HOW TO BUILD AN EFFECTIVE CORPORATE SECURITY TEAM

A guide by **Premier Risk Solutions**

Table of Contents

Introduction: **The Role of Corporate Security**

Picture this: a Fortune-500 software company produces cutting edge services and tools for its clients, who, as a result, are able to run their businesses safely and efficiently. The company hires top programmers and project managers, investing in their growth within the company as well as their overall health and satisfaction. As a driver of innovation, the company makes the world a better place.

But none of this would be possible without an effective corporate security team.

Corporate security departments dynamically assess and manage risk. Their work goes beyond checking badges at the entrance, reviewing surveillance footage, or any other highly visible task. Corporate security is embedded into the business itself, active around the clock and adaptable to unpredictable scenarios.

In the future, in-house corporate security will be an increasingly important enabler of corporate growth. As we've observed from the COVID-19 pandemic in 2020-21, change within corporate security — and most other industries — has accelerated greatly. Security professionals have learned, likely the hard way, how important disaster resilience and crisis management are. Plus, with physical and cybersecurity attacks on the rise, organizations large and small need to learn how best to mitigate their unique risks.

This white paper will discuss the current landscape of corporate security and how security professionals can adapt to ever-changing threats in the future. We will detail the importance of talking to a corporate security consultant to help manage these dynamic variables.

Problem: **Failure to Recognize the Value of Corporate Security**

When done right, security allows operations to occur without incident. However, this can inadvertently prompt even the most well-intentioned leaders to take security for granted.

If decision-makers are unaware of the full scope of duties that a security team handles on a daily basis, when it's time to make budget cuts, for example, security is often the first to go. It's normal for companies to periodically slim down and optimize their budget, but cutting essential operations due to a lack of understanding is unacceptable.

Sometimes, security executives themselves don't fully know how to articulate their responsibilities to senior management. As a result, they run the risk of underestimating themselves, underperforming, and exposing their organization to avoidable threats.

Misconceptions about Corporate Security

One of the biggest problems facing corporate security departments is poor perception of what they actually do.

Generally, security departments are regarded as a large but necessary financial burden. This could not be farther from the truth.

The role of security is often only apparent when big breaches or disasters happen, which contributes to security's faulty reputation as an expensive accessory. While it's true that successful security should not be so highly visible, corporate security is much more vital to a company's growth potential than is currently recognized by most.

Compared to an organization's other departments, corporate security is one of the most essential and least understood. Here are some of the most popular misconceptions about corporate security:

? Security does not generate revenue

? Security has nothing to do with optimizing overall corporate operations

? Security mainly deals with prevention

Misconceptions #1 and #2 are directly related. Where business units generate revenue via some form of transaction, corporate security generates revenue by streamlining and securing that process. Everyday transactions wouldn't be able to happen if not for security. Corporate security not only secures operations — it enables them.

Furthermore, the investigative capacity of a corporate security department oftentimes recovers tangible assets of their organization, which can and should be attributed to optimizing corporate profits. Recovering lost assets also enhances brand integrity and, ergo, brand reputation.

As for misconception #3, the role of security encompasses far more than prevention. In this day and age, security must also detect attacks that have already bypassed preventative measures and move to contain them. Security must be versatile enough to address unforeseen issues and deal with them before they have the chance to affect the rest of the organization. These breaches have an unknown quantifiable value, so preventing and containing them goes a long way towards protecting the organization's profitability, integrity, and reputation.

Corporate security not only secures operations — it enables them.

Failure to Align Strategically with Corporate Goals

As a result of these misconceptions, corporate security often fails to align with the company's strategic goals.

A strategy is a consolidated plan of action intended to achieve specific objectives. Strategic management should make use of all the tools and resources at its disposal, in order to advance the company's long-term goals.[1] All too often, though, security is an afterthought or left out altogether when company leaders make these strategic plans of action.

These problems will only figure more prominently going forward, so the need for a professional consultant to help boost corporate security's profile will be greater than ever.

Take Action

1. Does your organization recognize the value of the corporate security department?
2. Is your security team currently aligned with long-term corporate goals?
3. Does your corporate security team face challenges internally? What plans or policies are in place to handle these challenges?

[1] Christopher Walker, "The Strategic Leader", ASIS International, 1 Feb 2018, retrieved 18 Jul 2021 from https://www.asisonline.org/security-management-magazine/articles/2018/02/the-strategic-leader/

Limited Solutions and Drawbacks in Current Corporate Security Management

There is no single way to have an effective corporate security department. Not only will it vary depending on the company's size, scale, industry, geographic location of physical operations and assets, and other factors, but security should also be fully customizable for the present and near future.

Unfortunately, as the COVID-19 pandemic revealed, many businesses are unprepared for times of uncertainty. Even before the pandemic, many business leaders opted to focus on the more predictable short term, an approach that Harvard Business Review reports "leaves billions of dollars of earnings on the table and millions of people needlessly unemployed."[2] As we'll discuss, if these insufficient processes continue going forward, there will be dire consequences.

Cost Reduction Instead of Cost Optimization

During the COVID-19 pandemic, many security departments were asked to cut spending. A good test of a security department's preparedness to demonstrate its value is to observe how they respond to this request. Many security and risk management leaders have discovered that they lacked experience in strategic planning during times of uncertainty.

Executive advising firm Gartner asserts that, because of this lack of experience, most chief information security officers (CISOs) jump to cost reduction rather than cost optimization. Gartner states that, "[b]y 2023, 30% of a CISO's effectiveness will be directly measured on the ability to create value for the business."[3]

Laying off employees is the easiest and least effective way to cut costs. This only causes organizations to become understaffed and overworked. When employees are overworked, they are less able to be proactive and strategic because they are putting out fires in the present. As a result, organizations become more vulnerable to internal and external threats.

Ideally, security managers would know how to optimize costs rather than simply cut them. But optimizing costs requires security leaders to know exactly how their department aligns with the strategic interests of the company itself — something many security leaders cannot yet do.

Many security and risk management leaders have discovered that they lacked experience in strategic planning during times of uncertainty.

[2] J. Peter Scoblic, "Learning from the Future", Harvard Business Review, Jul-Aug 2020, retrieved 8 Aug 2021 from https://hbr.org/2020/07/learning-from-the-future

[3] Beth Wasko, "How Security and Risk Leaders Can Prepare for Reduced Budgets", Smarter with Gartner, 7 Jul 2020, retrieved 1 Aug 2021 from https://www.gartner.com/smarterwithgartner/how-security-and-risk-leaders-can-prepare-for-reduced-budgets/

Limited Adoption of Convergence

Convergence is the centralization of physical security, cybersecurity, and business continuity. Business continuity is an organization's ability to respond effectively to threats like natural disasters or data breaches and, thus, to continue functioning in the wake of such threats.

The purpose of convergence is to take an all-hazards approach to protecting the company. Theoretically, convergence should both strengthen and streamline security processes.

However, despite how popular the term "convergence" has become over the last decade, only a small fraction of companies have actually put it into practice. According to a 2019 study by the ASIS Foundation, just under a fifth of respondents converged all three areas of security, while those who partially converged made up 33%.[4] Nearly half remained unconverged.

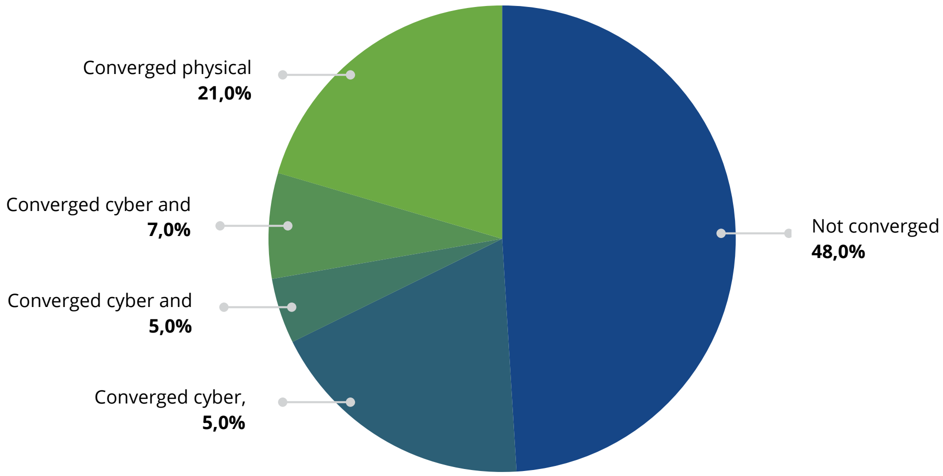


Figure 1: Respondents to a 2019 ASIS study found limited adoption of full convergence across multiple industries

These findings demonstrate that there is still plenty of potential to optimize corporate security. The same study also found that the most significant benefit reported among converged organizations was the "alignment of security strategy with corporate goals."[5]

This is exactly what organizations do: integrate security into the very fabric of their strategic plans. Yet few have actually taken steps to converge and reap these benefits from the onset of the organization's initiatives.

[4] Scott Briscoe, "How Converged Are Corporate Security Functions?", ASIS International, 17 Dec 2019, retrieved 18 Jul 2021 from https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2019/december/How-Converged-Are-Corporate-Security-Functions/?_t_id

[5] Ibid

Neglectful Investment in Corporate Security

Many small and medium sized businesses look at high-profile security incidents like the Colonial Pipeline breach[6] and assume that criminals have no interest in smaller, lesser-known companies. The truth is that small to medium sized businesses are still targets, if only because attackers know that these companies are less likely to invest in quality physical and cybersecurity.

A Ponemon Institute study in 2019 reported that 76% of small to medium sized U.S. businesses have experienced a cyberattack.[7] Yet almost 90% of these businesses spend less than 20% of their IT budget on cybersecurity.

These findings suggest that the more a company invests in cybersecurity, the more they trust that these measures are effective. The same goes for physical security — making an effort to update surveillance technology, key cards, and personnel training goes a long way in protecting the company in a way that inspires confidence.

About 60% of small businesses shut down within six months of suffering a cyberattack.[8] The most unfortunate part is that these outcomes are preventable.

76% of small to medium sized U.S. businesses have experienced a cyberattack.

Take Action

1. If your security department were asked to make a 10% budget cut today, what areas would be cut first? Do these cuts optimize overall costs or simply reduce them?
2. To what extent have you converged cybersecurity and physical security? Are you satisfied with this level of convergence?
3. How do you identify physical and cyber security breaches or threats today? How much of your budget is currently allocated toward physical security and cybersecurity? What is your confidence level that your current investment is sufficiently protecting your company on all fronts?

[6] William Turton and Kartikay Mehrotra, “Hackers Breached Colonial Pipeline Using Compromised Password”, Bloomberg, 4 Jun 2021, retrieved 3 Aug 2021 from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[7] “Exclusive Research Report: 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses”, Ponemon Institute LLC, Oct 2019, https://start.keeper.io/2019-ponemon-report

[8] Joe Galvin, “60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here’s How to Protect Yourself”, Inc., 7 May 2018, retrieved 22 Aug 2021 from https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

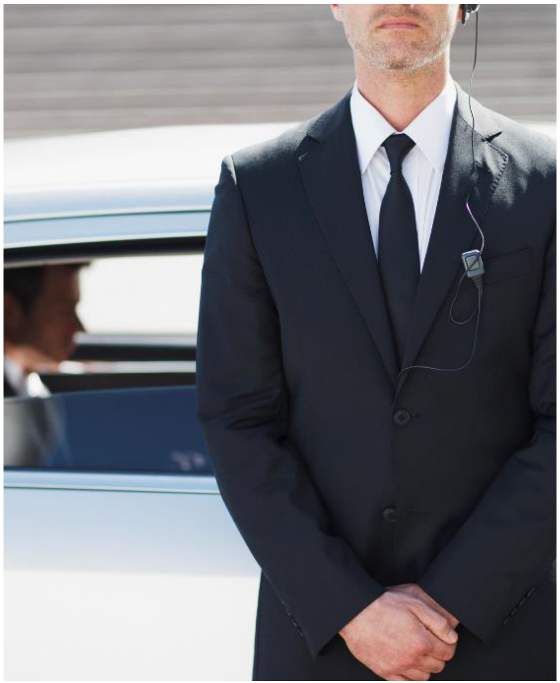
A Better Solution: **Building an Effective Corporate Security Team**

Given the limitations outlined above, there must be a better solution. Here's what that would look like.

Balanced Budget Allocation

In addition to not converging or only partially converging, companies also make the mistake of allocating a lopsided budget for cybersecurity and physical security. Secure identity product manufacturer HID Global observes:

> *"IT departments typically enjoy much larger budgets than physical security departments, and they're used to receiving funds for constant updates to keep up with advances in technology. Physical security departments, on the other hand, may invest in cameras and card systems that are expected to remain in place for decades. Such thinking is no longer practical as technology evolves and vulnerabilities are publicly revealed. Physical security equipment needs to be on a refresh rate closer to that in the IT industry."*[9]



Furthermore, IT and physical security should collaborate much closer than they currently do. While nearly 90% of companies conduct physical security risk analyses, only two-thirds of these respondents share the results with IT.[10]

A corporate security consultant can help set company-wide security standards and advise on the best budget for your security department.

[9] "The Convergence of Physical and Logical Access: What it Really Means for an Organization's Security", HID Global, page 5, https://info.hidglobal.com/PACS-Global-ConvergenceofPhysicalandLogicalAccess_LP-Request.html

[10] Ibid, page 7

Diverse Team Members

The right corporate security team isn't merely a group of people with the most years of combined experience. Team members also need to be of diverse backgrounds, in terms of cultural environments, geographic experience, and exposure to different disciplines. Most of all, they should be able to adapt to changing environments.

Another essential trait that is more difficult to hire for but just as important: having the courage and conviction to challenge higher-ups. Long-time security professionals can often find themselves on autopilot, going through the motions instead of making individual decisions. New and diverse talent can come in with a fresh perspective and point out crucial gaps that are overlooked out of routine.

Corporate security leaders should, in turn, be open to hearing opinions that differ from their own. The free exchange of knowledge and experience will benefit the company as a whole.

In the same way, an external corporate security consultant is best positioned to offer quality, unbiased guidance on how to optimize your corporate security department, including benchmarking and developing current best practices. It's a win-win: the consultant can apply their comprehensive industry knowledge without the complication of being too familiar with your organization's challenges.

The right corporate security team isn't merely a group of people with the most years of combined experience.

Strategically Aligning with Corporate Goals

Once the best team members are in place, the corporate security department must be able to show that it is an indispensable part of the company's overall growth, not only by saving money in losses but by enabling the company to make more.

Consider the following real-life example that has been adapted from ASIS:

> *The security executive of Company X wants to show how her department aligns with the company's overall objectives, so she begins by gathering input from her staff: the consensus is to improve the company's access control systems, which affect every part of the business.*
>
> *In order to tackle this monumental task, the executive works with the finance department to settle on a reasonable budget for a new system. She meets with the legal department to work out any liability issues and human resources to develop new training for employees. She then calls a joint meeting with the HR, operations, and legal departments to create new policies to support the proposed system.*
>
> *Later, the security executive meets with external suppliers to start an open bidding process and hammer out a timeline for the delivery of the new system. She also meets with Company X's business developers in order to time the installation so that it reduces the overall financial impact on the company. When she brings these plans to senior management, it is approved.*[11]

This is an example of strategic security leadership. The new access control system brings multiple sections of the company together towards a common goal: reduce threats while controlling costs. In the process, the security executive raises her department's profile and saves money for the company in the long run.

If your corporate security department cannot currently shoulder these responsibilities — appropriately allocate security funds, hire diverse team members, and align strategically with corporate goals — you are in need of expert consulting. An effective corporate security consultant can perform an in-depth risk assessment and create a personalized security management plan that is unique to you.

Take Action

1. What proportion of your budget is set aside for cybersecurity and for physical security? Do both areas have enough to be able to do their jobs effectively?
2. What backgrounds and perspectives do your security leaders and staff represent? Do they challenge one another to consider alternative approaches?
3. If your corporate security executives were asked today to demonstrate their value to the company, what would be their value proposition?

[11] Walker

Buyer's Guide: **What to Look for in a Corporate Security Consultant**

To summarize, a quality corporate security consultant:

- Provides an unbiased holistic perspective covering both physical and cybersecurity concerns
- Shows how your corporate security department can position itself as an integral enabler of corporate growth
- Provides a consistent and standardized plan for security processes, including procedures for regional differences, standard hierarchy, etc.
- Advises an adaptable approach that combines the benefits of both prevention and detection
- Has professional experience in a variety of industries and has performed risk assessments for both individuals and organizations
- Ranks and prioritizes your current organizational needs based on the resulting risk uncovered through the risk assessment consulting engagement so you know where to best begin mitigating your organizational risks

Premier Risk Solutions (PRS)® Case Studies

Premier Risk Solutions (PRS)® is a leader in corporate security consulting. Our professional experience in law enforcement, military, and private sectors have equipped us with the knowledge to manage today's unique security concerns.

We have a long track record of optimizing customized corporate security in a variety of industries. Our experts have led security at technology companies like Honeywell, AT&T, and Microsoft, as well as advised government agencies on sensitive security matters.

PRS® Asset Protection

PRS® often helps clients perform active asset protection. This scenario is taken from a real case we worked for one of our clients:

> *While patrolling the premises of the client company's office building, security personnel observed over 400 unsecured laptop computers after working hours, even though employees were given locking cables. The officers created and distributed professional cards reminding employees to secure their computers. Over the next 30 days, the number of unsecured assets was reduced by 98% and stayed there.*

This was not a complicated security operation, but it resulted in significant financial savings.

To calculate this value, let's estimate that about 20 company laptops are stolen per year, each one priced at $1,500. Then factor in the cost of the intellectual property (IP), which can vary from one device to another.

Also consider the productivity and diverted resources that are lost. The employee who lost the computer can use a different temporary device during the 10 to 14 days it usually takes to get a ready-to-use replacement, but during that time he or she will likely not be fully engaged. Add on top of that the labor costs involved in reporting the loss, authorizing a replacement, and then ordering, preparing, shipping, and formatting the computer before it gets to the employee.

In reality, the average cost per loss is much higher than the price of the computer. It actually hovers between $10,000 and $20,000.

Multiply that by our earlier estimate — 20 laptops lost per year — and the total loss to the company balloons to $200,000-$400,000 annually.

In our example, security reduced that loss by 98%, meaning that their simple action saved the company $196,000-$392,000.

Compare this figure to the cost of creating reminder cards for the employees: $200. For every dollar spent, security returned about $1,000.[12]

Plus, with more secured equipment, the company dramatically reduced the chance that sensitive data could fall into the hands of malicious actors. As seen from the 2021 Colonial Pipeline breach, it only takes a single compromised password to threaten the whole system, not to mention the corporation's public reputation.

Security is worth the investment. This was just one of many ways in which PRS® has helped clients with their budget — not by pinching security funds and talent, but by taking action in the moment to save larger sums of money in the long-term.

[12] "The Value of Value Proposition for Security", Premier Risk Solutions, 18 Feb 2018, retrieved 18 Jul 2021 from https://www.premierrisksolutions.com/blog/the-value-of-value-proposition-for-security/

PRS® Consulting Services

PRS® consulting consists of creating strategic governance standards that detail how clients' corporate security operations should run for optimal safety and security. For example, in early 2021, PRS® completed a consulting job for a high-tech, Fortune-500 software company.

The consultation began by conducting extensive interviews with client personnel on their existing processes and making suggestions based on industry standards and best practices. These interactions resulted in a series of documents specifying the framework that would enable security to meet the company's business needs, in alignment with organizational policies and strategic objectives.

For example, in order to protect the company's employees, customers, visitors, buildings, and other assets, PRS® recommended the client organize their physical security operations into 12 program areas:

- Corporate Physical Security
- Crisis Management
- Data Center Physical Security
- Event Security
- Enterprise Technology
- Investigations
- Personnel Protection
- Regional Physical Security Operations
- Intelligence
- Threat Management
- Travel Security
- Risk Management

The documents also outlined hierarchies of standards, guidance on regional differences, and more. The reports are highly comprehensive and the client can choose how and to what extent they want to implement our recommendations. In this case, our client chose to fully implement.

Every consultation will differ based on your unique needs and evolving industry demands. Contact us to discuss scope of work, current pricing, and more.

We can consult with you wherever you are. PRS® serves Seattle, Atlanta, Charlotte, Chicago, Columbus, Dallas, Honolulu, Las Vegas, Los Angeles, Miami, New York City, Orlando, Portland, Phoenix, Salt Lake City, San Francisco, and many other cities across the U.S. as well as select cities in 70 countries around the world.

Conclusion: **Corporate Security is Vital to Corporate Growth**

It is now more important than ever to ensure that your corporate security department is up to the challenge of tomorrow's combined IT and physical threats. Given the complexity and unpredictability of everyday business, companies that are poised to counter the unexpected are most likely to succeed.

Seek an impartial, comprehensive consultation with a professional corporate security specialist. They can identify security gaps that can be difficult to observe from inside the company. Plus, their experience in other industries (as well as yours) will inform the security plan they build for you.

Whether you're a leading software company or multinational industrial manufacturer, the plan will be customized to your organization's unique needs. The security plan will allow you to reevaluate your corporate security department's value proposition and present it to senior management with the confidence of a department that knows exactly how it enables the company not only to save money but also to grow.

An effective corporate security strategy will protect financial assets, physical infrastructure, information technology, intellectual property, and human life. In short, corporate security is essential to improving the state of the world. Talk to a consultant today to give your corporate security department the tools it needs to do all of this and more.

You can reach out to Premier Risk Solutions by any of the following manners:

Phone: +1 (206) 735-4956
Email: info@premierrisksolutions.com
Website: www.premierrisksolutions.com

References

Beth Wasko, “How Security and Risk Leaders Can Prepare for Reduced Budgets”, Smarter with Gartner, 7 Jul 2020, retrieved 1 Aug 2021 from https://www.gartner.com/smarterwithgartner/how-security-and-risk-leaders-can-prepare-for-reduced-budgets/

Christopher Walker, “The Strategic Leader”, ASIS International, 1 Feb 2018, retrieved 18 Jul 2021 from https://www.asisonline.org/security-management-magazine/articles/2018/02/the-strategic-leader/

“Exclusive Research Report: 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses”, Ponemon Institute LLC, Oct 2019, https://start.keeper.io/2019-ponemon-report

Joe Galvin, “60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here’s How to Protect Yourself”, Inc., 7 May 2018, retrieved 22 Aug 2021 from https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

J. Peter Scoblic, “Learning from the Future”, Harvard Business Review, Jul-Aug 2020, retrieved 8 Aug 2021 from https://hbr.org/2020/07/learning-from-the-future

Scott Briscoe, “How Converged Are Corporate Security Functions?”, ASIS International, 17 Dec 2019, retrieved 18 Jul 2021 from https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2019/december/How-Converged-Are-Corporate-Security-Functions/?_t_id

“The Convergence of Physical and Logical Access: What it Really Means for an Organization’s Security”, HID Global, page 5, https://info.hidglobal.com/PACS-Global-ConvergenceofPhysicalandLogicalAccess_LP-Request.html

“The Value of Value Proposition for Security”, Premier Risk Solutions, 18 Feb 2018, retrieved 18 Jul 2021 from https://www.premierrisksolutions.com/blog/the-value-of-value-proposition-for-security/

William Turton and Kartikay Mehrotra, “Hackers Breached Colonial Pipeline Using Compromised Password”, Bloomberg, 4 Jun 2021, retrieved 3 Aug 2021 from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

PRS

PREMIER

RISK SOLUTIONS

STRONG, SAFE & TRUE