DATAMINR PULSE

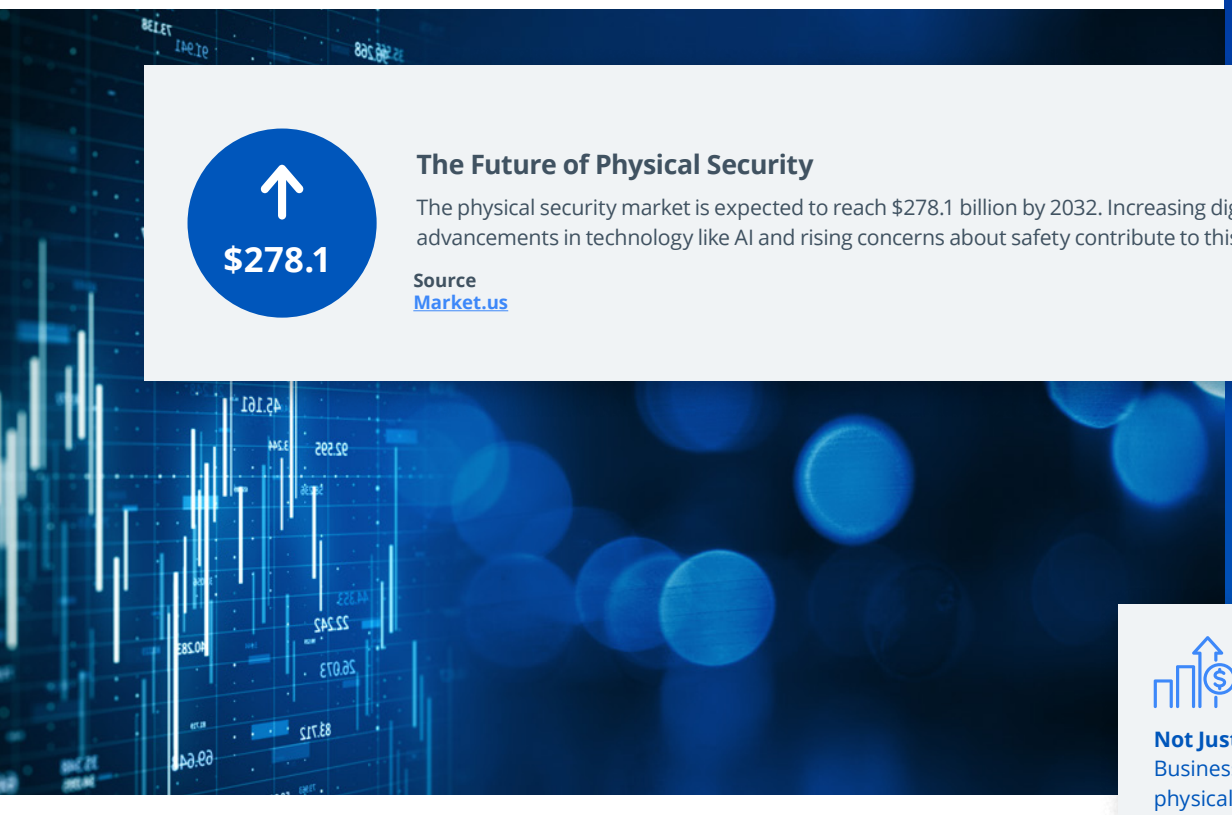
How to Make a Strong Business Case for Investing in Corporate Security

When it comes to business security, much of the attention in recent years has been given to cybersecurity due to the **exponential rise in cyber crime** against organizations worldwide. However, companies must keep in mind that physical (or corporate) security is an equally important aspect of organizational safety, and **operational and physical resilience**.

As physical events are occurring at an unprecedented frequency and unpredictability—such as extreme weather events, workplace violence and geopolitical conflicts—neglecting physical risk management can lead to severe consequences. These include operational disruptions, product losses, damages to physical and digital assets, reputational damage, human injury or even loss of life.

As such, it's imperative that C-suite executives and boards prioritize investments in technology and resources to address this increase in physical risks. Corporate security leaders and teams know this, but many keep encountering the same obstacle: obtaining buy-in from their senior management.

Here, we explore best practices you can consider to build a strong, compelling business case for your security investments.



$278.1

The Future of Physical Security

The physical security market is expected to reach $278.1 billion by 2032. Increasing digitalization, advancements in technology like AI and rising concerns about safety contribute to this growth.

Source
Market.us

Understand the Strategic Value of Physical Security Investments

Security operations are an indispensable component of every business. By being able to ensure the safety and wellbeing of employees, assets and critical operations, organizations can maintain business continuity and better withstand and recover from shock events and risks. Thus, sufficient investment in security is inherently a strategic business investment.

Not Just a Cost Center
Businesses should view physical security as more than just a cost center. Profit-center functions depend on it to maintain operational continuity and generate revenue.

Best Practices for Developing a Compelling Business Case

Prior to developing and writing a business case, it's vital that physical security leaders gain an accurate and holistic understanding of their operating environment, including the:

Needs of team members

Priorities and constraints of colleagues responsible for cybersecurity, executive protection, and any other security-related functions

Vision and strategy of senior management

Having an accurate grasp of your environment will help inform the parameters of a strong business case. It's also important to remember, as you write the business case, to align it with management's corporate strategy and to frame the story in a way that clearly supports the strategy.

As you start building your case, consider the following six steps, as recommended by Dataminr and the U.S. **Cybersecurity and Infrastructure Security Agency** (CISA). Although CISA's work focuses on **cyber-physical security convergence**, the same process and business case components also apply to physical security.

No. 1 Establish a security project team

- Include multiple representatives. Work with adjacent risk management functions to identify areas where you can cooperate to generate efficiencies and, when possible, form a coalition so that you can advocate together for your business case.
- Establish clear roles, responsibilities, expectations for involvement, and create a project timeline and the team's communication schedule

No. 2 Conduct a risk assessment

- Review your organization's current security posture, and conduct a risk assessment to understand the organizational risks (threats, vulnerabilities and consequences)
- Document the assessment results to help define the business case rationale
- Identify all assets that require safeguarding and the associated risks for each
- Determine if similar initiatives or investments are being considered

Risk Assessment Examples from the International Organization for Standardization (ISO)

These guidelines can help inform your risk assessment

ISO 31000:2018: Risk management guidelines

ISO 22361: Security and resilience crisis management guidelines

No. 3 Analyze benefits and costs

- Using the risk assessment results, develop a description for the security project or program
- Identify quantitative and qualitative benefits of the program
- Analyze the security investments required, including the potential opportunity cost and impact to the business of not making these investments

No. 4 Anticipate potential resistance factors

- Consider the various factors that can hinder executive buy-in
- Prepare responses to potential objections, including supporting data points
- Be ready to answer questions typically posed by senior executives, including:

Have you consulted with other stakeholders, such as legal, HR, etc.?

What will happen if you don't get the requested budget/capability?

Can we combine budget/ capabilities through other security functions? For example, can this software be shared with the cybersecurity team?

What if we outsourced some or all of this capability?

While there are no set answers to these questions as they vary by organization, adequate preparation and a well-crafted narrative that explains the practical consequences of the requested security investment should better position you for success.

No. 5 Develop implementation plan, schedule and performance criteria

- Demonstrate security investment strategy and steps
- Assign tasks, provide a project schedule, and define milestones and metrics for success
- Describe how the rollout will impact the organization, and the resources and communication plan needed to do so

No. 6 Build and deliver a strong presentation with engaging narrative and data

- In your presentation, make clear the decisions you want senior management to make. Follow with the security project or technology description; business impact; analysis of alternatives; costs and benefits; implementation plan and schedule; and detailed recommended security investment
- When possible, articulate risk in financial terms of lost revenue or legal/compliance risk
- Remember: The business case is a story. Decide the story you're going to tell and how to make it as compelling as possible. A proven best practice is to make the story vivid by stating scenarios and consequences. For example, "with this level of funding we can reliably protect our company against [a specific risk]. Or, "without this funding/capability, we run the risk of this [incident] happening and these will be the consequences for the business."

Pro Tip: What to Include in Your Presentation
All information in your presentation should support the overarching narrative. Don't mistake metrics for analysis. Just because you have a lot of statistics to create visually appealing, attention-grabbing charts—even if they add some context—doesn't mean you need to include all of them. Restrict your visuals to only the data that is truly needed and relevant for decision making.

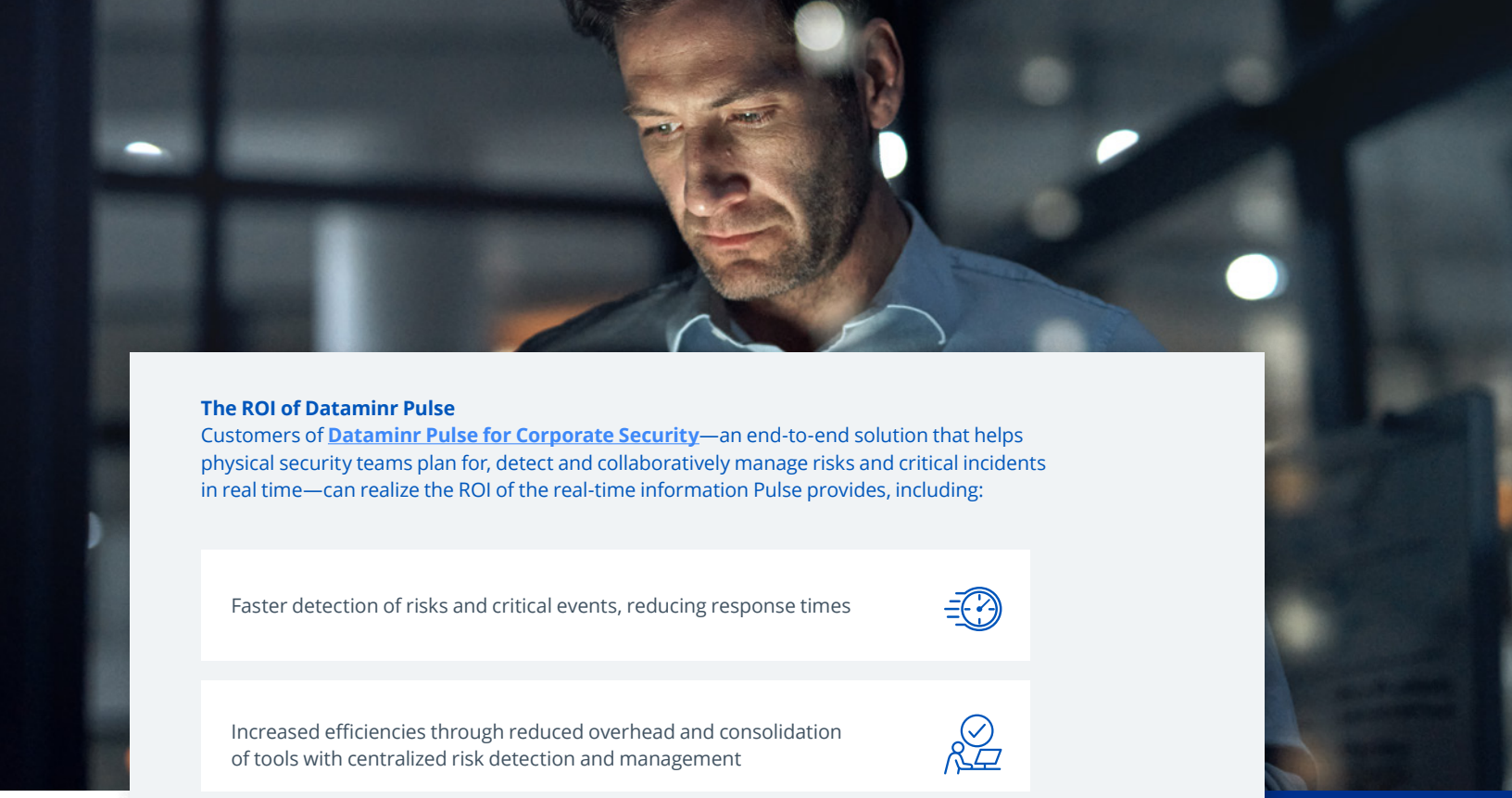
Demonstrate Return on Investment (ROI)

As you present your business case, it's likely that you'll be asked to demonstrate what the return on investment (ROI) of the requested security program or technology will be. Benefits like financial costs and savings are key, but aim to have a mix of quantifiable and qualitative benefits. That will allow you to truly show the value of your program or tech.

Questions to consider:

- What does success look like for the security team and the organization?
- What efficiencies will be achieved?
- What's the **total cost of ownership (TCO)**?
- What are the costs or risks of not making the security investment?
- What past examples of high-impact events can be used as case studies to describe the risksand support the benefits associated with the program investment?

Be sure to focus on the metrics that matter most to your organization and those of your key stakeholders, such as your cybersecurity colleagues. Industry benchmarks can also prove useful in showing senior management how your organization fares against competitors.



The ROI of Dataminr Pulse
Customers of Dataminr Pulse for Corporate Security—an end-to-end solution that helps physical security teams plan for, detect and collaboratively manage risks and critical incidents in real time—can realize the ROI of the real-time information Pulse provides, including:

- Faster detection of risks and critical events, reducing response times
- Increased efficiencies through reduced overhead and consolidation of tools with centralized risk detection and management
- Increased awareness of threats—and improved security posture— as measured over time
- Higher value of sustained business continuity, as measured by revenue protected against benchmarked average loss (per event type over time)

Read more about the ROI of Dataminr's real-time information.

Businesses today are undoubtedly facing a more dynamic and complex threat landscape than ever. The cost to recover from a physical or cyber incident is often more expensive than the cost of preventing them. That's why securing both the physical and digital aspects of an organization is vital to improve its overall security posture and business resilience. By investing in physical security, and providing the function with sufficient resources, companies are investing in their agility, resilience and long-term success.

Learn More

Request a demo to see how organizations like yours protect their people and assets against physical threats with Dataminr Pulse for Corporate Security.

REQUEST A DEMO