everbridge®

10 Step Guide to **Staying Ahead of Emerging Security Threats**

This guide gathers useful insights from our experience in deploying **some of the largest and most complex security systems in the world.**

Overview

Staying ahead of security threats is paramount for top 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.

This guide gathers useful insights from top companies who have deployed some of the largest and most sophisticated security systems around the world.

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

1. Business Case

Proving value to stakeholders is a prerequisite for every top security executive.

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 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.

Your roadmap should identify a timeline of coherent actions to address the challenge.

2. Security Strategy and Roadmap

Top security executives need to build increasingly diverse strategies and roadmaps to manage existing and emerging 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.

Strong leadership skills are also 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.

Prioritize security architecture improvements aligned to the organizational strategy.

3. Security Architecture

It's unlikely that many security executives will be able to build their technology architecture from the ground up. This would be prohibitively expensive.

Strategically and conceptually architect your security stack to evolve in a managed way; making it easier to resource, deploy, and run.

The objective of evaluating the security architecture is to identify how systems become:

+ as resilient as possible,
+ interoperable,
+ open, to integrate existing and future systems and devices,
+ powered by data and insights,
+ easier to use,
+ more operationally efficient,
+ faster at responding to events,
+ more cost efficient,
+ more effective at safeguarding people, facilities assets, and,
+ more effective at ensuring business continuity.

Security decisions made today will need to support your operational requirements tomorrow.

4. Security Operations

Primarily, security operations need to be fail-safe in managing emerging threats and critical events.

When something happens, security operatives need to have comprehensive real-time situational awareness, actionable insights, fast decision-making and the ability to rapidly respond to mitigate any threat. They need complete visibility and control over all people, facilities and assets or to know that local operatives are equally equipped.

A standardized user interface and common operating framework will enable security operatives to function more effectively. Standard operating procedures (SOPs) and workflows should be pre-defined and configured to ensure the required level of security for emerging threats and critical events.

The aim of all security operations is to keep their people, facilities and assets safe, and their operations running.

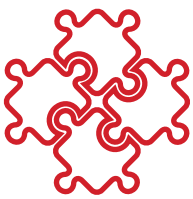
Every organization evolves over time, be it through M&A activity, organic growth or staff changes.

5. Scalability & Flexibility

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.



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

6. Data and Insights

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, and the actions needed to be taken have become more dynamic and varied.

Security operations require predictive intelligence to identify emerging threats, and 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.

Provide an understandable security narrative to senior management.

7. Measure and Report What Matters

Having a robust security business case, strategy and roadmap will require top security executives to measure and report key performance indicators that matter to senior management.

Examples of key performance indicators are:

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

In addition to using numbers, provide an understandable security narrative to senior management that helps them understand the success and value of their security investments.

The purpose of a safety and security aware culture is to prioritize the security agenda across the organization.

8. Establish Partnerships with Key Stakeholders

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.

Engaging the CEO in a security business case and getting sign-off becomes important when engaging your organization more broadly. If the CEO thinks and says that safety and security are important, many people will be inspired to participate.

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.

Organizations must keep track of all emerging security threats.

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

9. Emerging Threats

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 them from harming your people or disrupting your operations.

10. Everbridge Control Center

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.

Control Center from Everbridge, is a physical security platform that is trusted by leading organizations around the world where safety and security are mission-critical.

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