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

EXECUTIVE SUMMARY

As vaccinations continue, employees return to the office, companies embrace hybrid work and the U.S. opens up and emerges from the pandemic, violence and physical threats to businesses are occurring at an unsettling, record-high pace. Pent up economic and political frustrations marked at the year's outset by the January 6 Capitol riot have been exacerbated by months of limits on in-person interactions and social distancing mandates. By the end of June, 317 mass shootings took place in the U.S in 2021, up 27% from the same point in 2020 and 59% from the same point in 2019.[1]

Accelerated by COVID-19 and an increasing volume of threats, corporate physical security and cybersecurity teams — often divided functions with physical security lagging in investing in and adopting modern tools and technologies — are rapidly coming together in terms of funding and the mindset that they must be inextricably connected to prevent devastating harm to their companies. A rash of cyber attacks shutting down critical industry supply chains and infrastructure is heightening concern and action within companies. So much so, the Biden administration publicly urged corporate executives and business leaders to discuss the implications:

> "To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat."[2]

1 - Gun Violence Archive (GVA) Mass Shooting Data — January-June 30 for 2021, 2020, 2019. GVA defines mass shootings as having a minimum of four victims shot, either injured or killed, not including any shooter who may also have been killed or injured in the incident.

2 - June 2, 2021 memo issued by the White House to corporate executives and business leaders from Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

Despite these events, corporate leaders are reluctant to believe their companies could be physical threat targets. But in the current powder keg of elevated political and social tensions, suppressed anger and grievances held at bay during the pandemic are being unleashed. These physical threats are anticipated to only grow as companies bring employees back to reopened offices and communicate health protocols and policies perceived by some as egregious and invasive.

As corporations advance the digital transformation of their physical security operations, it has never been more important to seize the opportunity to align their cybersecurity operations and infrastructure. Bringing together all threat data and intelligence in an always-on technology-driven approach to security is the most effective way to advance business continuity in today's increasingly hyper-connected, hyper-violent environment.

PRO·TECT·IVE IN·TEL·LI·GENCE

Protective intelligence is an investigative and analytical process used by protectors to proactively identify, assess, and mitigate threats to protectees.

The Ontic Center for Protective Intelligence commissioned a mid-year survey of 300 physical security directors, physical security decision-makers, chief security officers, chief information officers, chief technology officers, chief information security officers and IT leaders at U.S. companies with over 5,000 employees to examine how physical security challenges and opportunities are unfolding in 2021 as America emerges from the pandemic.

In this report, we explore the study findings in further detail and expose the severity of the physical threat landscape, as well as its far-reaching human and business costs. We hope to inform the need for both physical security and cybersecurity leaders to immediately stand up a proactive protective intelligence strategy to fundamentally transform and strengthen security across the organization.

OUR MID-YEAR SURVEY SURFACED THESE KEY TAKEAWAYS:

1. **THREATS ARE IMPACTING BUSINESS CONTINUITY** Since the beginning of 2021, unmanaged and rising physical threats are increasing corporate risk, financially crippling and negatively impacting business continuity. Companies need an immediate and consistent investment in technology to advance physical security effectiveness and mitigate violent threats. Given the situation has become more urgent so early in the year, companies must invest in a proactive approach.

2. **THE THREAT LANDSCAPE IS EXPANDING** Intelligence failures at U.S. companies are a regular occurrence, resulting in CEOs, their family members and employees being threatened and/or harmed, active shooters, and insiders abusing authorized cyber access leading to supply chain damage or property theft.

3. **LACK OF UNIFICATION IS DETRIMENTAL** Of the physical threats that resulted in harm or death at companies in 2021, security and IT leaders think most or almost all could have been avoided if cybersecurity and physical security intelligence were unified — a single platform for identifying threats, investigations, data and analytics — so threats could be shared and actioned by cross-functional teams.

4. **BIGGEST CHALLENGES ARE UNEXPECTED** Physical security leaders shared what they expected to be their biggest physical security challenges in 2021 in the inaugural 2021 State of Protective Intelligence Report study conducted October 2020. But seven months later as they struggle to effectively assess physical threats, dealing with regulation and compliance reporting and demonstrating a return on physical security investment are some of the biggest challenges they did not expect in 2021.

CONTENTS

2021 Mid-Year Outlook
State of Protective Intelligence Report

06 Section 01
ESCALATING PHYSICAL THREATS, HARM ARE CORPORATE CONCERNS AS U.S. REOPENS

12 Section 02
VOLUME AND TYPES OF PHYSICAL THREATS OCCURRING AT AMERICAN BUSINESSES

16 Section 03
THE CASE FOR PROTECTIVE INTELLIGENCE AND CYBER-PHYSICAL SECURITY CONVERGENCE

25 Section 04
PHYSICAL SECURITY INVESTMENT PRIORITY ACCELERATION

Section 01

ESCALATING PHYSICAL THREATS, HARM ARE CORPORATE CONCERNS AS U.S. REOPENS

Physical threats are rising, unmanageable and missed because of protective intelligence failures.

Companies are experiencing an increase in physical threat activity as compared to the beginning of 2021. The physical threat landscape has dramatically changed and expanded, which has created an exponential increase in data and pre-incident indicators that are unmanageable. In the first few months of 2021 following the January 6 Capitol riot and uptick in mass shootings, the lack of unified digital protective intelligence has resulted in missed threats and physical harm to employees, customers and people at U.S. businesses.

In fact, as the U.S. reopened from the pandemic, from March through May 2021, the string of mass shootings was one of the worst on record, matching the highest three-month total going back to 1966.[3] It's no wonder, then, that **65% of physical security leaders feel less prepared to do their jobs now as compared to the beginning of the year.**

3 - Wall Street Journal, "Recent Spate of Mass Shootings Is Among Worst in U.S. History", — June 8, 2021

PHYSICAL SECURITY AND IT LEADERS AGREE, COMPARED TO THE BEGINNING OF 2021

71%

The physical threat landscape has dramatically changed and expanded, which has created an exponential increase in data and pre-incident indicators that are unmanageable.

69%

In the first few months of 2021, the lack of unified digital protective intelligence has resulted in missed threats and physical harm to employees, customers and human assets for my company.

64%

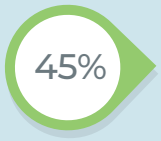
My company is experiencing an increase in physical threat activity.

58%

I feel less prepared to handle physical security for my company.

Following the January 6 Capitol riot and uptick in mass shootings, CEOs and corporate leaders mandated that new measures to increase physical security be implemented, allocated additional funds for expanding Physical Security headcount, digital tools and training to keep their companies safe, and companies significantly increased active social media monitoring of extremist views and physical threats.

THINKING ABOUT TODAY'S CLIMATE, PHYSICAL SECURITY AND IT LEADERS AGREE *

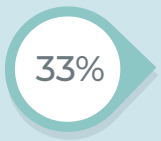


My company's CEO or leadership mandated and allocated additional funds for expanding Physical Security headcount, digital tools and training to keep our company safe.

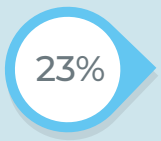
My company's CEO or leadership mandated that our company implement new measures to increase physical security.

My company has significantly increased its active monitoring of extremist views and physical threats on social media.

My company's CEO or leadership has publicly expressed concern about physical security related to extremists that has resulted in new physical security threats.



My company has experienced an increase in physical threats and backlash tied to extremism, racial justice and political issues.



My company has experienced failures in protective intelligence communications that have resulted in missed physical threats and harm to employees.

* Responses to survey question: When thinking about your company's physical security operations following the January 6 Capitol riot and the recent uptick in mass shootings, with which of the following statements do you agree?

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.

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.**

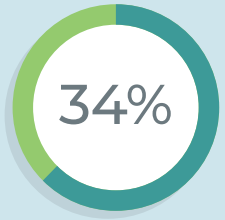
More than half of all respondents agree their CEO has received physical threats both as a result of either expressing (58%) or not expressing (40%) a position on racial and/or political issues. More than one-third (35%) agree that their CEO's expressing concern publicly about extremists has resulted 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.

Intelligence failures led to harm and threats to CEOs, employees, theft, supply chain damage and active shooter events ... and it will happen again.

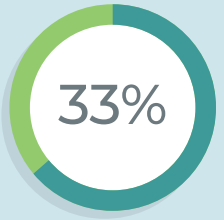
As a result of intelligence failures since the beginning of 2021, threats and harm to CEOs, their families, and employees have occurred both while working remotely from home and at company facilities. Those surveyed say at their company an employee was threatened and/or harmed while working at company facilities (33%), while working remotely (28%); and that a former employee threatened and/or harmed current employees (25%). Thirty-four percent say their company has experienced property theft or supply chain damage resulting from an insider abusing authorized cyber access.

Nearly one-quarter (24%) of physical security and IT leaders say their CEO and/or family members received threats and/or were harmed when working from their private residence or while traveling. An active shooter event at a company location also occurred due to intelligence failures, 18% say.

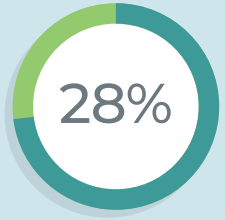
HARM, THREATS AND DAMAGE AT U.S. COMPANIES AS A RESULT OF INTELLIGENCE FAILURES (SINCE THE BEGINNING OF 2021)



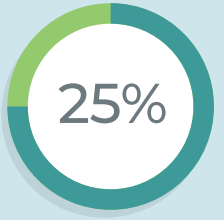
An insider abused authorized cyber access that led to property theft or supply chain damage



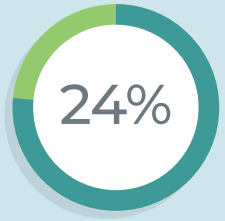
An employee was threatened and/or harmed while working at company facilities



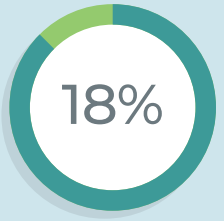
An employee was threatened and/or harmed while working remotely



A former employee threatened and/or harmed current employees



Our CEO and/or family members received threats and/or were harmed when working from their private residence or while traveling



An active shooter event occurred at one of our locations

It will never happen here: CEOs reluctant to believe their company will be a target

Despite the frequency of shootings with multiple victims, a majority of physical security and IT leaders (55%) say their CEO believes training employees so they are better prepared for potential workplace violence will create a culture of fear, and does not see the ultimate risk to business continuity. Three-quarters (75%) agree that based on the current unmanageable physical threat data, physical threats will increase exponentially as they begin to reopen and return to the office. Still, 19% say their CEO does not believe their company will ever be a target for significant physical harm and does not value employee training and preparedness for dealing with such crises.

Promisingly, more than half surveyed (51%) say they have a physical threat action plan in place and employees receive regular training. Still, 36% do training for workplace violence from time to time but have no formal program.

Vaccinations, office reopening health protocols driving physical security threats

A majority of Physical Security and IT leaders say their company has experienced physical security threats related to requiring employees to show proof of vaccination in order to return to the office (72%), and nearly three-quarters of respondents (74%) anticipate significant conflicts between management and employees regarding health and safety protocols, as well as work-from-home policies when businesses reopen.

26% of respondents say that their company has never addressed the potential for workplace violence and employees would not know what to do if an active shooter entered their facilities.

Section 02

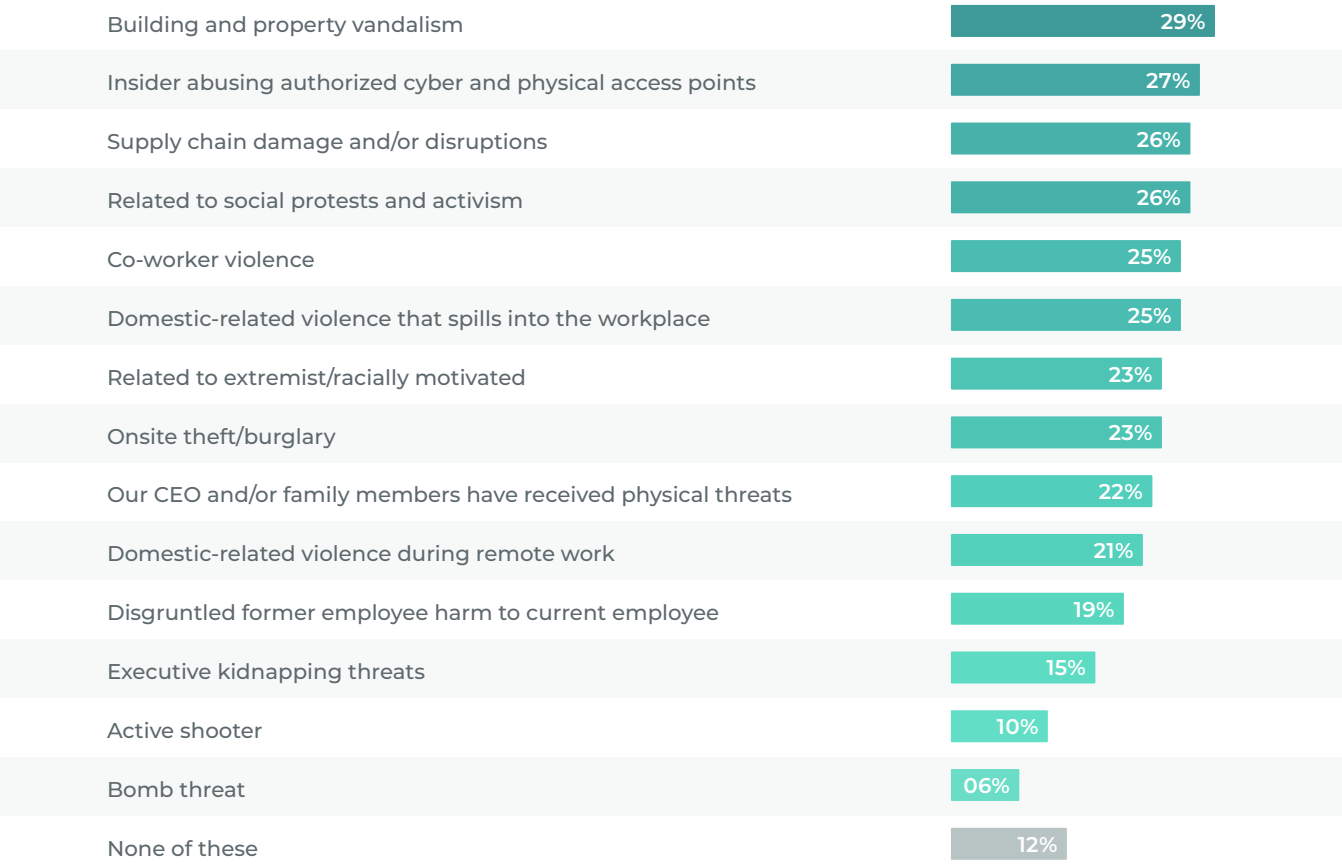
VOLUME AND TYPES OF PHYSICAL THREATS OCCURRING AT AMERICAN BUSINESSES

PERCENT WHO LIST EACH AS ONE OF THE TOP THREE PHYSICAL THREATS IN 2021

American companies on pace to receive and investigate hundreds of physical threats annually

In view of the volume, variation and growing severity of physical security threats that companies are receiving and investigating, it is understandable that leaders feel heightened pressure and the threats are unmanageable. Since the beginning of 2021, those surveyed have experienced a myriad of physical threats.

PHYSICAL THREATS EXPERIENCED SINCE THE BEGINNING OF 2021



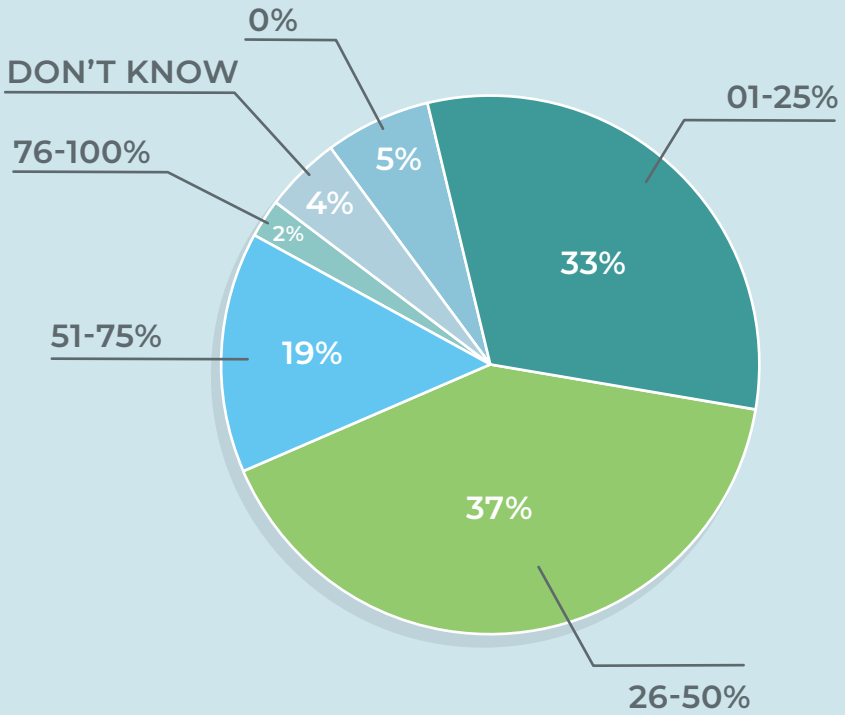
Nearly one-third of U.S. companies receiving or investigating physical security threats every week

Since the beginning of 2021, one-third of Physical Security and IT leaders say they have received or investigated at least one physical threat per week, while 21% say between two and five per week, and another 4% say over six per week. Thirty-eight percent have received or investigated less than one physical threat per week.

Companies anticipate they will miss up to 50% or more of physical threats in next six months

What should be even more concerning for companies is their ability to get ahead of or mitigate physical threats. Given their current physical security operations, 37% of Physical Security and IT leaders anticipate that in the next six months they will miss 26-50% of physical security threats while 33% anticipate they will miss 1-25% of physical security threats. Still another 19% of those surveyed anticipate missing 51-75% of physical threats.

PERCENTAGE OF PHYSICAL THREATS ANTICIPATED WILL BE MISSED AT AMERICAN COMPANIES IN NEXT 6 MONTHS



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
- Domestic-related violence that spills into the workplace (16%)
- Bomb threats (8% had this in their top three threats)
- Domestic-related violence during remote work (15%)

Section 03

THE CASE FOR PROTECTIVE INTELLIGENCE AND CYBER-PHYSICAL SECURITY CONVERGENCE

Greater urgency to unify cyber and physical security, fund them equally

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. Underpinning this sentiment may be that 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.

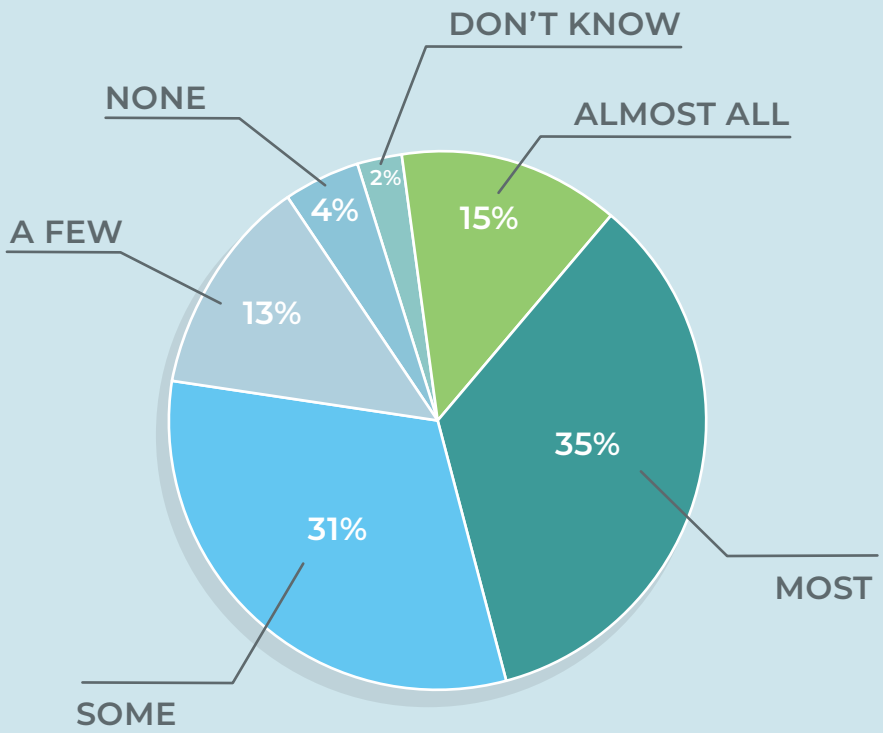
Furthermore, of the physical threats that have resulted in harm or death at their company this year, respondents say almost all (15%), most (34%), some (27%), or a few (15%) could have been avoided if cybersecurity and physical security intelligence were unified so threats could be shared and actioned by cross-functional teams.

Of the physical threats that have resulted in harm or death at your company this year, how many do you think could have been avoided if cybersecurity and physical security intelligence were unified so threats could be shared and actioned by cross-functional teams?

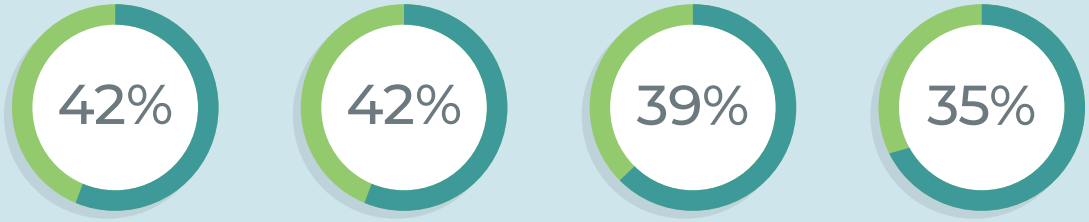
Business continuity has also been disrupted in 2021 by physical threats, but again, security and IT leaders surveyed say some (31%), most (35%) or all (15%) of those physical threats **could have been avoided** if cybersecurity and physical security intelligence were unified so threats could be shared and actioned by cross-functional teams.

PHYSICAL THREATS DISRUPTING BUSINESS CONTINUITY THAT COULD HAVE BEEN AVOIDED

Of the physical threats that have disrupted business continuity this year, how many do you think could have been avoided if cybersecurity and physical security intelligence were unified so threats could be shared and actioned by cross-functional teams?



TOP IMMEDIATE INTEGRATION AND CROSS-FUNCTIONAL COLLABORATION PRIORITIES FOR PHYSICAL SECURITY OPERATIONS (% WHO HAD EACH IN TOP THREE)

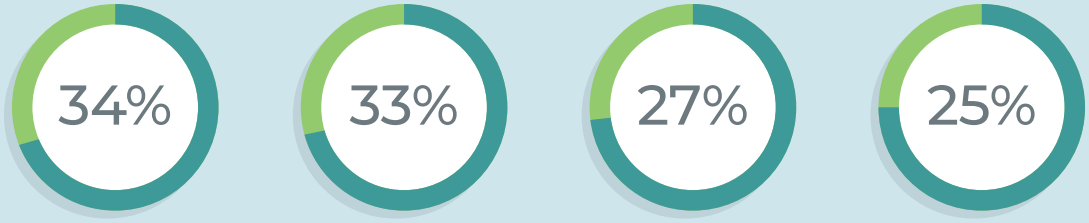


Cybersecurity alignment

Critical event management and alerting

Cross-departmental physical threat intelligence sharing / alerts

Partnering with Human Resources for employee background checks, regulatory requirements and compliance



Implementation of a company-wide crisis plan

Regular communications with Public Relations and Corporate Communications

CISO reporting structure change to encompass Cyber and Physical Security

International and domestic communications

There is overwhelming agreement among both Physical Security (95% agree, including 45% who agree strongly) **and IT professionals** (95% agree, including 55% who agree strongly) that cybersecurity and physical security must be integrated, otherwise cyber and physical threats will be missed.

What's more, 42% of those surveyed say cybersecurity alignment is among their top three immediate priorities for physical security operations integration and cross-functional collaboration, along with critical event management and alerting.

Cross-departmental physical threat intelligence sharing/alerts (39%) and partnering with HR for employee background checks, regulatory requirements and compliance (35%) are also among the top three immediate integration and cross-functional collaboration priorities.

This is also reflected in Physical Security and IT leaders' agreement with different characterizations of their company's plans to align the two functions:

Recent highly visible events are bringing new awareness to the prevalence of physical security threats that may originate on cyber channels and vice versa, and how devastating missing such signals can be. Intelligence agencies are reported to have failed to properly assess the social media chatter ahead of the Capitol riot violence, the Colonial Pipeline suspended its operations after hackers held its computer systems for ransom, and a hack contributed to the shutdown of plants that process roughly one-fifth of the nation's meat supply. In May, authorities stopped a would-be mass shooter who held extremist ideologies after they intercepted a message that he was allegedly planning a mass shooting at a major retailer. From the beginning of 2021 through June there have been 317 mass shootings with 77 recorded in June alone.[1]

1 - Gun Violence Archive (GVA) Mass Shooting Data

Some of the biggest challenges for physical security in 2021 are unexpected.

Physical Security leaders shared what they expected to be their biggest physical security challenges in 2021 in the inaugural 2021 State of Protective Intelligence Report study conducted in October 2020. But seven months later, some of their biggest challenges are those they did not expect.

Regulation and compliance reporting (33%) has risen to the top of the biggest 2021 challenges of Physical Security leaders as has benchmarking and measurement to demonstrate return on investment (27%), though these were low on the list of challenges previously expected, having been cited at 12% and 8%, respectively. Effectively assessing physical threats, however, expected by 21% to be a challenge this year, is in reality a significantly bigger 2021 challenge (35%). A potential factor could be the unexpected situation in which physical security leaders find themselves. As they continue to address a hybrid workforce, need to travel and be in multiple office locations, for nearly one-quarter (24%) of Physical Security leaders a lack of mobile capabilities in their physical threat solution is one of their biggest 2021 challenges (though only 8% previously cited it as a challenge they expected).

In yet another proof point that cyber-physical convergence is underway, only two percent of those surveyed cited launch of a Fusion Center uniting cyber and physical security as among their biggest 2021 challenges, though 19% previously expected it to be one.

Regulation and compliance reporting has risen to the top of the biggest 2021 challenges of Physical Security leaders as has benchmarking and measurement to demonstrate return on investment, though these were low on the list of challenges previously expected.

BIGGEST 2021 PHYSICAL SECURITY CHALLENGES IN 2021: EXPECTATIONS VERSUS REALITY

	BIGGEST EXPECTED PHYSICAL SECURITY CHALLENGES IN 2021 *	BIGGEST PHYSICAL SECURITY CHALLENGES IN 2021 **
Regulation and compliance reporting	12%	33%
Benchmarking and measurement to demonstrate return on investment	08%	27%
Mobile capabilities in our physical threat management solution	08%	24%
Effectively assessing physical threats	21%	35%
Former employee litigation	04%	16%
Pressure from a board, shareholders or other senior management	14%	25%
Muddled cross-company communication	17%	25%
Launch of our Fusion Center uniting cyber and physical security	19%	02%

* 2021 State of Protective Intelligence Report — October 2020 survey, 200 physical security leaders at U.S. companies

** 2021 Mid-Year Outlook State of Protective Intelligence Report — May 2021 survey, 200 physical security leaders at U.S. companies

As physical security teams continue to address their biggest challenges in 2021, the nearly unanimous sentiment (91% agree) is that they need a technology-driven industry standard for actively identifying, investigating, assessing, monitoring and managing physical security threats. Consistent with the 2021 State of Protective Intelligence Report study findings in October 2020, this continues to be way overdue.

PHYSICAL SECURITY AND IT LEADERS AGREE:

Physical security needs a technology-driven industry standard for actively identifying, investigating, assessing, monitoring and managing physical security threats, and it is way overdue.

To help mitigate potential harm from physical threat actors, it is essential that companies accelerate implementation of unified threat management platforms.

Given the unprecedented increase in the physical threat landscape, every company needs to implement threat management platforms so employees, stakeholders and regulators have confidence (and proof) they are doing everything possible to keep their people and assets from physical harm.

Among respondents' biggest 2021 physical security operations challenges are:

Among respondents' biggest 2021 physical security operations challenges are COVID-19 recovery and vaccination verifications across facilities; managing office/facilities reopenings, return and safety protocols; effectively assessing physical threats; physical security threats to remote workers, C-suite and company leadership; regulation and compliance reporting, managing physical threat data; hybrid remote working/office work structures and protocols; mobile capabilities in their physical threat management solution; among other challenges.

BIGGEST PHYSICAL SECURITY OPERATIONS CHALLENGES IN 2021 (MULTIPLE RESPONSES ALLOWED)

Section 04

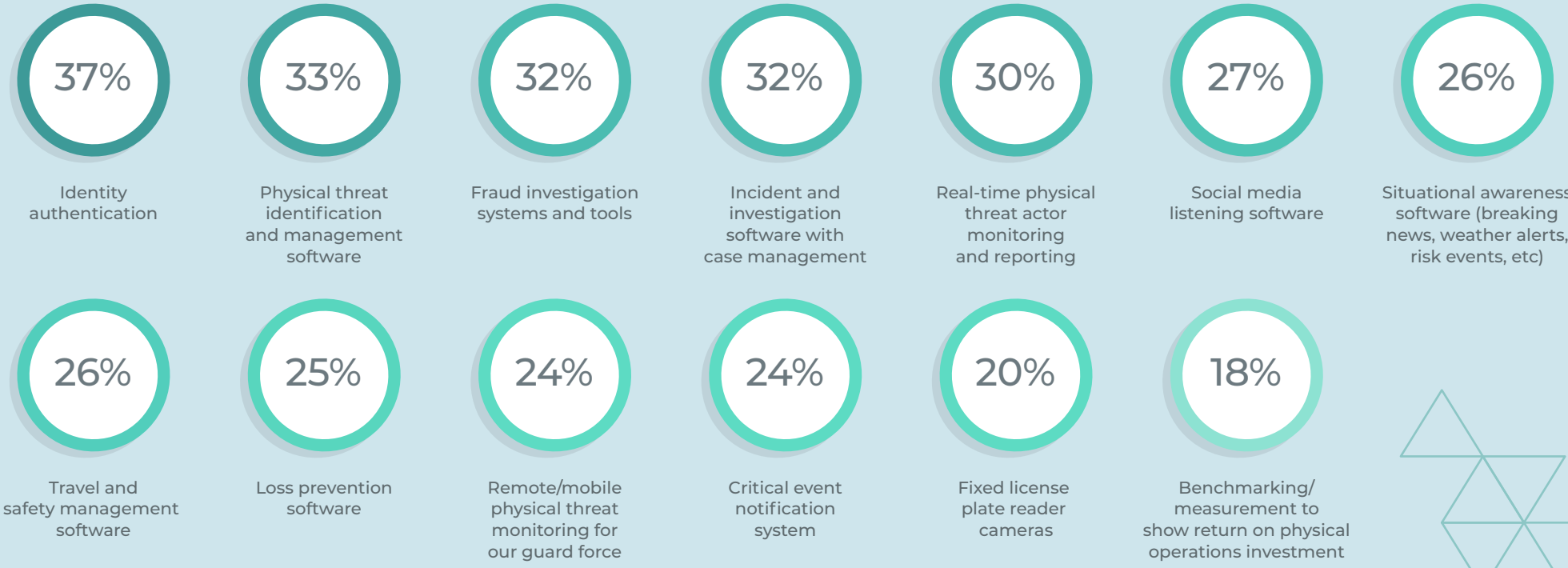
PHYSICAL SECURITY INVESTMENT PRIORITY ACCELERATION

Companies are investing in a myriad of physical security operations software solutions

To help mitigate potential harm from physical threat actors, 88% of respondents agree it is essential that companies accelerate implementation of unified threat management platforms. Operations and integration areas in which companies are investing include physical security, cybersecurity and HR integration; access control, visitor management system and threat actor identification software integration, hiring protective intelligence analysts, integrating fixed license plate reading cameras to identify threat actors and the buildout/fusion of a cyber-physical security operation center.

A strong majority of respondents agree (86%) that using software to manage their physical security solutions would play a critical role in protecting their company financially, culturally and brand-wise.

COMPANIES ARE INVESTING IN THE FOLLOWING PHYSICAL SECURITY OPERATIONS SOFTWARE SOLUTIONS IN 2021:



The Protective Intelligence Imperative Remains Strong

Now is the best time to invest in physical security digital transformation, critical for protecting companies financially, culturally, brand-wise … and for their future.

A strong majority of those surveyed agree (87%) that now is the best time to invest in physical security digital transformation and security leaders who do not adopt a digital mindset, 82% agree, will quickly be business irrelevant. Nearly 9 in 10 (86%) agree digitally transforming their physical security solutions would play a critical role in protecting their company financially, culturally and brand-wise, while 88% agree investment in technology to advance physical security effectiveness and mitigate violent threats is necessary for the future of their company.

About the study

A total of 300 respondents completed the survey, which was conducted May 13-27, 2021. These included chief security officers, chief information officers, chief technology officers, chief information security officers, physical security directors, executive protection directors, IT vice presidents and directors and physical security decision-makers at U.S. companies with over 5,000 employees in the technology, retail, automotive, healthcare, pharmaceutical, financial services, travel and hospitality, media and entertainment, consumer goods, insurance, telecommunications, government and education sectors.

About the Ontic Center for Protective Intelligence

The Ontic Center for Protective Intelligence provides strategic consulting, multidimensional services and resources for safety and security, legal, risk and compliance professionals at major corporations across nearly every industry sector. Through its initiatives, global industry experts and authorities in protective intelligence share best practices, insights on current and historical trends, and explore lessons learned from physical security peers.

About Ontic

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. For more information please visit www.ontic.co.

For inquiries related to the study, contact info@ontic.ai

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