The Business Case for **Security**

"Can you put a price on the value your people and assets provide to your organization?" That is the key question when your organization considers investment in security. Leaders can build and sustain a culture of readiness within their organizations by investing in security measures to drive strategy, policy, revenue, and actions. Improving the organization's resilience requires an enterprise security program that addresses both physical and cybersecurity risk.

A business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment (ROI). According to recent reporting, **43% of cyberattacks are aimed at small businesses; however, only 14% of small businesses are prepared to defend themselves.**[1] Physical and cyber incidents can have catastrophic impacts on the daily operations of small and mid-sized businesses (SMB). Moreover, physical security incidents—whether targeted violence or natural disaster—can have catastrophic impact on the daily operations of small and mid-sized businesses (SMB). **Having the flexibility to securely adapt to current and future threats will increase resilience.**

Key Considerations/Potential Threat Vectors

Physical threats

- Burglary
- Vandalism
- Insider threat
- Theft
- Arson
- Terrorism
- Natural disaster
- Active assailant
- Vehicle ramming
- Improvised explosive device
- Improvised incendiary device

Cyber threats

- Ransomware
- Data breach
- Malware
- Phishing
- Hacking
- Denial of Service

[1] Scott Steinberg, "Cyberattacks now cost companies $200,000 on average, putting many out of business," March 9, 2020, CNBC, cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

[2] Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Resources, n.d., cisa.gov/publication/insider-threat-mitigation-resources.

[3] Cybersecurity and Infrastructure Security Agency, Cost of a Cyber Incident: Systematic Review and Cross-Validation, (October 26, 2020), accessed May 25, 2021, cisa.gov/publication/cost-cyber-incident-systematic-review-and-cross-validation.

[4] Cyentia Institute, Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents (IRIS 20/20), published 2020, site updated 2021, accessed May 25, 2021, https://www.cyentia.com/iris/.

What is the typical cost of an incident?

The cost to recover from a physical or cyber incident is often more expensive than the cost of preventing such events. Though the cost of remediating a physical or cyber incident is quantifiable, recovering a company's damaged infrastructure and reputation can be difficult to assess. In the final analysis, **there is no substitute for the public's trust.**

Moreover, employee safety is a crucial measure of a company's commitment to ensuring a culture of security. Workplace violence affects 2 million people each year, directly impacting the physical requirements and cost of security.

Leadership within an organization **must** consider investing in the long-term well-being of their organizations to prevent future costs stemming from security incidents.

Physical security and insider threats can result in sizable financial losses for an organization and can adversely impact continuity of operations.[2]

50%
decrease in productivity for the organization

20-40%
employee turnover following an incident

$500,000
average out-of-court **settlement**

Cyberattacks can be very costly to mitigate, especially when they require new systems or architecture or cause the loss of company data, intellectual property, and other sensitive information.

Only 35%
of SMB could remain profitable for more than three months if they lost access to essential data,

with more than half
becoming unprofitable in under a month.[3]

A $100 billion enterprise that experiences a typical cyber event should expect a cost that represents less than 1% of annual revenues. **A SMB that brings in $100,000 per year, on the other hand,will likely lose 25% of its earnings or more.**[4]

Developing a business case for security will add value and drive the importance of investing in physical security and cybersecurity for your organization. The following steps can help you assess your security vulnerabilities and develop actionable mitigations before an incident occurs.

Understand Your Security Posture

Understand the business' security posture

- Does your company have a Chief Information Security Officer, Chief Security Officer, and Chief Information Officer?
- Are existing vulnerabilities linked to physical or cyber assets?
- Do the security gaps threaten the infrastructure?

Identify business assets that need to be protected

- Physical: People, property, and facilities, including access
- Cyber: Server rooms, computers, and IT infrastructure, including means of information sharing

Align security investments to business objectives

- Business needs, risks, and compliance requirements
- Company-specific numbers quantified by business impact analysis
- The cost of investing versus the cost of an attack

Determine the right areas for investment

- Risk/reward ratio
- Knowing and understanding your threat environment
- Prioritization of quick wins and urgent gaps
- Employee training and security awareness
- Partnerships for security purposes
- Establishing an advisory team

Implement a security plan and schedule

- Develop employee training for existing and new security measures
- Exercise the plan in coordination with local first responders
- Create a schedule for implementing the security plan

Preparation

- Focus on resource requirements for security that buys down risk
- Anticipate questions and have answers

Industry Tips

KNOW YOUR AUDIENCE

Getting buy-in from senior executives means presenting the business case with their decision-making process in mind. Consider known resistance factors the team has already identified, and craft your presentation to demonstrate how your approach addresses them. Align your analysis and recommendations with the organization's business priorities and strategic objectives. Present a strong narrative—thoughtful storytelling engages an audience.

IDENTIFY YOUR CHAMPION(S)

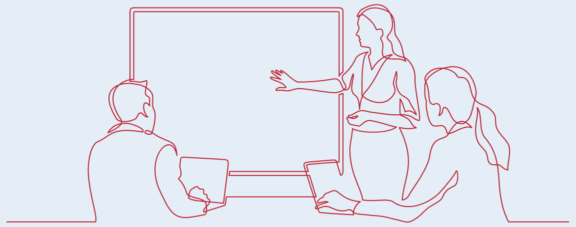
With an enterprise security approach, security investment recommendations should not come as a surprise to senior executives. Prior to writing the full business case, identify a champion or two among senior leaders who will support and defend the project, and consult them throughout process to ensure the messaging is on point.

PARTICIPATE IN INDUSTRY ASSOCIATIONS

Industry associations are excellent resources. Participating in industry association security committees is a great way to become aware of the challenges facing your industry; identify opportunities for funding; learn industry best practices; receive trainings; and identify resources through information-sharing collaborations. Senior leadership will be encouraged to understand that your security strategy is partially cultivated by best practices among other industry members.

UNDERSTAND HOW LEADERSHIP DECISIONS ARE MADE

Security leaders need to understand how the organization makes decisions, allocates money across functional areas, prioritizes initiatives, and develops strategic plans. Determine if security measures are implemented annually or ad hoc. Identify how often security measures are reviewed against organizational risks and strategic priorities. These insights will inform the business case rationale and help determine the right approach for presenting this information.



For more information or to seek additional help, contact us at **Central@cisa.gov** or visit:

Consider Convergence (cisa.gov/publication/cybersecurity-and-physical-security-convergence)
Stop Ransomware (cisa.gov/stopransomware)
Conduct a Cybersecurity Assessment (cisa.gov/cybersecurity-assessments)
and **Infrastructure Vulnerability Assessments** (cisa.gov/critical-infrastructure-vulnerability-assessments)