ONTIC®

Whitepaper

Managing Through Change: How Increased Cyber-Physical Security Threats Will Impact Companies

By The Ontic Center for Protective Intelligence

GARTNER PREDICTS 75% OF CEOS WILL BE PERSONALLY LIABLE for cyber-physical security incidents by 2024 and the financial impact of cyber-physical attacks resulting in fatal casualties will reach over $50 billion by 2023.

When it comes to enterprise security, it often takes a tragedy or a threat too close for comfort to drive needed change to industry practices. Corporate security teams have a long history of treating the physical world and the cyber domain as distant relatives despite the fact that in today's hyper-connected world, managing cyber-physical security threats collaboratively is no longer a nice to have but an imperative.

In order to fully comprehend the risk of treating the two security functions as separate units, it's important to consider the following:

- **CURRENT THREAT ENVIRONMENT**
  What is the impact of remote and hybrid work on the threat landscape
- **LESSONS FROM CYBER-PHYSICAL INTELLIGENCE FAILURES**
  What we can take away from recent intelligence failures from cyber and physical systems being treated separately
- **ENTERPRISE SECURITY ORGANIZATIONAL STRUCTURE**
  Rethinking the organizational structure and shifting the mindset to converge all threat data under one umbrella
- **URGENCY AND GOALS FOR A STRONGER SYSTEM**
  Data supporting the need for a unified, more proactive approach to assessing threats

> *"To dismiss one area of security puts the other at risk."*
>
> *Thomas Kopecky*
> *Co-Founder and*
> *Chief Strategy Officer, Ontic*

The Indisputable Rise in Threat Activity

Companies are dealing with and reacting to new and emerging threats around the globe, and the headlines have become impossible to ignore. In fact, 78% of security, legal and compliance leaders agree that the dramatic change and expansion of the physical threat landscape has created an **exponential increase in data and pre-incident indicators that are unmanageable.** (Ontic, 2021) These incidents overlap into the physical and cyber domains and — more often than not — feel like a tidal wave of information that provides security teams with little guidance on what to act on first and how.

As corporate settings have evolved to incorporate remote and/or hybrid work, the threat landscape now includes risks beyond the office walls. Here's what the data has revealed:

74%
OF SECURITY AND IT LEADERS
anticipate significant conflicts between management and employees regarding health and safety protocols, as well as work-from-home policies when businesses reopen.*

33%
OF SECURITY AND IT LEADERS
agree that as a result of intelligence failures, incidents such as employees being threatened or harmed while working at company facilities (33%) or working remotely (28%) have already occurred at their company.*

63%
OF US CYBERSECURITY PROFESSIONALS
said attacks increased due to employees working remotely.**

* Ontic's 2021 Mid-Year Outlook State of Protective Intelligence Report ** VMware's 2021 Global Security Insights Report

The amount of incoming data and intelligence has also grown alongside the expanding threat landscape. **Security analysts today face a daunting task of reviewing massive amounts of data — a daily volume projected to grow to 2 million words by 2025, 10 times the 200,000 words they read today,** according to Aberdeen Group (2021).

Learning from Cyber-Physical Intelligence Failures

There are many recent examples of cyber and physical systems not working as one, resulting in repercussions related to safety, business continuity and brand perception. It's important to take time to review cyber-physical intelligence failures to learn from the past and to establish a more proactive and preventative approach.

Two recent cyber-physical intelligence failures include:

1

Oldsmar, Florida's water treatment system

In early 2021, a hacker remotely accessed the Oldsmar, Florida water treatment plant computer system. In the attack, the threat actors attempted to increase the amount of sodium hydroxide in the water supply to potentially dangerous levels. While the method for the attack was cyber, had it not been caught, thousands of people could have been harmed by drinking that water.

2

Colonial Pipeline

In mid-2021, there was a ransomware attack on the Colonial Pipeline. The impact was far-reaching as it is one of the nation's largest pipelines, carrying refined gasoline and jet fuel from Texas up the East Coast. The cyberattack provoked a shutdown for five days, leading to temporary fuel shortages along the East Coast. While no individuals were harmed, the economic impact of an event like this could be staggering. With gas prices going up, so will the cost of other goods and services as gasoline surcharges are taken into account when shipping and transporting items.

NEW THREAT

Many large technology companies are cutting pay for remote employees who move to less expensive areas, which presents a new cause for concern for corporate security teams managing dispersed workforces.

What can we take away from this?
Siloed operations are endemic to the corporate world, across nearly all functions. So it shouldn't surprise anyone that security teams focused on the physical and cyber realm might not collaborate — or even speak the same language.

Systems that straddle the physical and cyber domains require that security professionals shift their mindsets. Today, IT systems affect physical outcomes and corporations must be able to appropriately handle the convergence of these threats.

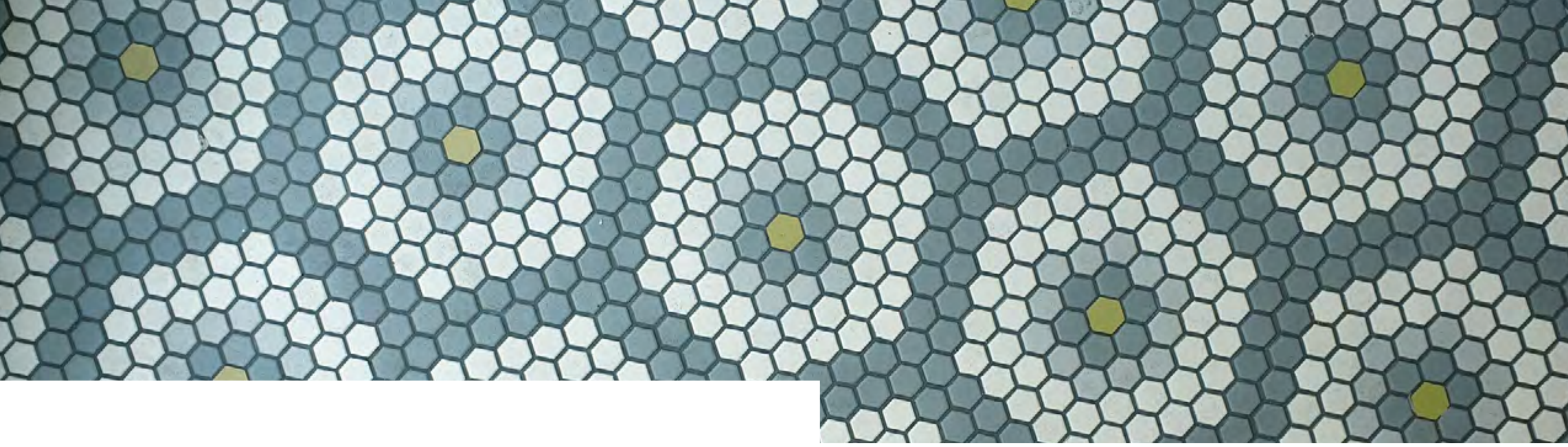
As any experienced practitioner knows, you only have control over a limited number of variables, and being prepared for high likelihood / high impact events is essential. While many cyber-threats stem from insiders, especially those involving infrastructure, the determination of external threat actors outside of your organization cannot be overlooked.

Taking the step to unify information under one view can facilitate communication and collaboration amongst corporate security teams, preventing these devastating attacks in the first place and ensuring that organizations are better prepared to handle incidents if and when they occur. What's more, having consistent and regularly evaluated security controls to address both physical and cyber threats is critical.

*

Physical security and cybersecurity are intrinsically connected

It is no longer effective to manage these threats separately. Cyber-physical incidents can quickly lead to physical harm, destruction of property, environmental disasters, and worse — all signs point to an increase in these destructive threats.



A Revised Enterprise Security Organizational Structure

While external threat hunting is usually known to fall under the purview of network security teams, insider threats are typically the responsibility of physical security teams that bring an intelligence-driven approach. That's why it's imperative for security teams to view protection from a converged point of view, especially as cyber-physical systems address a new set of risks that few security and risk leaders have had to consider.

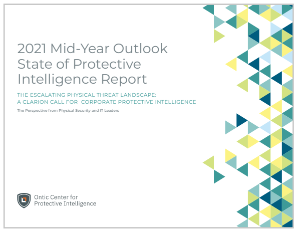
This revised structure of viewing cyber and physical threat activity under one roof allows organizations to assess the physical security controls at their facilities and ensure that they are proactively hunting for threats that may disrupt operations (e.g. pattern analysis). What's more, it is imperative to acknowledge the role of hardware and IoT devices in corporate security (e.g. smart devices) as a gateway for cyber-physical threats, and executives are especially vulnerable.

GARTNER PREDICTS THAT BY 2025, 50% of asset-intensive organizations such as utilities, resources, and manufacturing firms will converge their cyber, physical, and supply chain security teams under one chief security officer role.

Final Thoughts: The Urgency for a Stronger System

With a digital transformation underway in a majority of global corporations, there is tremendous opportunity for aligning cybersecurity infrastructure with physical security operations. Bringing together all threat data and intelligence with a technology-driven approach has turned into a 'must-have' for corporations to anticipate risk events. Our 2021 Mid-Year Outlook State of Protective Intelligence Report shares the collective views from 300 physical security and IT leaders, and it's clear that enterprise companies are prioritizing this shift in mindset:

ONTIC'S 2021 MID-YEAR OUTLOOK STATE OF PROTECTIVE INTELLIGENCE REPORT



2021 Mid-Year Outlook State of Protective Intelligence Report

THE ESCALATING PHYSICAL THREAT LANDSCAPE: A CLARION CALL FOR CORPORATE PROTECTIVE INTELLIGENCE

The Perspective from Physical Security and IT Leaders

Ontic Center for Protective Intelligence

2021 Mid-Year Outlook State of Protective Intelligence Report

PHYSICAL SECURITY AND IT LEADERS AGREE:

74% Given the current environment, I am under more pressure than ever before to keep my company's CEO and our employees safe.

59% As a result of expressing a position on racial and/or political issues, my company's employees have received physical threats.

58% As a result of expressing a position on racial and/or political issues, my CEO has received physical threats.

56% As a result of encouraging vaccinations and mask use, my CEO has received physical threats.

40% As a result of not expressing a position on racial and/or political issues, my CEO has received physical threats.

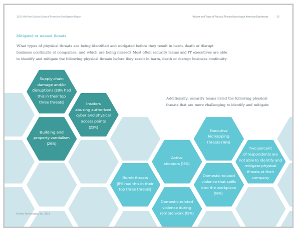
© Ontic Technologies, Inc. 2021

Escalating Physical Threats, Harm Are Corporate Concerns as U.S. Reopens 09

Double-edged sword for CEOs

As activism around social justice and geopolitical issues took center stage, some CEOs vocalized stances publicly while others have refrained. Both of these actions have spurred physical security threats against CEOs, as has voicing concerns about extremists, encouraging vaccinations and mask use. Given the current environment, Physical Security and IT leaders agree **they are under more pressure than ever before to keep their company's CEO and employees safe.**

More than half of all respondents agree their CEO has received physical threats both as a result of either expressing (58%) or not expressing (40%) a position on racial and/or political issues. More than one-third (35%) agree that their CEO's expressing concern publicly about extremists has resulted in new physical security threats, and nearly the same amount (33%) agree their company has experienced an increase in physical threats and backlash tied to extremism, racial justice and political issues. Over half (56%) also agree their CEO has received physical threats as a result of encouraging vaccinations and mask use.



2021 Mid-Year Outlook State of Protective Intelligence Report

Volume and Types of Physical Threats Occurring at American Businesses 15

Mitigated or missed threats

What types of physical threats are being identified and mitigated before they result in harm, death or disrupt business continuity at companies, and which are being missed? Most often security teams and IT executives are able to identify and mitigate the following physical threats before they result in harm, death or disrupt business continuity:

Supply chain damage and/or disruptions (28% had this in their top three threats)

Insiders abusing authorized cyber and physical access points (23%)

Building and property vandalism (26%)

Additionally, security teams listed the following physical threats that are more challenging to identify and mitigate:

Executive kidnapping threats (16%)

Active shooters (15%)

Two percent of respondents are not able to identify and mitigate physical threats at their company

Bomb threats (8% had this in their top three threats)

Domestic-related violence that spills into the workplace (16%)

Domestic-related violence during remote work (15%)

© Ontic Technologies, Inc. 2021

Equal funding of cyber and physical security
As people begin to return to the office and also continue to work remotely, nearly half (48%) of physical security and IT leaders say it is more urgent than it was at the beginning of 2021 that funding for physical security and cyber security technology solutions is allocated at the same levels.

Evaluating pre-incident indicators
The vast majority surveyed say most (37%), some (29%) or all (11%) of the physical threats their company has received this year originated as a cyber-threat. Pre-incident indicators (or threats) first appeared in cyber auditing tools, email, on social media, in antivirus software via a cyber-breach or ransomware attack.

A unified view and mindset
Of the physical threats that have resulted in harm or death at their company this year, respondents say almost all or most (49%) could have been avoided if cybersecurity and physical security intelligence were unified so threats could be shared and actioned by cross-functional teams.

PREVENTING NEGATIVE FINANCIAL IMPACT

Attacks against data centers can cost millions of dollars for data center operators. The impact on their clients could be much greater in terms of downtime and lost opportunities.

Having stronger barriers against cyber attacks and evolving protocols as threat actors mature their tactics is necessary, but providing this information to the broader enterprise security team will allow the organization to more effectively see around corners and get ahead of threats.

At Ontic, we believe that businesses like yours can be safer by serving intelligence to those who protect. Visit the Center of Protective Intelligence to learn more.

Learn More

Let’s make nothing happen together™

Ontic is the first protective intelligence software company to digitally transform how Fortune 500 and emerging enterprises proactively address physical threat management to protect employees, customers and assets. Ontic’s SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge so companies can assess and action more to maintain business continuity and reduce financial impact. Ontic also provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals at major corporations via its Center for Protective Intelligence.

To learn more about Ontic's Protective Intelligence Platform, contact us at info@ontic.ai

ONTIC®