringing in people that "match" in terms of function and seniority level.

For example, if you work at a start-up and the founder of your company wants to be involved in the buying process, ask the vendor's founders to join, too. Likewise, if the Head of Infrastructure is joining from your side, ask someone in a similar function to join from the other side. Why? Like-for-like people will be best placed to answer one another's questions. And, with that in mind...

14

Be considerate of people's busy schedules

Decisions about security solutions can involve a lot of different people. That means you'll have to balance several conflicting schedules and fight for time.

Your best bet? Book meetings with *all* relevant people at once and get the vendor involved at the same time. Ahead of the meeting, share an agenda along with any relevant documents (see tip 8).

15

Preempt questions and prepare answers

No one likes to be put on the spot. To avoid being asked a question that you don't know the answer to, spend a good amount of time considering *all* the questions different stakeholders may ask and drafting well-thought-out answers. (Better yet, fit the answers into briefing documents or the presentation itself!)

Remember, people are generally concerned with how a problem/solution affects them directly. That means the CEO will have different questions than the CFO, who will have different questions than the Head of IT.

16

Get *specific* customer references from the vendor

EVERCORE

HILL DICKINSON

Man Group plc

arm

rightmove

COASTAL Housing Group

laya healthcare

gubra

webb henderson Legal and Regulatory Advisors

NORTH SERVICE, STRENGTH, QUALITY

大成 DENTONS

Polarcus

We mentioned in tip 3 that you should lean on the vendor, especially when it comes to specific resources and customer references. And, we mentioned in tip 11 that you should match like-for-like people in meetings.

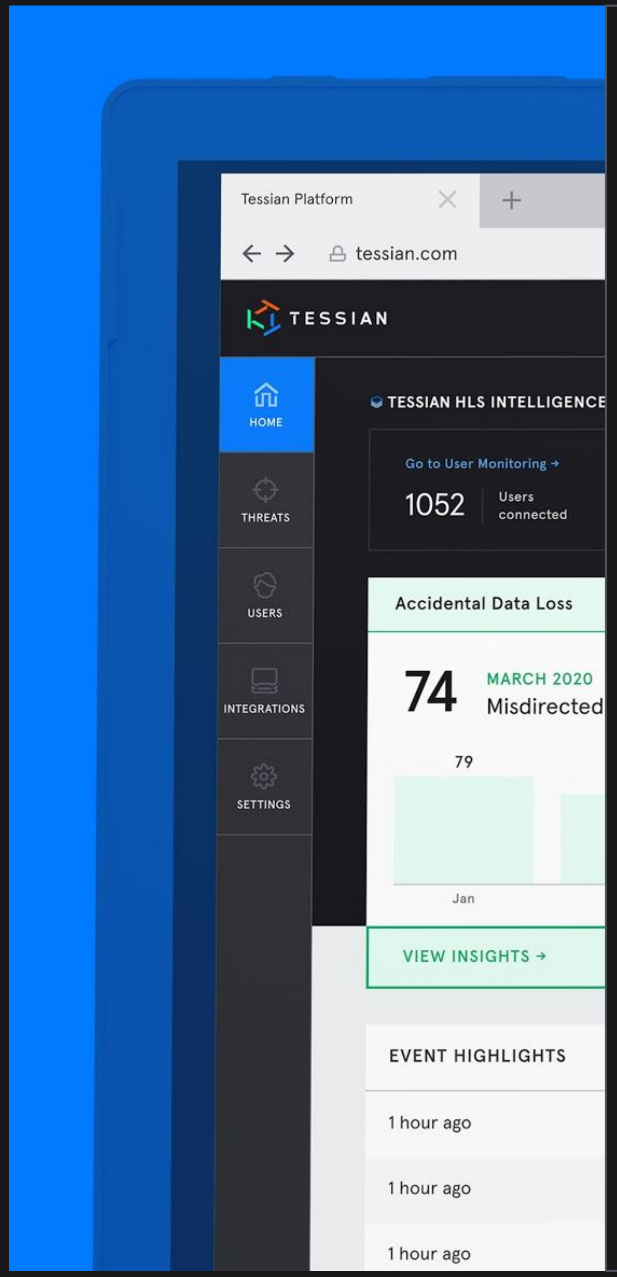
It should make sense, then, that specific customer references will be more powerful than generic ones. For example, if you're the CISO at a 4,000-person tech firm in North America, and you're trying to convince you're CTO that you need to implement a new solution, you should share a case study (or customer reference) from the vendor that outlines how their product has helped an organization in the same industry, that's the same size, and in the same region. Ideally, it will also feature quotes from the CTO.

Why? Professionals trust and rely on their peers when making difficult decisions.

TESSIAN

Tessian builds technology to empower people to work safely, without security getting in their way. We believe people shouldn't have to be security experts to do their jobs. Tessian's Human Layer Security platform automatically protects your employees on email - where they spend 40% of their time - from risks like data exfiltration, accidental data loss and phishing.

TESSIAN.COM



The best way to get any further information is to speak to a real person. Anything from the content in this guide, and the pains you are feeling, to how you can effectively secure your email environment from inbound and outbound threats; we are here to help.

TALK TO AN EXPERT →

How to Communicate Cybersecurity ROI to Your CEO

3 tips to help you demonstrate the business value of cybersecurity solutions and get buy–in from your CEO.

LEARN MORE →

How are We Securing the World's Leading Businesses?

Don't take it from us. Hear it from them. View our case studies from the FS, Legal,Tech industries & more.

LEARN MORE →

TESSIAN

TESSIAN.COM/BLOG →

Share this report