everbridge®

WHITE PAPER

Bridging the Digital & Physical

A UNIFIED APPROACH TO CRITICAL EVENT MANAGEMENT

To achieve maximum resilience, organizations must recognize that **digital and physical environments are becoming inextricably connected to one another** - and must embrace a more holistic approach to protect them.

A case needs to be made for the unification of managing risk and response across both digital and physical environments.

For many, digital and physical environments have been considered as standalone entities requiring separate and unique handling. Because of this, businesses have historically built and authorized separate teams to manage response to critical events that may affect either their digital or physical environments.

However, treating these environments separately results in organizational silos that negatively impact resilience in the face of a critical event.

Isolating the digital and physical from one another often leads to two, or more, teams that begin operating with different tool sets, priorities, and processes. The separation of digital and physical response teams can even lead to contradictory messaging, which diminishes trust.

A case needs to be made for the unification of managing risk and response across both digital and physical environments within one centralized "fusion center". Especially in our current threat landscape that can produce far from isolated disruptions, resilience and success is achieved from the breakdown of siloed response activity.

To achieve maximum resilience, organizations must recognize that digital and physical environments are becoming inextricably connected to one another - and must embrace a more holistic approach to protect them.

Managing risk under one unified platform, or "fusion center," results in streamlined communications and response, faster remediation of disruptions, and ultimately reduced impact to business continuity.

Connecting previously independent teams to a unified system standardizes process and ensures incidents are transparently communicated, while enabling anyone and everyone to understand how the incident affects their team and business in general.

Breaking Down the Wall Between Physical and Digital Teams

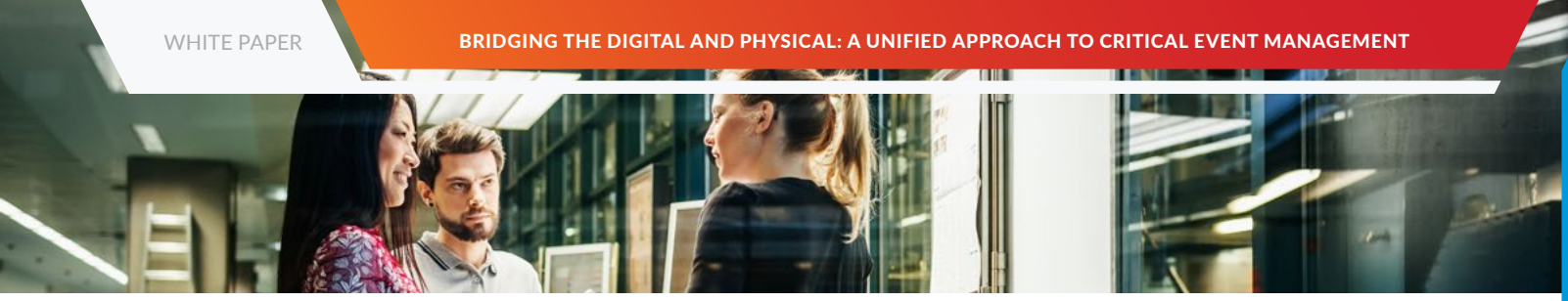
Those charged with safeguarding physical environments might include teams such as:

- **Security**
- **Human Resources**
- **Corporate Communications**
- **Crisis and Business Continuity Teams**

These teams are tasked with creating policies and procedures to best protect physical environments. This includes enforcing security models with multi-tiered perimeter and internal defences to protect employees, facilities, equipment, and resources from potentially damaging or harmful events such as severe weather, terrorist attacks, or crime.

A key component to successfully responding to a physical threat has often been based on proximity. Being near to the actual event has allowed organizations to understand the exact nature of the risk they may be dealing with, answering questions such as:

+ What assets, people, buildings, or facilities may be impacted?
+ What is the location of potentially impacted people & those who can assist in responding?
+ Are supply chains disrupted?
+ What communications are necessary to send to employees, stakeholders, and customers?
+ Is brand image or reputation at risk?



They can then determine whether this is a facilities issue impacting the useability of a workspace, an external event such as severe weather impacting people's ability to access the office or plant, or a threat to life and safety.

However, it is no longer an absolute necessity to be in the physical place where a critical event occurs to identify most answers to these vital questions. What is important is that designated on-the-ground teams have access to a system that connects them to the organization at large. This way, headquartered teams can properly provide instruction of exactly what is happening and how to proceed when a disruption occurs. Additionally, those on the ground can respond back to headquarters with progress reports.

Furthermore, impact to physical environments may also cause impact to digital environments and visa-versa. Teams need transparency and collaboration abilities to better investigate, detect, respond to, and remediate disruptions.

For example, when a system outage occurs due to severe weather it can appear there is a single amorphous IT organization that is responsible for resolving the issue within a single service level agreement. However, it is much more complex than that. Various teams may have been tasked with different responsibilities and possess different skill sets and knowledge about the incident.

Connecting previously independent teams to a unified system standardizes process and ensures incidents are transparently communicated, while enabling anyone and everyone to understand how the incident affects their team and business in general. Furthermore, it allows all teams to proceed in unity with the clarity and assurance that a set protocol for remediation is being followed.

Without proper planning and management, a critical event can disrupt business continuity and lead to devastating consequences.

The Physical is Now Digital

More and more, our physical systems have digital components. The world of the Internet of Things (IoT) is here, with an expected 75 million connected devices by 2025. The Internet powers everything from health devices to banking systems to household appliances but being connected also introduces additional risk. A cyber-attack can now have real, physical implications.

Stakeholders, customers, shareholders, suppliers all expect businesses to be running. Banking customers expect to be able to access their funds. Suppliers expect orders. Customers expect to be able to purchase merchandise regardless of a critical event. Without proper planning and management, a critical event can disrupt business continuity and lead to devastating consequences.

The Real Impact of Digital Attacks on Physical Environments

When DarkSide deployed a ransomware cyberattack against Colonial Pipeline, even they did not expect the pipeline to be taken down. They said: "Our goal is to make money and not create problems for society." While steps were taken, including the issuing of emergency legislation by the US government, this is an example of where the physical and digital worlds collided and created real world impacts that affected people and businesses. The attack cost Colonial a $5 million ransom and the country and people significantly more.

The Irish Health Service recently suffered a cyber-attack on its computer systems, described by a minister as "possibly the most significant cybercrime attack on the Irish state." This resulted in the temporary shutdown of their IT systems, causing a significant impact to patient care. Appointments were cancelled and long delays were forced upon those who needed care.

It is no longer the case that attacks on digital environments remain isolated within that realm. Digital attacks have the potential to affect our physical experiences and environments, often more so than even intended.

It is no longer the case that attacks on digital environments remain isolated within that realm. Digital attacks have the potential to affect our physical experiences and environments, often more so than even intended.

There are many other examples, from hackers targeting electricity grid operators in India to others attempting to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida. It is estimated there is a cyber-attack every 39 seconds on average; since COVID-19, the US FBI has reported a 300% increase in reported cybercrimes as hackers leverage the opportunity to attack vulnerable home networks and leverage communications related to COVID-19 as bait.

All of these examples highlight the risk ransomware can pose to citizens, businesses, and to the critical national industrial infrastructure. These threats only continue to increase in both scale and frequency. Today, those engaged with cybercrime operate as a business. This is a world apart from the stereotypical view of hackers often perceived as shadowy, secretive, and working alone.

Such calculated and powerful attacks require businesses to be just as intelligent in their protections. The combination of the monetization and transformation of hacking into a business, the expansion of remote working accelerated dramatically by the Covid-19 pandemic, and the increase in IoT devices means that businesses must bring digital transformation to physical security.

To ensure the effectiveness and efficiency of the fusion center, technology to facilitate and automate the response needs to be in place.

The Solution

Increasingly organizations are combining the 24x7 response function of business continuity, physical security, cyber security and crisis management in what is commonly called a “fusion center,” “joint information center” or “centralized incident response team.” The goal of the fusion center is to provide a centralized response team with the resources, expertise, and information needed to detect, prevent, and minimize the business impact and disruption of critical events.

To ensure the effectiveness and efficiency of the fusion center, technology to facilitate and automate the response needs to be in place. Organizations need a single technology solution that enables all teams to effectively:

+ Assess and understand the situation and potential impact
+ Locate affected employees, stakeholders, assets, or facilities regardless of whether they belong to physical or digital systems
+ Take action by automatically identifying and deploying the correct response teams and empowering them with standard operating procedures
+ Run books allowing for post incident reporting and analysis to help improve processes in the future

With Everbridge’s Critical Event Management for Digital and Cyber Incident solution, organizations are empowered to build remarkable customer experiences while protecting against service disruptions. Development teams can rapidly iterate to create new and exciting innovations. Physical safety and digital security operations are integrated into a single pane of glass, enabling a proactive cybersecurity posture while providing uninterrupted services.

Let’s Talk

Want to learn more about Everbridge Critical Event Management? Get in touch or just call us at +1-818-230-9700 to learn more.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications for automating and accelerating an organizations' operational response to critical events in order to Keep People Safe and Organizations Running™. During public safety threats such as active shooter situations, terrorist attacks, a global pandemic or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,800 global customers rely on the Company's Critical Event Management (CEM) Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication modalities, and track progress on executing response plans. Everbridge serves 8 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, 47 of the 50 busiest North American airports, 9 of the 10 largest global consulting firms, 8 of the 10 largest global automakers, 9 of the 10 largest U.S.-based health care providers, and 7 of the 10 largest technology companies in the world. Everbridge is based in Boston with additional offices in 25 cities around the globe.

For more information visit **everbridge.com**, read the company **blog**, and follow us on **LinkedIn** and **Twitter**.

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

 |