everbridge®

Brief Guide to Physical Security

For many organizations, managing safety and security can be a daunting task. **Threats are increasing and risks are becoming more diverse.**

It is important not to oversimplify the emerging threat narrative.

Overview

Staying ahead of security threats is paramount for executives and each year, those threats become increasingly complex.

Emerging threats could be economic, environmental, geopolitical, societal or technological. It is important not to oversimplify the emerging threat narrative, as security risks are progressing faster than organizations can adapt.

Strong leadership skills are required to drive a culture of advocating security within the organization. In an uncertain globalized world with a growing number of risks, many colleagues will be inspired by a security executive that emphasizes the importance of proactively safeguarding employees and the environment in which they live and work.

Managing security awareness and advocacy across an organization can be difficult as people are often resistant to change. The purpose of a safety and security aware culture is to prioritize the security agenda across the organization and establish how colleagues can engage.

Establishing cross-departmental partnerships and getting all stakeholders behind the mission is key to getting the support needed to deploy an organization-wide security approach. Focus your team and agenda on facilitating colleagues to action security safely, rather than telling people what not to do. Keeping regular scheduled communications with all stakeholders will enable any issues to be quickly identified and managed.

Set out a business case that shapes the CEOs view of safety and security as a commercial investment.

Leading physical security platforms are designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

To stay secure in a connected world, organizations must keep track of all emerging security threats and assess the potential commercial and operational impacts of when, not if, they will experience a critical event. With an increasingly complex and unpredictable threat environment, it has never been more imperative to act faster. With more complete intelligence, you'll be able to increase your speed and decisiveness in order to assess risks and prevent those risks from harming your people or disrupting your operations.

Leading physical security platforms are designed to integrate multiple unconnected security applications and devices; and control them through one comprehensive user interface. They collect and correlate events from existing disparate security devices and information systems (video, access control, sensors, analytics, networks, building systems, etc.) to empower security personnel to identify and proactively resolve critical events.

The platform will deliver numerous organizational benefits, including increased control, improved situational awareness, actionable insights and proactive management reporting. Ultimately, these solutions allow organizations to reduce costs through improved efficiency and to improve security through increased intelligence.

Proving safety, security and commercial value to stakeholders is a prerequisite for every top security executive in building a business case for a physical security project.

Security is a commercial investment, not a technology or facilities spend.

Few CEOs have a background in risk management or security, and therefore, may feel uncomfortable prioritizing the required level of investment to stay ahead of emerging threats and to comprehensively manage everyday organizational risks. Set out a business case that shapes the CEOs view of safety and security as a commercial investment, not a technology and/or facilities spend.

Doing a wholesale technology refresh is unlikely to receive sign-off. Instead, measure your organizational risks, and combine the intelligence with a fully costed strategic security plan and delivery roadmap. Top security executives need to build increasingly diverse strategies and roadmaps to manage existing and emerging

Security operations require clear situational awareness to identify emerging threats, and provide actionable insights during critical events.

threats. Your strategy should uniquely define or explain the nature of the security challenge for your organization. Next, clearly state the approach for dealing with your challenge. Finally, your roadmap should identify a timeline of coherent actions to address the challenge.

Having a robust security approach requires security executives to measure and report key performance indicators that matter to senior management. Examples are:

+ Number of incidents from emerging and known threats
+ Number and classification of critical events
+ Range of time to respond to incidents and critical events
+ Measurable impacts on people, facilities, assets and/or business continuity.

In addition to numbers, provide a security narrative that helps senior executives to understand the success and value of their security investments.

Keep your people, facilities and assets safe and secure, and your operations running.

A standardized user interface and common operating picture will enable security operatives to function more effectively. Standard operating procedures (SOPs) and workflows should be pre-defined and configured to establish the required level of security for emerging threats and critical events. The aim of all security operations is to keep your people, facilities and assets safe and secure, and your operations running.

Every organization evolves over time; through M&A activity, organic growth or staff changes. Furthermore, processes vary to meet new business and compliance requirements. Security is a long-term investment; a decision made today will need to support your requirements tomorrow, whatever emerging threats arise. Conducting a full organizational audit of security needs is useful to ensure you have a complete list of requirements that will future-proof your technologies and operations.

Ensuring you choose solutions that allow you an easy and cost-effective path to scale-up or down to meet your needs will reduce the risk of needing to change expensive systems a few years down the line.

Implementing the right security processes and procedures is a necessity to deal with the ever-increasing amount of data used by organizations. Silo processes and lack of technology interoperability hamper data insights. Poor data management also leads to data hacks, impacting an organization both financially and reputationally.

Information flows in quickly to security operations every day from many different internal and external sources.

Information flows in quickly to security operations every day from many different internal and external sources, and the actions needed to be taken have become more dynamic and varied. Security operations require clear situational awareness to identify emerging threats, and provide actionable insights during critical events. Automated tools enable staff to promptly manage emerging threats and critical events. Be prepared, informed and able to act when it comes to safeguarding your people, facilities and assets during critical events.

It's time to weigh your priorities and invest in the most pragmatic solution that meets your business demands.

Analyst viewpoints

The Forrester Tech Tide™: Digital Physical Security And Employee Safety, Q2 2020 states, "Today's businesses must manage an increasingly complex and challenging world of physical security challenges. These can range from unpredictable weather-related disruptions to criminal or terrorist events and the loss of physical data. All these incidents disrupt business operations, detract from employee productivity, and affect customer perceptions. The increasing severity and scope of potential security attacks requires organizations to reevaluate and reassess their current physical security posture to determine if existing plans and policies are appropriate for dealing with today's myriad of physical threats.

With so many fresh and innovation technologies entering the market, it's time to weigh your priorities and invest in the most pragmatic solution that meets your business demands."

Gartner's Hype Cycle for Physical Security, 2018 states, "Physical security is no longer a separate function from IT in today's enterprise. A forward-looking strategic investment approach toward physical security is required, and needs to be aligned with the organization's business objectives and risk priorities."

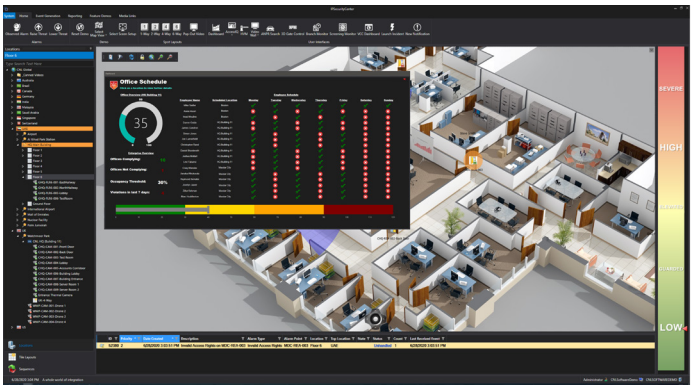
About Control Center

Control Center correlates events from disparate safety and security systems into a common operating picture to focus people's attention on what matters. The platform provides users with actionable alerts, next step actions, and automated reporting to better manage risks, ensure compliance with operating procedures and support your business continuity. Automated workflows ensure rapid, consistent responses, reducing the risk of human error. It also facilitates device activation to ensure you are always in operational control and protecting your people. Dynamic reports and dashboards provide real-time actionable insights for your operations teams and senior executives.

With Control Center...

- ✓ Control your assets with a common operating picture for real-time situational awareness
- ✓ Reduce risk through automated decision-making and compliance procedures
- ✓ Accelerate response times with automated actions and consistent next step tasks
- ✓ Avoid technology lock-ins and big-bang expenses with an open integration platform
- ✓ Prevent information overload with a powerful orchestration engine to correlate events
- ✓ Keep stakeholders informed, wherever they are, with real-time dynamic dashboard

EVERBRIDGE
CONTROL
CENTER



When it comes to complex security programs our global experience, insights and reference accounts are unparalleled. Find out how we can help you achieve your long term security management objectives by visiting **everbridge.com**.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running. With the acquisition of CNL, Everbridge has proudly unveiled new critical event capabilities focused on physical security. As a result, organizations will be able to gather a broader range of situational intelligence and automate targeted responses throughout their entire safety, security, and operational continuum – from across a global footprint to within campuses and facilities.

Everbridge serves 9 of the 10 largest U.S. cities, 8 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Kolkata, London, Oslo and Stockholm. For more information, visit www.everbridge.com, read the company blog, and follow on LinkedIn, Twitter, and Facebook.

everbridge®

VISIT WWW.EVERBRIDGE.COM

CALL +1-818-230-9700