The CEO's Security Transformation Playbook

The CEO's Security Transformation Playbook

Every CEO has a responsibility to consider how they manage security within their enterprise: to safeguard employees, facilities and assets while ensuring business continuity.

Leading an enterprise today is not for the faint-hearted and therefore, proactively managing security needs an informed and decisive CEO.

Enterprise Security Risk Management: A Strategic Imperative

CEOs have a continually growing list of priorities for board level discussion, and cybersecurity is one boardroom topic that has become increasingly important. However, cybersecurity is only one aspect of a much broader security topic: enterprise security risk management.

CEOs manage extensive customer footfall through retail banks, stores, transport and transport facilities. They also manage extensive physical assets in the form of facilities, offices and factories. Some CEOs manage critical national infrastructure such as refineries, energy facilities or communications networks. All these assets face increasingly credible disruptive forces to people and facilities. Therefore, every CEO should view safety and security as a strategic imperative. Otherwise, they may experience economic, environmental, geopolitical, societal or technological disruptions. It is important not to oversimplify the safety and security management narrative, as threats are progressing faster than enterprises can adapt.

Security Transformation Playbook

Successful security playbooks exist to help showcase value and effectiveness to stakeholders. Enterprises need to build increasingly diverse strategies, tactics and teams to handle their disparate risk factors. The Security Transformation Playbook helps most CEOs to drive significant change within their enterprise. At the heart of the transformation is how an organization's enterprise security risk management strategy can accelerate business growth while managing risks.

Few CEOs will have a background in risk management or security, and therefore, may feel uncomfortable pushing a security transformation agenda. Enterprise security is a commercial investment, not a technology and/or facilities spend. The CEO can fully align security tactics to the enterprise strategy. The CEO can set the right course with a fully costed business case and can chart progress, while sending a message throughout the organization of the intent to transform their approach to enterprise security.

There is no single organizational security playbook; the CEO and their team must diagnose their enterprise's unique internal and external challenges. This creates different policies and actions for each company to be able to deal with their strategic challenges. However, five examples of security challenges all CEO's face are:

- Reducing operational costs through technology automation. Avoiding expensive rip-and-replace technology projects and reducing staffing needs with automation enhancements.
- Preventing and managing critical events efficiently and effectively to mitigate business disruptions. Enhancing operational resilience to be able to respond,

adapt, recover and learn from critical events as they happen.

- Reducing risk to safely and securely manage people in your facilities: e.g. using access control, building, and facilities management systems to heat map people's use of facilities to rationalize resources, while enhancing safety and reducing operational costs.
- Increasing operational effectiveness while reducing operational costs. During any critical event, a flood of information flows into the organization which can be overwhelming. Reducing the noise and focusing people's attention on what needs to be done immediately through automating decision-making and compliance procedures, accelerates response times and mitigates business impacts.
- Driving digital transformation and innovation to build an organization that is adaptable to critical events as they happen. Preparing for predictably unpredictable future crises.

Inspiring a Security Culture and a Successful Security Transformation Program

Transformation agendas are often hampered by most organizations' instinctive resistance to change. The purpose of a Security Transformation Playbook is to prioritize security across the enterprise and establish how colleagues can contribute to driving transformation. This helps reinforce a culture of change and shows that change is necessary. In an uncertain globalized world with a growing number of risks, employees are motivated by a CEO that emphasizes the importance of proactively protecting employees and the environment in which they live and work.

Once the strategy is created, revising the security operational blueprint is likely to be required for creating a common operating picture that works effectively in practice. The CEO and their teams need to organize and manage resources to achieve the security transformation. Ineffective silo processes and lack of technology interoperability will hamper the effectiveness of employees; and will inevitably lead to a strategy implementation gap and a failed security transformation program.

Today's global security operations demand converged digital and physical capabilities. Within any enterprise's security ecosystem the convergence reality may be more complex than many CEOs realize. Digital capabilities may sit in physical assets, such as sensors inside fire systems and alarms and CCTV that send data to command and control centers. It is illogical to view digital and physical security as mutually exclusive. Therefore, cybersecurity and physical security should be assigned equal boardroom importance through a converged common operating picture at a global, regional and local level.

The common operating picture may mean an enterprise has core security capabilities, such as visualization and communications that are powered by actionable insights. An additional integration service layer would utilize add-on capabilities and features that would mean technology could evolve more easily.

Security operations should deliver consistent treatment of incidents, emergencies and crises and allow more standardized insights to be delivered to the boardroom.

The overriding purpose of a robust security strategy is to drive security technology and process transformation that is fully adopted across the enterprise and makes commercial sense.

Quantifying Security Impacts in a Business Context

It is time to ensure that safety and security are regular boardroom topics. The discussion should be as insightful and quantifiable as all other commercial discussions where investments and benefits are relevant to boardroom members.

Ultimately, safeguarding people, facilities and assets while ensuring business continuity are everyday CEO concerns.

Let's Chat

Do you have questions? Would you like to know more about Everbridge?
Get in touch or just call us at +1-818-230-9700 to learn more.

ABOUT EVERBRIDGE

Everbridge, Inc. (NASDAQ: EVBG) is the global leader in critical event management and enterprise safety software applications that automate and accelerate an organization's operational response to critical events in order to keep people safe and businesses running. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Kolkata, London, Oslo, Singapore, and Stockholm.

everbridge®

VISIT WWW.EVERBRIDGE.COM
CALL +1-818-230-9700