ONTIC | SEC SECURITY EXECUTIVE COUNCIL

How to Prove the Value of Corporate Security

Earn the Recognition and Support Your Teams Deserve

Table of Contents

Why Are Businesses Still Expecting to Miss Threats if Security Is So Important?

No successful business leader would argue against the importance of corporate security today. Having protocols in place for keeping employees safe and property secure is crucial — especially as physical threat activity continues to grow in frequency and severity.

Unfortunately, when business leaders discuss the function of security, it's often in the context of a cost center — like insurance or facilities maintenance. It's something executives know they need to invest in, but, ultimately, don't expect to generate a return. This line of thinking makes it challenging for security leaders to earn executive approval for advanced initiatives. Because, to claim a seat at the decision-making table, gain influence, and win the budget necessary to scale your efforts, you have to demonstrate clear ROI and connection to your company's mission.

> The truth is, corporate security does yield financial benefits. But shifting the way executive leadership thinks about security as a "net contributor" is a tall order and demonstrating it does more than the traditional mantra of "guns, guards, and gates" takes effort.

Fortunately, it is possible. We've witnessed security leaders alter how their organization regards corporate security, finally earning their efforts the attention and resources they deserve.

In this guide, we will cover how to qualitatively and quantitatively demonstrate the value of your corporate security program, based on our experience working with security professionals and insight and advice from the Security Executive Council (SEC). After finishing this resource, you will have the knowledge to craft a compelling case for unlocking budgets, claim your seat at the table, and get the support you need amid our rapidly expanding threat landscape.

Evaluating the Effectiveness of Your Program

Before you can begin putting together a persuasive case for senior decision makers, you need to get clear on the current effectiveness of your corporate security program.

According to the SEC, you should be able to say "yes" to these three questions:

1. **Does management believe the program is adding value?**

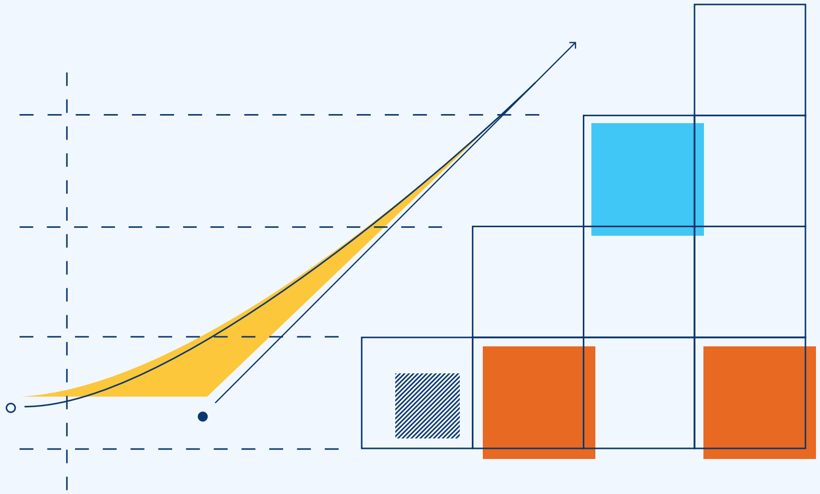
   If senior executives don't believe in the power and purpose of your security program, it could become irrelevant.

2. **Does the program have the influence to help eliminate risky business practices?**

   If senior executives don't believe in the power and purpose of your security program, it could become irrelevant.

3. **Do employees and management accept shared responsibility for people and asset protection?**

   If the workforce believes the security team is solely responsible for protecting the organization from threats, you're not effectively communicating program operations. Your team should provide the tools and first response, but managers are the custodians of the assets, and the entire organization should support those efforts.



If you cannot confidently respond “yes” to all three of the questions on the previous page, you have work to do. But you’re not alone.

If your program is perceived as ineffective, senior leaders may reduce your budget without considering its potential risk to the organization. Additionally, you may be unable to fix or eliminate vulnerabilities, and your organization might experience significant downtime due to security issues. You may also find that employees frequently bypass security safeguards because it’s not a foundational part of the culture.

Luckily, it’s possible to course correct and boost your security effectiveness — and it all starts with earning the confidence of your leadership team and bringing security into the company’s culture. But, to do this, you have to understand who you need to engage with and what they value.

Additionally, Security teams must start speaking to stakeholders in a language they can understand (i.e., talk finance to finance, HR support to HR). Finance understands controls enable both compliance and net profitability, while HR looks to enhance engagement and lower voluntary turnover through proven health, safety and security practices. Both drive bonus-ability and bottom line. This approach will help demonstrate to other business lines that your team is part of the company’s ecosystem — a trusted partner in the enterprise and not just the “break glass” in an emergency group.

Understanding Your Internal Audience

Knowing your customers is critical to earning their attention and fostering a sense of trust. The better you understand their needs and motivators, the easier it will be to tailor your communication, approach, and solutions to keep them engaged.

According to the SEC, there are three things you can focus on to understand internal customers better and earn their buy-in:

1. Personas
   Read Now →
2. Customer Satisfaction Surveys
   Read Now →
3. Interviews
   Read Now →

Personas

Personas are research-based prototypes developed to represent individuals within a demographic — including their challenges, needs, and motivations. These highly realistic yet fictional characters can help you understand how a person might feel about a product or service offering.

Example internal stakeholder personas might include an HR leader responsible for talent strategy and headcount planning, a business unit director charged with improving production, and a chief legal officer concerned with liability and reputation.

There are two strategies you can use to build your personas:

1. Observations from day-to-day interactions, such as meetings and conversations.

2. Surveys or interviews where you ask questions about goals and objectives to gauge how people feel about the existing security program.

It helps to give your personas names and photos to help you visualize real people when building out your strategies. Then determine how you can align needs. For example, a CLO would be especially concerned to learn that security issues are creating vulnerabilities and jeopardizing business continuity — particularly when an unmitigated security vulnerability creates a compliance shortfall or a duty of care lapse.

Customer Satisfaction Survey

A satisfaction survey can help you better understand the effectiveness and value of your program by determining how people perceive security within your organization, as well as what's working and what's not. This will help you glean insight into how you can better engage end-users.

For example, you might discover that onsite employees are frustrated by an unreliable keycard entry system, so they think nothing of holding the door open for others entering the building.

When compiling your survey, be sure to consider the following:

Select simple but specific questions:

"Please rate your confidence in the visitor badging system on a scale of 1 to 10."

Make questions relevant to each audience:

"As an HR leader, how satisfied are you with the visitor check-in process for candidates visiting the building?"

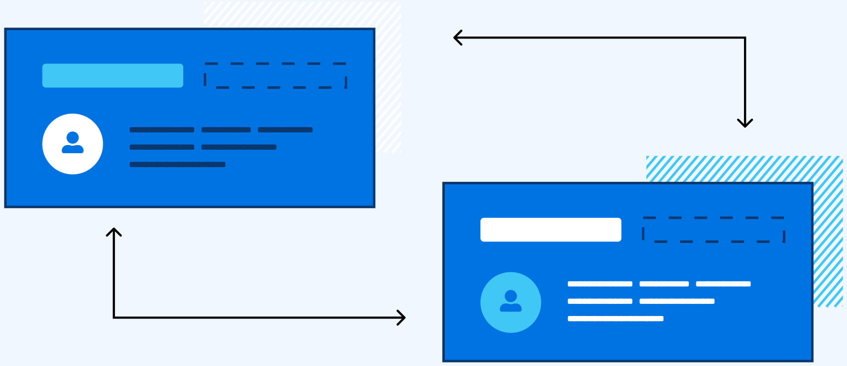
Include a few open-ended questions to allow comments:

"If you could change anything about the organization's on-site security, what would it be?"

Don't provide too many answer options.

Interviews

Candid conversations can be helpful, but having more formal interviews with a standardized set of questions is better — especially when speaking with senior stakeholders. This will help you explore their understanding of your program, existing securityrelated concerns and perceived ownership of security processes.



Here are a few things you can do to ensure your interviews are a success:

- **Create a base set of questions and tailor them to each audience or role**
- **Follow your line of questioning and leave room for outside comments and follow-up questions**
- **Consider having someone outside the security team conduct the interview (to ensure interviewees are forthcoming)**
- **Retain a professional security research and advisory group that can help you**

Making the Case

Once you've identified your audiences, their pain points, and a few shared objectives, the next step is to educate the organization on how strengthening the corporate security program and building a culture of care with improved health, safety and security oversight will benefit everyone. You'll also need to prove its value with real numbers.
Here's how:

Outline Corporate Security's Lesser-Knowns
Take time to acknowledge and cover all of security's many benefits — beyond typical expectations. Here are a few advantages, per the SEC:

- Corporate security actively supports enterprise risk management strategy and helps the business meet its risk management agenda. Security can help shore up dangerous and costly vulnerabilities that, unmitigated, can come back to haunt the organization.
- Security does not own the risk; the business owns the risk. It is security's role to identify risks, give the business various risk mitigation options, then enable the business to decide its risk appetite.
- Security knows the importance of working as a team with other functions.
- Security partners with internal and external stakeholders after an incident to determine what lessons can be learned that can be applied to the next crisis. They advise what tools and resources they need to properly plan, prepare and manage the next crisis.
- Security can meet the needs of the organization regarding emerging issues intelligence.
- Security can provide effective crisis plans founded on thoughtful creative planning, rigorous testing, and the ability to act swiftly and decisively when faced with limited and changing facts. They rely on solid communications tactics and strategies that reach all their internal and external stakeholders in a timely manner and well ahead of traditional and social media.
- Security monitors and mitigates incidents from many domains, such as pandemics, climate change impacts, supply chain fragility, social unrest, workplace violence, travel safety, and labor shortage.
- More and more security organizations are increasing the bench strength of the security team with people who have non-security backgrounds, such as data analysts and technologists. A team with diverse skill sets can improve security's value and service offerings and help discover relevant trends and insights.
- Due to recent events, many security organizations have invested in frictionless access controls and security systems that integrate with other business unit platforms, such as visitor systems tied to pre-employment background investigation files for identifying red flag entries, and access controls that interface with HR systems for tracking building occupancy and attendance.

continued ↳

- Security is generally good at fact gathering and communicating in a crisis, and there is some movement to provide actionable intelligence to “see around corners.” Security is well versed in how intelligence works, how to use it, and where to get it.
- Security operations centers (SOC or GSOCs) are becoming 24×7×365 in some companies, and corporate security is running them in a way that is ROI capable and significantly quantifiable. They have discovered new ways to use SOCs that can positively impact the organization in areas outside security’s traditional purview, including quality control, HR, logistics, and more.
- Security is evolving to a more precise idea of all-hazards risk. Many are distributing responsibilities across their internal network.

Demonstrating the Value of Security to the Business

SEC Emeritus Faculty member J. David Quilter says so-called “smart security” enables the bottom line. It does this by supporting and collaborating with all departments — from communications and facilities to HR, compliance, legal teams, and more. But for this to be sustainable, you have to keep all departments engaged in security efforts long term.

One of the best ways to achieve smart security is by showing how great corporate security can take problems off managers’ hands. Start by identifying the root cause of a business loss, and highlight how security can alleviate this loss by having a frank and open discussion about the risk. Then, determine how you can partner to address the loss and improve the bottom line.

Here’s an example:

Suppose you manage corporate security for a retail chain, and you recognize that extreme weather events account for a significant annual business loss. To remedy this issue, you and your team develop a series of weather emergency protocols to reduce or eliminate losses in the company’s retail stores and ensure customers have access to the supplies they need beforehand. For example, you might put together a plan for monitoring conditions and activating procedures for moving or redirecting products as needed.

You present this to the CFO, leveraging your knowledge that they’ve been struggling with the amount of loss and supply chain disruptions in the wake of extreme weather. You suggest working together to ensure the new protocols are implemented — thereby solving a pain point you share. The preventive measures will reduce the amount of loss and positively impact the company’s bottom line.

continued ↳

Measuring and Reporting Performance

A highly effective corporate security program will make your organization more profitable. But proving this can be a bit challenging — especially if you haven't compiled the correct data.

Here are three ways to make that easier:

1. Run security as a business

When you run security as a crucial element of the organization — and track and measure it as such — senior executives will have more confidence in your operations and be more willing to increase your decision-making power.

Linking improved engagement scores with attracting and retaining talent is often coincidental with all-hazards communications, accountability and improving injury or asset loss claims. You just need to ensure you're tracking metrics most relevant to executives. Like, for example, how much downtime security events caused and how that has changed as you've implemented new initiatives.

2. Centralize your security data

Too often, security data is scattered across several disparate systems. For example, you may have your building security system activity in one application, social media monitoring data in another application, and visitor management data in yet another application. You might even be collecting data in spreadsheets or tracking threats on paper.

These silos make it challenging to cross-reference data to identify related events, investigate and act on existing threats, or compile comprehensive reporting with meaningful context. But, when everything is contained in one central location — especially leveraging a solution with configurable metrics dashboards, like Ontic — you'll benefit from unified data governance and automated end-to-end audit tracking.

3. Communicate and foster cross-team collaboration

Corporate security is only successful when everyone is engaged and committed. But to keep physical security top-of-mind, you have to ensure you're regularly communicating with the entire workforce. When all of your data is collected in a centralized solution, and you have real-time insight into threats, you can quickly get the message out and work with other departments to proactively neutralize that threat.

This is especially useful for bringing together the teams whose collaboration you need most — like IT, HR, facilities, and legal and compliance departments.

> "Running the security department as a business means you approach every problem with the interest of the owners and, other stakeholders of the business, at the front of your thoughts. As you formulate solutions, operate projects, or make decisions, you should be looking for solutions that empower the business to achieve the best possible outcome. Security is a function of the business – so why would you try to run it as an ad hoc service function within the organization?"
>
> **Herb Mattord, PH.D**
> Security Executive Council Content Faculty Expert

Communicating Brand Reputation and Business Continuity

Corporate security has a brand problem, and security professionals typically struggle with documenting their accomplishments. People often forget that a security team is most successful when nothing happens. If there's no violence, theft, or other serious security events, that may be a good sign that your program is effective. However, like any business function, it's essential to have key data to demonstrate efforts taken to ensure nothing happens and how they've reduced the frequency or severity of key risks over time with growth, revenue, and other relevant metrics.

It's a crucial and highly strategic element of the business that mitigates risks. Security teams make decisions every day that help ensure employees and assets are safe and secure from harm. And by communicating this with the right narrative and data, you can help improve the security brand and earn your internal customer's confidence and support.

In addition to keeping employees safe, another significant way corporate security impacts the organization is by maintaining business continuity and enabling the resumption of better-than-normal operations following an incident.

When you can anticipate threats and vulnerabilities and minimize their risk, you can protect the business from potentially devastating losses — or, at the very least, an expensive disruption. Using a software platform ensures you have access to those early warnings and can make data-driven decisions about how to better handle them.

Claiming Your Seat at the Table

We live in complicated times, and organizations of all sizes are grappling with a growing wave of interconnected threats. Today, identifying and managing security risks can be overwhelming — especially when you don't have the right services, technology, or cross-departmental collaboration to help fend off those threats.

Arguably, corporate security has never been more critical than it is now. But, to be highly effective in successfully fighting off these growing threats, security teams need additional business acumen, acknowledgment, support and a seat at the decision-making table. And so long as the senior leadership team regards security as a cost center rather than a value-adding arm of the organization, it will be difficult to earn the budget and influence your team needs to be effective.

According to the SEC there is likely a persuasive business case to be made, but if you don't yet have the talent, raise your hand and ask for help from an influential collaborator, colleague, or mentor.

ONTIC

Modernize your security program with Ontic

Ontic makes software that corporate and government security professionals use to proactively manage threats, mitigate risks, and make businesses stronger. Built by security and software professionals, the Ontic Platform connects and unifies critical data, business processes, and collaborators in one place, consolidating security intelligence and operations. **We call this Connected Intelligence.**

Learn More

About The Security Executive Council

The Security Executive Council is the leading research and advisory firm focused on corporate security risk mitigation strategies and plans. We work with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video for a quick overview or visit us at www.securityexecutivecouncil.com.