2022 State of Protective Intelligence Report

HEIGHTENED THREATS, BUSINESS CONTINUITY AND ADVANCING PROTECTIVE INTELLIGENCE: PERCEPTION VERSUS REALITY IN CORPORATE AMERICA

The Outlook from Physical Security, Legal, Compliance and Risk Leaders

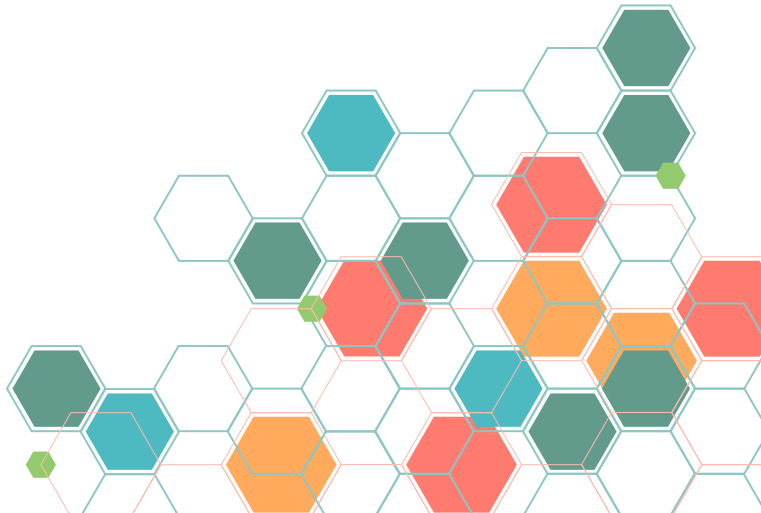
Ontic Center for Protective Intelligence

EXECUTIVE SUMMARY

In this third year of COVID-19, companies and employees working remotely while also anticipating a return to offices have been experiencing changing and varying health protocols, vaccine mandates and stages of "open." Supply chain challenges have at times shifted the focus of American business leaders from immediate on-the-ground matters to those of macro global security. As midterm elections near and January 6 arrests mount, political schisms show no sign of abating. Previously unseen "smash and grab" robberies by organized retail gangs, "air rage" on planes, threats towards health care, retail and restaurant workers and some 693 mass shootings occurred in 2021.[1]

At the same time, the pandemic has accelerated digital transformation, technology adoption and new ways of working, lessening concern among security professionals about managing remote and office workers. By most measures the U.S. economy is off to a solid start in 2022 and finished 2021 strong.[2] As compared to last year, financial cutbacks or staff reductions no longer rank among security professionals' biggest challenges.[3]

A majority of companies have in place programs to address mental health issues the pandemic has exacerbated, although higher demand for mental health care nationwide has resulted in longer waits to access care. Board-level reviews of physical and cyber security vulnerabilities, threats and activities are taking place at companies nationwide. But taking action to acknowledge and address the real dangers can be an issue — perceived as potentially creating a culture of fear that could damage the brand and corporate reputation. However, the physical threats and harm happening at companies, including to CEOs and their families, can be even greater menaces to business continuity that are anticipated to only rise in 2022.



1 - Gun Violence Archive

2 - VOA News

3 - 2021 State of Protective Intelligence Report

This juxtaposition of recovery from a pandemic recession with continued societal disruption at times creates a pressure cooker for security leaders, as the already significant volume of physical threats U.S. companies are receiving grows even greater, and increasingly becomes a weekly occurrence. More so than they did in 2021, security professionals feel less prepared to handle the greater frequency and volume of physical threats coming at them in 2022.

With significant advancements in technology, software, data capture, analysis and automation, in 2022 companies are actively advancing the digital transformation of their physical and cyber security operations. It is critical that corporations unite all threat intelligence across the enterprise, fuse infrastructure, training, data and operations and leave ineffective legacy systems and ways of working behind. Corporations are duty-bound to employees, customers, partners and investors to do all they can to proactively and better protect every aspect of their business.

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 its annual survey of chief security officers, chief legal officers, chief compliance officers, general counsels, physical security directors, corporate attorneys and physical security decision-makers at U.S. companies with over 5,000 employees to examine how they see physical security challenges and opportunities unfolding in 2022, and the potential impact on business continuity.

In this report we delve more deeply into these findings, the large-scale and growing threat landscape, the implications for people and businesses, and the imperative for corporations to adopt a software platform that unifies and operationalizes proactive cyber and physical security across nearly every function of the enterprise.

OUR ANNUAL STUDY SURFACED THESE KEY TAKEAWAYS:

1. **GLOBAL SECURITY TAKING PRECEDENCE OVER LOCAL** Companies are prioritizing security as it relates to geopolitical issues, supply chain risk and the global threat landscape but mitigating potential local acts of violence at offices or other company locations in the U.S. is not a priority.

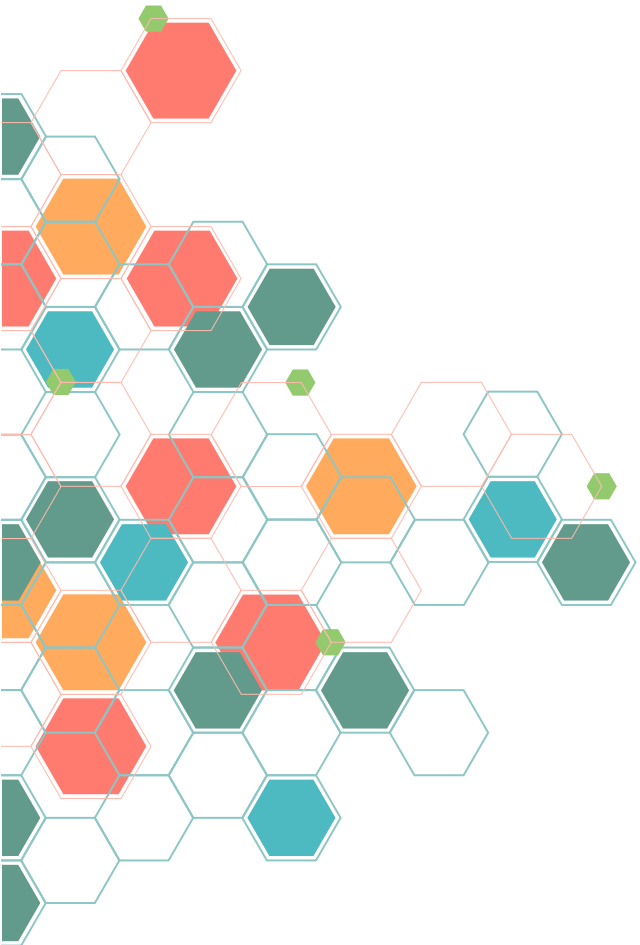
2. **INCREASING THREAT VOLUME AND FREQUENCY MEAN MORE WILL BE MISSED** The number of threats American companies receive or investigate in 2022 is expected to increase as compared to 2021 and the scale of those they expect to miss will expand. Forty-one percent anticipate missing 51%-100% of physical threats in 2022.

3. **RISKS TO BUSINESS IGNORED SO TRAINING, ACTION, COMMUNICATIONS FALL SHORT** Well-intentioned but contradictory security strategies are playing out at American companies. An inability to imagine the unimaginable and a desire to project the appearance of a safe environment can result in passive, reactive stances, little-to-no workplace violence training, and inconsistent policies, procedures and cross-functional communications.

4. **LARGE-SCALE MOVEMENT TO CONSOLIDATE INTELLIGENCE** A lack of unified protective intelligence has in the past year resulted in missed threats and harm at companies. But in a new significant development, almost universally, U.S. companies are actively consolidating their multiple threat intelligence, monitoring and alerting solutions into a unified system of record that enables holistic data analysis and reporting across physical security, cybersecurity, human resources (HR), legal and compliance.

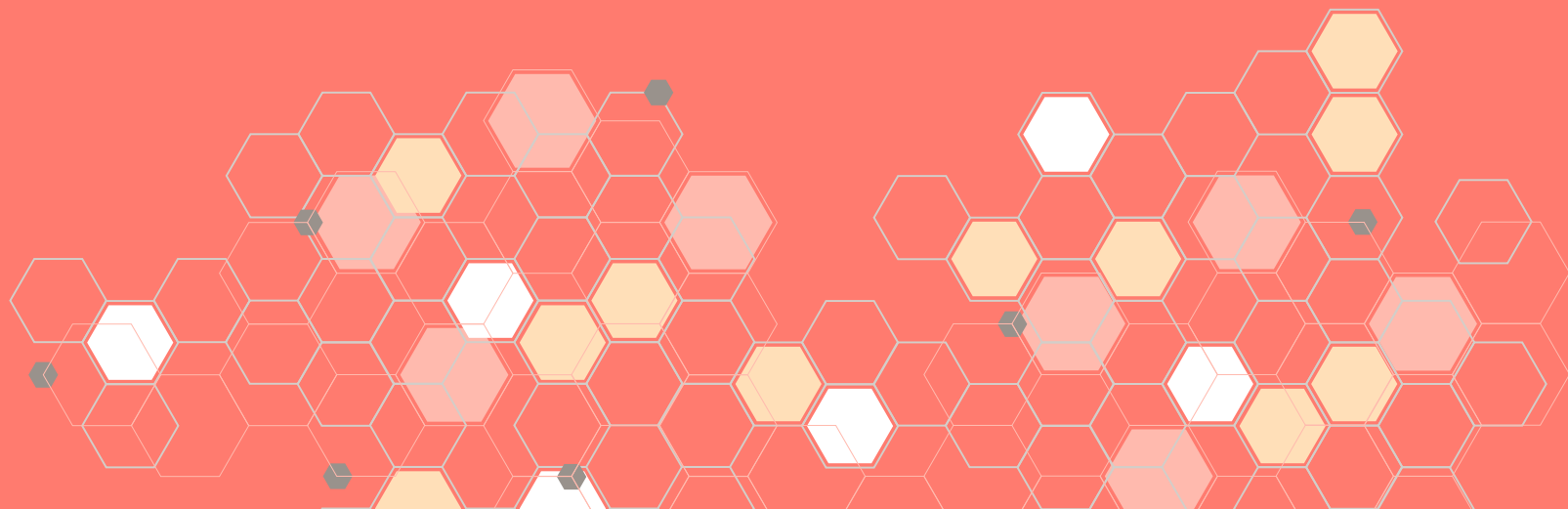
CONTENTS

2022 State of Protective Intelligence Report



Section 01

AS PHYSICAL THREATS AND HARM AT U.S. COMPANIES CONTINUES TO RISE, WORDS AND ACTIONS DON'T ALWAYS ALIGN



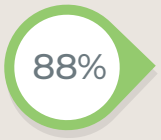
2022 marks a significant turning point in prioritizing physical security as threats are anticipated to grow

Compared to the beginning of 2021, 88% of respondents agree, companies are experiencing a dramatic increase in physical threat activity. The physical threat landscape has significantly changed and expanded, which has created an exponential increase in data and pre-incident indicators that 85% of physical security, legal and compliance leaders anticipate will only grow and be unmanageable in 2022.

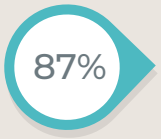
In the past year the lack of unified digital protective intelligence to proactively identify, assess and mitigate threats has resulted in missed threats and physical harm to employees, customers and human assets for companies, the overwhelming majority of respondents said.

For these reasons, a strong majority agree (85%), 2022 marks a significant turning point in prioritizing physical security for their company.

PHYSICAL SECURITY, LEGAL AND COMPLIANCE LEADERS AGREE:



My company is experiencing a dramatic increase in physical threat activity that I anticipate will only grow in 2022, 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.

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 I expect to be unmanageable in 2022.

For my company, 2022 is a significant turning point in prioritizing physical security due to the unprecedented increase in physical threats.

In the past year, the lack of unified digital protective intelligence — an investigative and analytical process used by protectors and physical security professionals to proactively identify, assess, and mitigate threats to protectees — has resulted in missed threats and physical harm to employees, customers and human assets for my company.

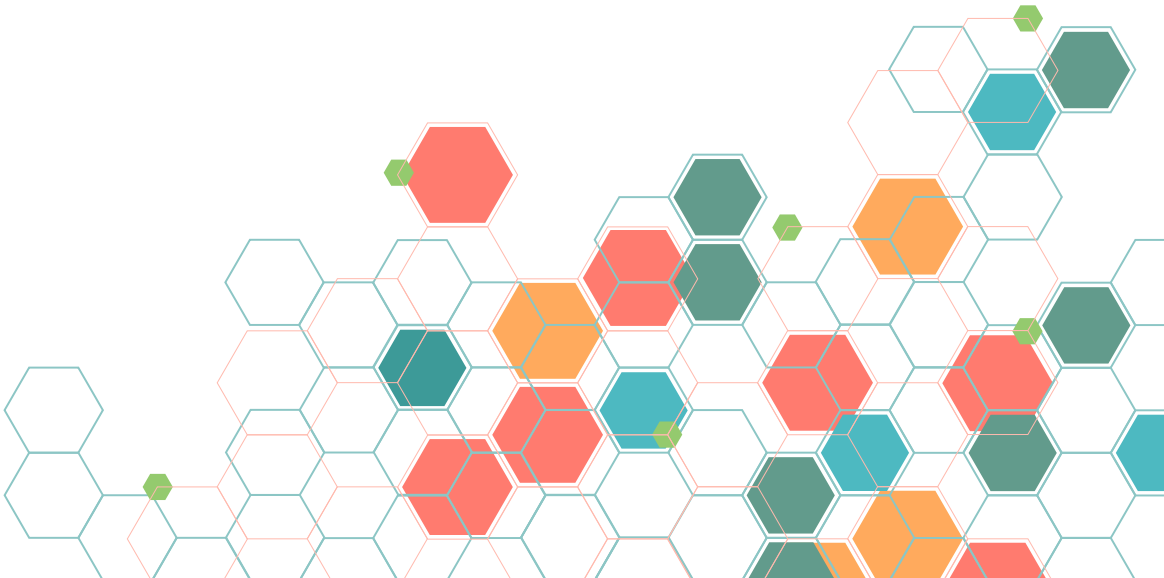
I feel less prepared to handle physical security for my company in 2022 as compared to the beginning of 2021.

Unmanaged physical threats are increasing corporate risk, are having a financially crippling effect and are negatively impacting business continuity at my company.

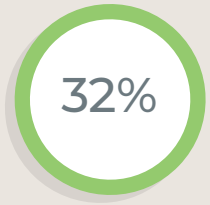
Global versus local danger, complementary and competing priorities disrupting sleep and business operations

When asked what issues "keep them up at night" as they consider their company's 2022 physical security program, increased physical threats and company backlash related to rising extremism, social and political issues were cited by one-third of physical security executives (33%) and vaccination requirements were cited by 31% of physical security and legal leaders. Also stirring concern among 28% of all respondents is that the lion's share of their management's attention is focused on macro global risk and supply chain security issues, to the detriment of prioritization and mitigation of location-specific physical security threats.

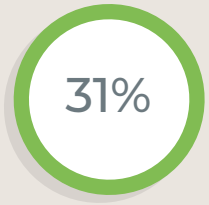
Executives worry about their management's greater attention to cybersecurity (26%) and about adjusting their skills as cyber-physical security operations increasingly converge (28%). A rise in physical insider threats and activist whistleblowers causes concern for 27% of respondents. Keeping employees and their CEO safe while working remotely, threats from former employees and effectively managing the volume of threat data all keep executives awake as does identifying potential threats to save their company money and reduce liabilities.



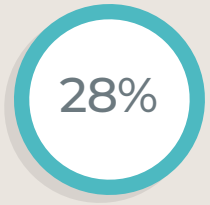
PERCENT OF PHYSICAL SECURITY, LEGAL AND COMPLIANCE LEADERS WHO SAY EACH PROGRAM ISSUE KEEPS THEM UP AT NIGHT



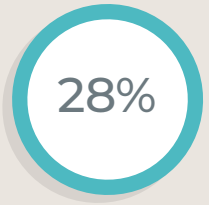
Increased physical threats and company backlash related to rising extremism, social and political issue



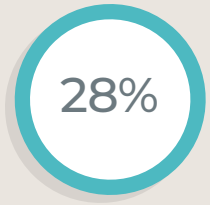
Increased physical threats and company backlash related to vaccination requirements



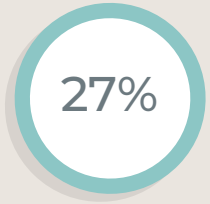
Preventing an active shooter event at one of our locations



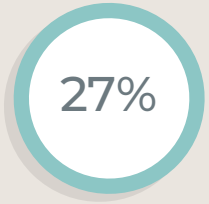
Management is predominantly focused on global risk and supply chain security issues so mitigating location-specific physical threats is not a priority



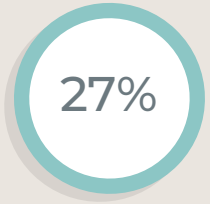
Adjusting my skills as cyber-physical security operations increasingly merge



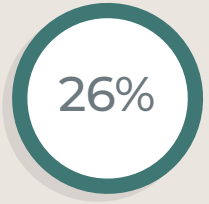
The rise of physical security insider threats and activist whistleblowers



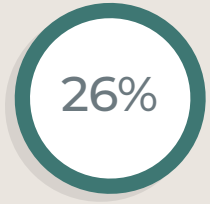
Keeping our employees safe as they work remotely



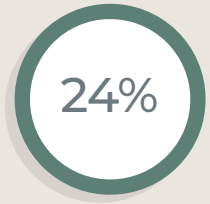
Increased physical threats and company backlash related to racial justice activism or political unrest



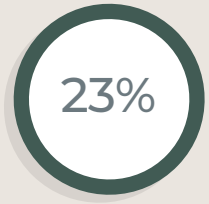
Management is focused more on cybersecurity



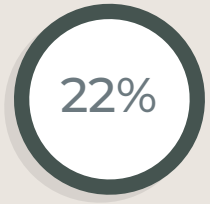
Protecting our CEO from harm when working from their private residence or while traveling



Effectively managing the volume of threat data



Identifying potential threats in order to save my company money and reduce liabilities



Dangerous threats from former employees

Downplaying what could again be the biggest 2022 business-related challenges

Among 18 physical security challenges mentioned, physical security threats to C-suite and company leadership was the most likely to be listed as one of the biggest challenges in 2022 for 44% of legal and compliance leaders followed by data protection and privacy (41%) as compared to 32% and 29% for physical security leaders, respectively.

Threat data management was the most likely to be listed as one of all respondents' biggest challenges in 2022, with 40% saying this. Insider threat management specific to physical security and threats to remote workers (32%) are expected to be equally challenging for just under one-third of those surveyed.

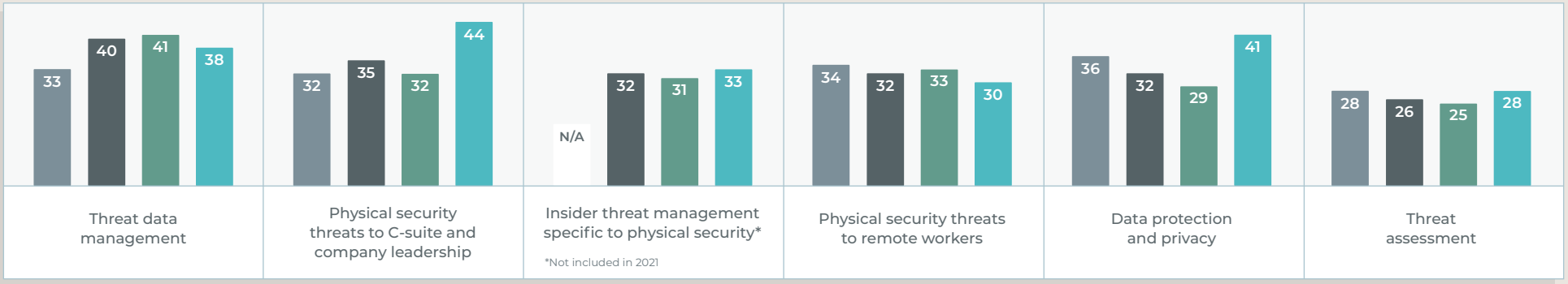
Only 12% expect COVID-19 recovery, managing permanent hybrid/remote office work structures and safety protocols to be among their biggest 2022 challenges, as compared to 38% in the **2021 State of Protective Intelligence Report.** This could be attributable to many companies having implemented corporate policies, procedures, health and safety protocols as vaccines began rolling out in the past year, as well as the experience executives have gained in dealing with these challenges.

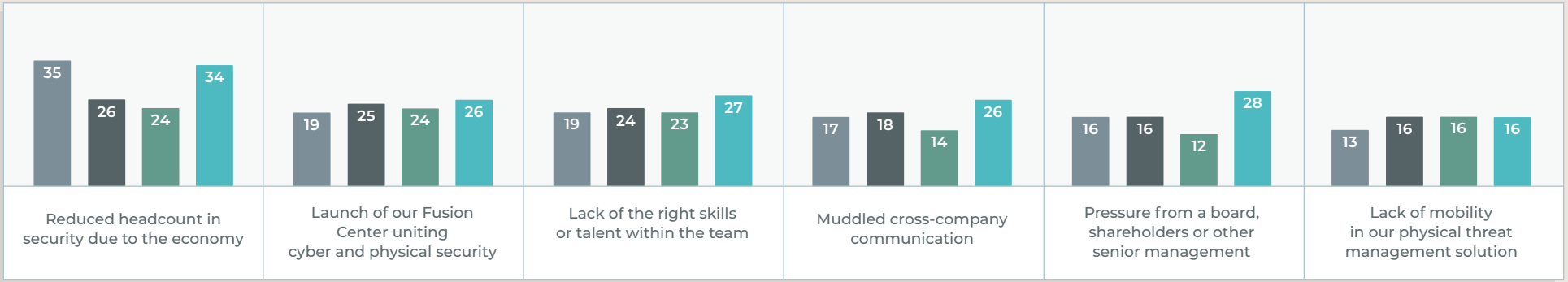
That said, expected 2022 physical security challenges for the most part mirror many of those shared in the inaugural **2021 State of Protective Intelligence Report.**

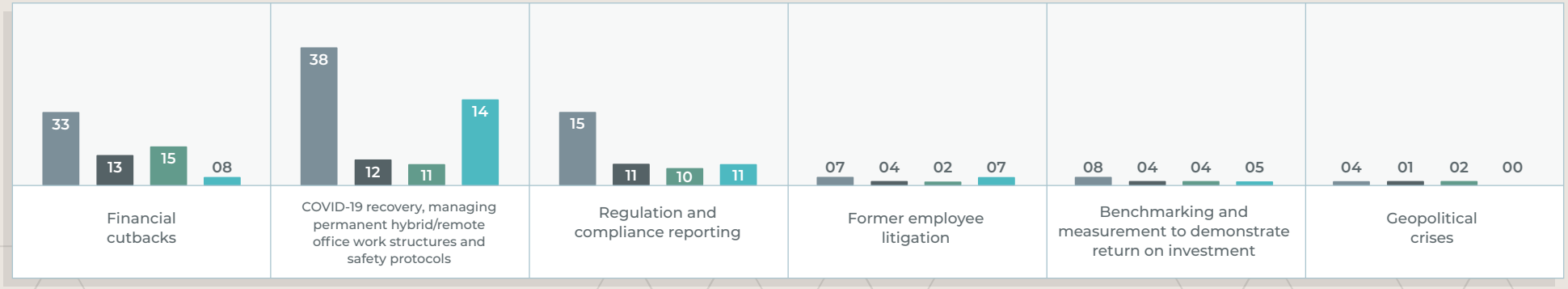
It's worth noting that in both studies, as respondents assessed challenges they might face in the new year ahead, they downplayed regulation and compliance reporting, as well as benchmarking and measurement to demonstrate a return on physical security investment. But if history is a guide, as 2022 progresses, these business-related issues could rise to become some of their biggest challenges, as they unexpectedly did in 2021.

BIGGEST PHYSICAL SECURITY CHALLENGES EXPECTED

% 2021 Total Respondents | % 2022 Total Respondents | % 2022 Physical Security Respondents | % 2022 Legal/Compliance Respondents







Among compliance, risk and regulation issues having an impact on physical security strategy, a majority of executives (64%) acknowledge corporations are targets that cannot rely on others for protection and at the same level, cite closing the gap between physical security solutions and compliance requirements. The changing profile of insider threats to corporate activists, increased personal liability for CEOs and C-level executives and the increased potential for financial losses are also cited by more than half of respondents as compliance, risk and regulation issues.

TOP COMPLIANCE, RISK OR REGULATION ISSUES IMPACTING PHYSICAL SECURITY STRATEGY*

	2022 Total	Physical Security	Legal / Compliance
Corporations have now become targets and can no longer rely on others for protection	64%	63%	64%
Closing the gap between physical security solutions and compliance requirements	64%	66%	58%
Corporate activists are becoming insider threats	62%	64%	57%
Increased personal liability for our CEO and C-level executives	59%	58%	63%
Increased potential for financial losses	52%	49%	58%

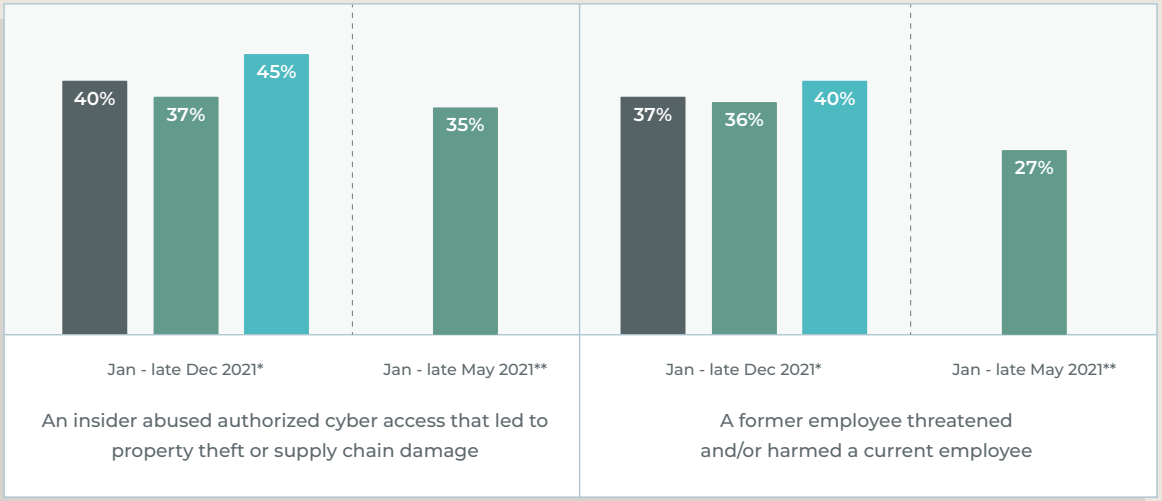
* Percentages reflect top 3 out of 5 choices

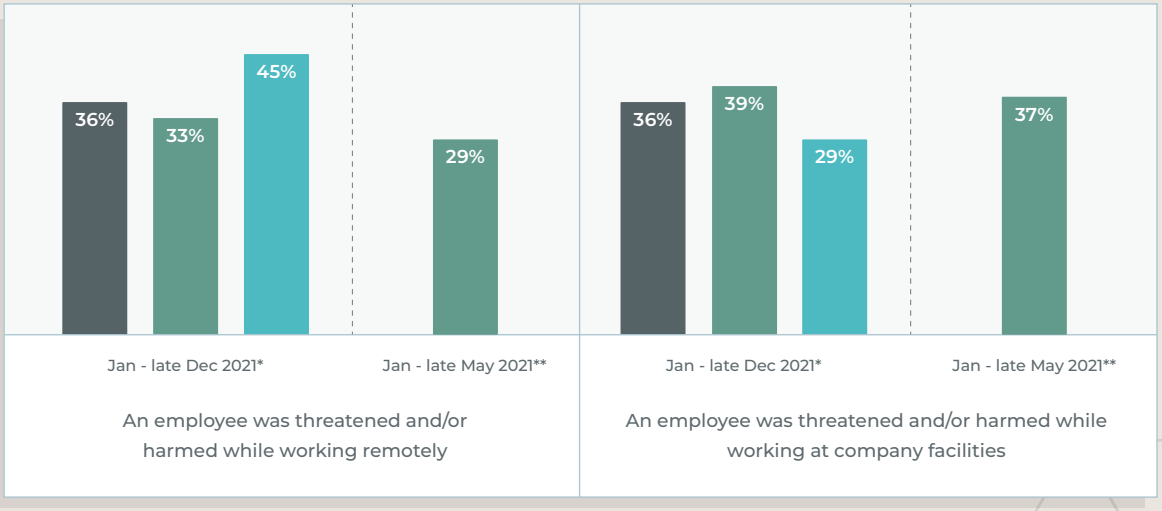
An uptick in intelligence failures, physical threats and harm at U.S. companies

Intelligence failures in 2021 led to employees being threatened and harmed. Research shows that malicious acts by insiders are becoming more prevalent. Forty percent of all respondents said as a result of intelligence failures in 2021, an insider abused cyber access that led to property theft or supply chain damage. **Employees were threatened or harmed by former employees (37%)**, both while working remotely and at company facilities (36%). Among physical security executives surveyed in 2021, this last statistic increased from 21% in May to 31% in December.

HARM, THREATS AND DAMAGE AT U.S. COMPANIES AS A RESULT OF INTELLIGENCE FAILURES

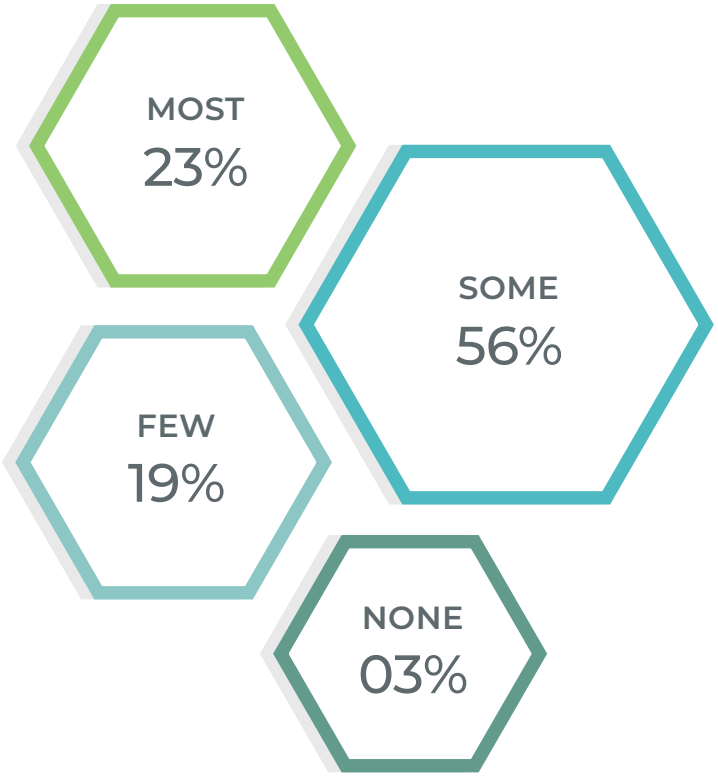
Total Respondents | Physical Security Respondents | Legal / Compliance Respondents



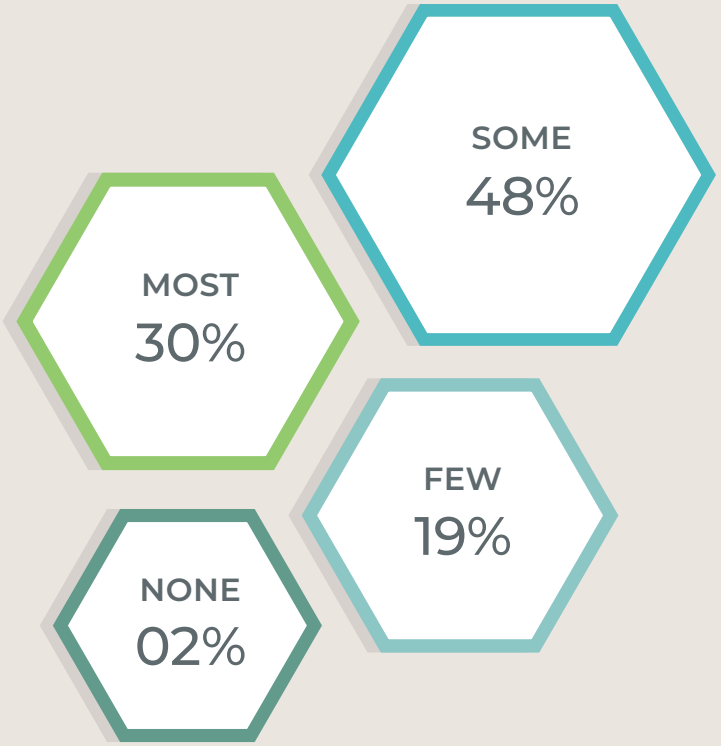


*2022 State of Protective Intelligence **2021 State of Protective Intelligence Mid-Year Outlook

The amount of **physical threats** their company received in 2021 that respondents said **originated as cyber threats** in cyber auditing tools, email, social media, antivirus software, or via a cyber-breach or ransomware attack:

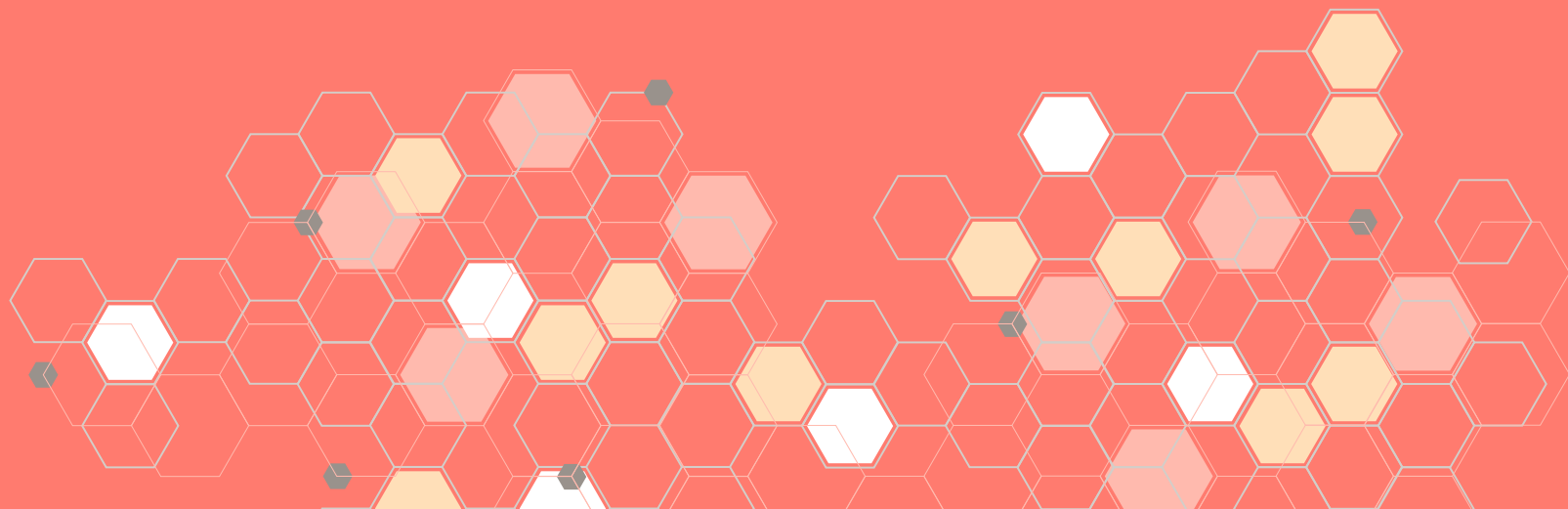


The amount of **physical threats** their company received in 2021 that respondents said **disrupted business continuity and caused harm or death**:



Section 02

MORE AMERICAN COMPANIES RECEIVING WEEKLY PHYSICAL SECURITY THREATS: VOLUME AND TYPES ANTICIPATED IN 2022



Physical threats are business continuity threats

The continuous operation of any business is critical to its ongoing success, but physical threats and violence against executives, employees and property can put business continuity at risk and have a lasting negative effect. Vulnerabilities that are ignored or incidents treated as "one-off" short-term issues can lead to greater compliance, regulation, reputation and recruiting challenges that impact business results and viability long-term.

In 2021, threats to the CEO and/or their family members ranked highest among disruptions to business continuity at their organization (23%), while other threats included supply chain damage and/or disruptions (15%), an insider abusing authorized cyber and physical access points (11%), executive kidnapping threats (8%), co-worker violence (8%), domestic-related violence that spilled into the workplace (6%) and during remote work (5%). Additional physical threats that disrupted business continuity included onsite burglary/theft, building and property theft, active shooters, social protests and activism, bomb threats and disgruntled former employee harm to current employees.

RANKING OF PHYSICAL THREATS DISRUPTING BUSINESS CONTINUITY AT COMPANIES IN 2021

Our CEO and/or family members have received threats	23%
Supply chain damage and/or disruptions	15%
Insider abusing authorized cyber and physical access points	11%
Executive kidnapping threat	08%
Co-worker violence	08%
Domestic-related violence that spills into the workplace	06%
Domestic-related violence during remote work	05%
Building and property vandalism	03%
Onsite theft/burglary	03%
Active shooter	02%
Related to social protests and activism	02%
Bomb threat	01%
Disgruntled former employee harm to current employee	01%
None of these	12%

Health and safety protocols are a source of return-to-office conflicts and physical threats

Varying hybrid work strategies, return-to-office false starts, disparate and continually shifting health and safety mandates and protocols are fueling frustrations and conflicts between employees and management. Though 93% of respondents agree their company has programs in place to address mental health issues the pandemic has exacerbated, 88% have reopened their offices and are encountering significant conflicts between management and employees regarding health and safety protocols as well as work-from-home policies. This new December 2021 finding on actual conflicts occurring at reopened offices is much higher than the 74% of physical security and IT leaders who said they anticipated significant conflicts when surveyed in May 2021 **(2021 State of Protective Intelligence Mid-Year Outlook).**

Based on current unmanageable physical threat data, 88% agree, physical threats will increase exponentially in 2022 as they reopen and return to the office. A strong majority (85%) say their company has experienced physical threats related to requiring employees to show proof of vaccination in order to return to the office. Fewer (69%) say their company is mandating employee vaccinations or regular COVID-19 testing in order to return to the office.

ON THEIR COMPANY'S HYBRID WORK POLICIES AND PHYSICAL SECURITY OPERATIONS, PHYSICAL SECURITY, LEGAL AND COMPLIANCE EXECUTIVES AGREE

93% My company has programs in place to address mental health issues that have been exacerbated by the pandemic.

88% My company has reopened its offices, and we are encountering significant conflicts between management and employees regarding health and safety protocols, and work-from-home policies.

88% Based on the current unmanageable physical threat data, I believe physical threats will increase exponentially in 2022 as we reopen and return to the office.

85% My company has experienced physical security threats related to requiring employees to show proof of vaccination in order to return to the office.

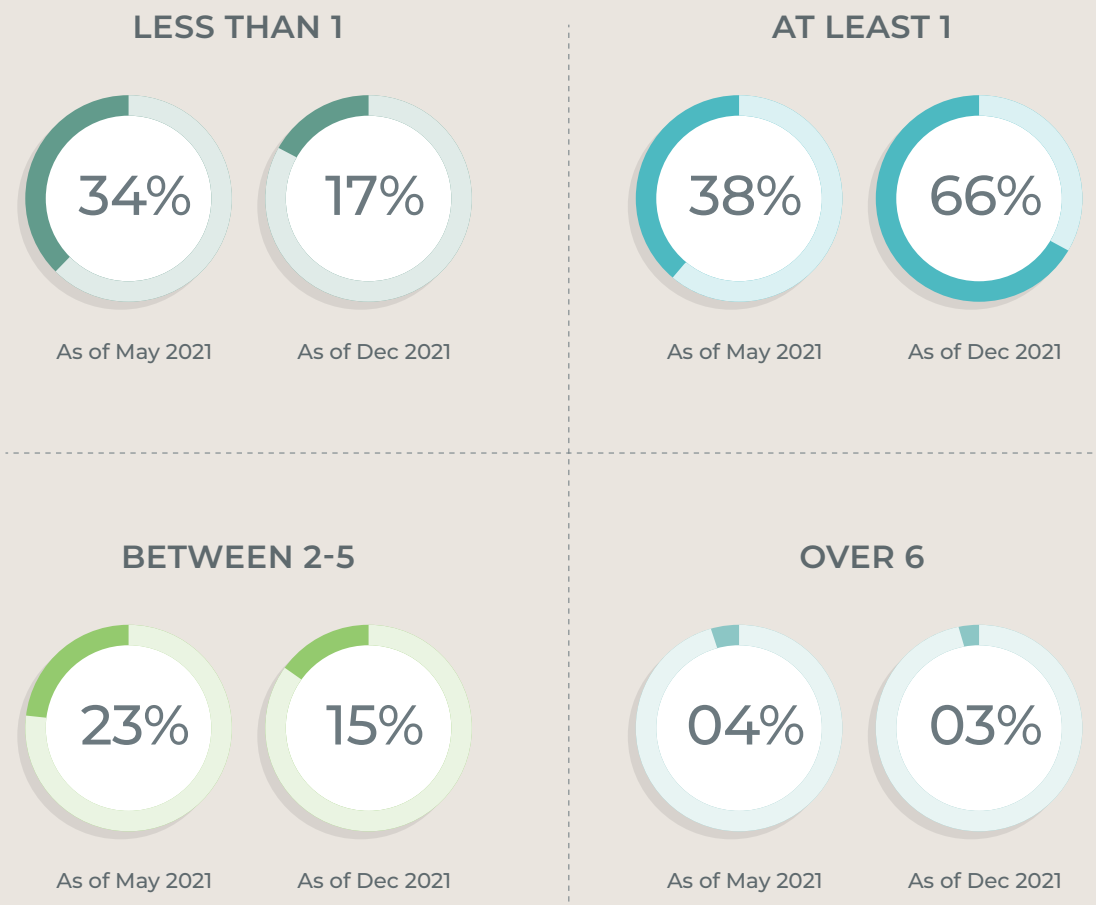
69% My company is mandating employees get vaccinated or undergo regular COVID-19 testing in order to return to the office.

Number of U.S. companies receiving or investigating weekly physical security threats doubles

In May 2021, 34% percent of physical security leaders surveyed had received or investigated less than one physical threat per week while 23% said between 2-5 per week and just over one-third received or investigated at least one physical threat per week. Another 4% reported over six per week **(2021 State of Protective Intelligence Mid-Year Outlook).**

Fast-forward just a few months to the end of 2021, and nearly double the percent of physical security leaders surveyed in May — two-thirds — said they received at least one physical threat per week in 2021. This increase in the percent of companies experiencing weekly threats may account for the cut by half, to 17%, of those saying they received less than one physical threat per week. In notable decreases from the May 2021 survey findings, only 15% of physical security leaders surveyed months later in December 2021 cited 2-5 physical threats weekly and three percent cited over 6 threats per week.

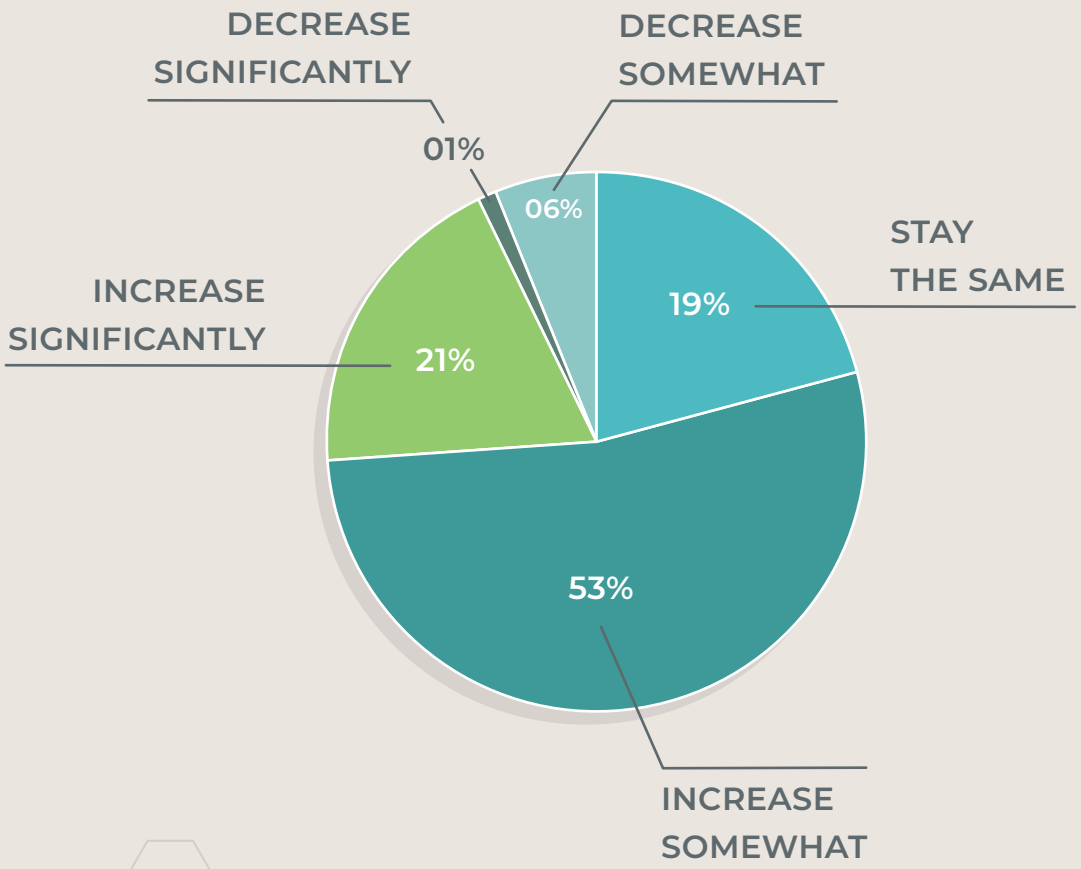
NUMBER OF PHYSICAL THREATS THEIR COMPANY RECEIVED OR INVESTIGATED PER WEEK IN 2021, ACCORDING TO PHYSICAL SECURITY EXECUTIVES



Nearly three-quarters of respondents expect 2022 physical threat volume to increase

Seventy-four percent of physical security, legal and compliance executives expect the number of threats their company will receive or investigate in 2022 to increase as compared to 2021, including 21% who expect physical threat volume to increase significantly. Nineteen percent expect the number of physical threats to stay the same in 2022, and another 7% expect they will decrease.

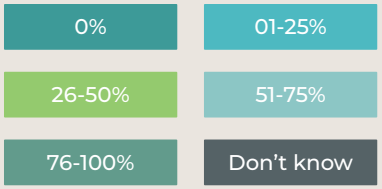
EXPECTATIONS FOR CHANGES IN THE NUMBER OF PHYSICAL THREATS MY COMPANY WILL RECEIVE OR INVESTIGATE IN 2022 (AS COMPARED TO 2021)

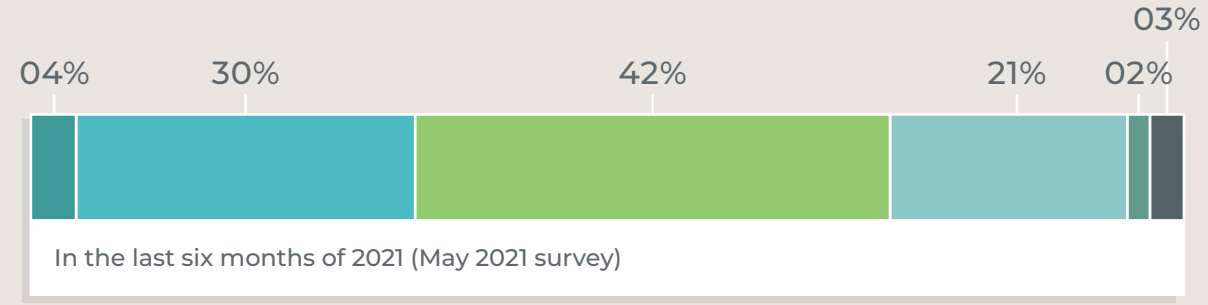


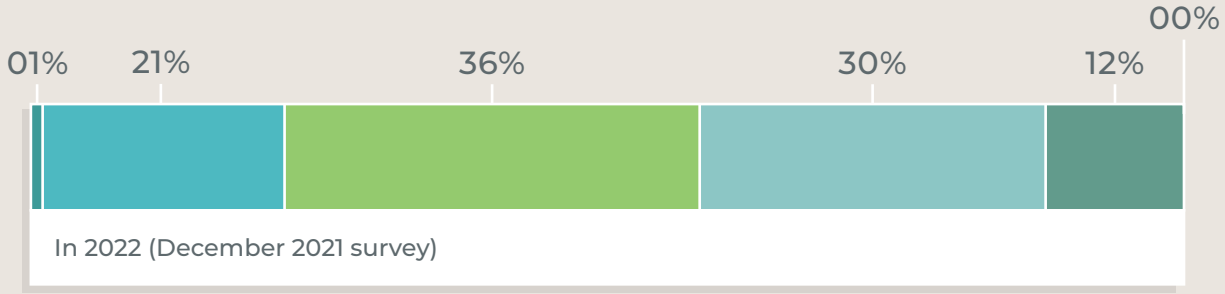
While many trends around physical threats should raise corporate alarms, the expanded scale of threats that physical, legal and compliance executives anticipate they will miss in 2022 is troubling. Forty-one percent of physical security, legal and compliance executives anticipate they will miss 51-100% of threats in 2022. Another nine percent anticipate they will miss 76-100% of physical threats. This is what executives mean when they say threats are unmanageable.

A disturbing trend becomes visible when physical security executive survey responses in December 2021 regarding physical threats they anticipate missing are compared to those six months prior. The percentage of physical security executives that anticipate missing 0-50% of physical threats in December as compared to May goes down, but the decline is negated by an significant increase in the percentage of physical executives that anticipate missing 51-100% of physical threats in 2022.

PERCENTAGE OF PHYSICAL THREATS ANTICIPATED WILL BE MISSED AT AMERICAN COMPANIES ACCORDING TO PHYSICAL SECURITY EXECUTIVES

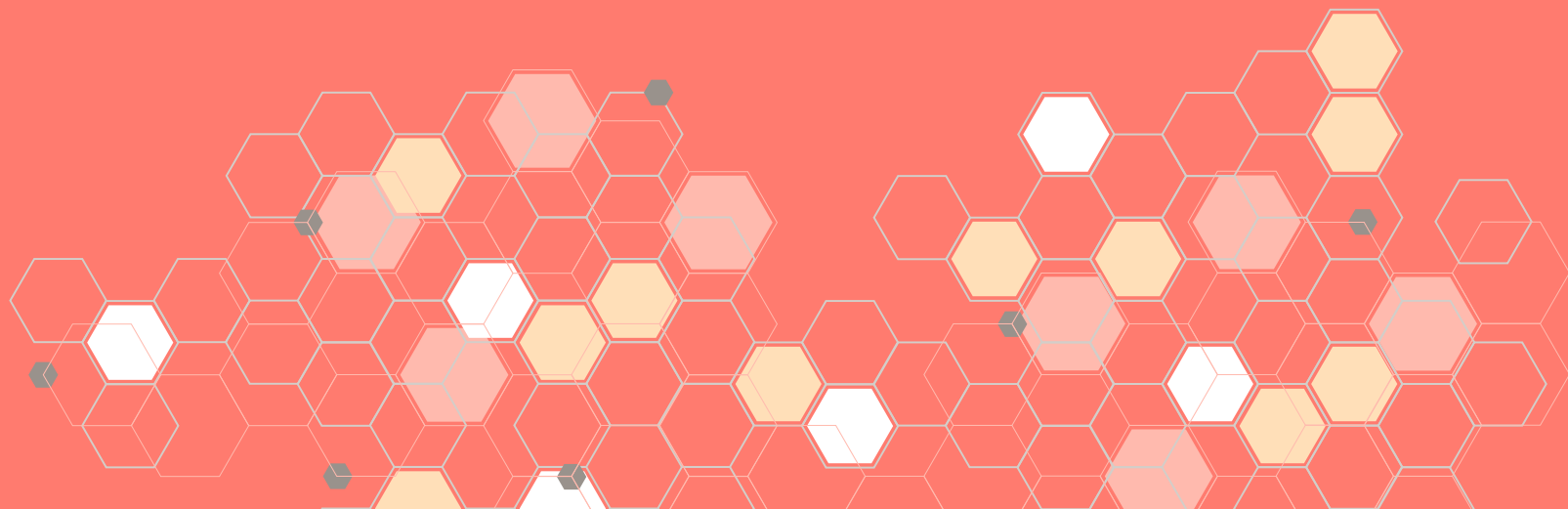






Section 03

PERCEPTIONS, ATTITUDES, INCONSISTENT PREPAREDNESS AND RISK DETERRENCE MEASURES



Wise business strategy or self-fulfilling prophecy? Fear of creating a culture of fear

Many seemingly contradictory but well-intentioned strategies, processes and policies around physical security are playing out at American corporations.

On the one hand, for more than half of respondents, rather than try to get ahead of potential threats, harm and damage to their business and its people in order to minimize impact, their company waits until catastrophe strikes, then reacts. Specifically, these companies believe that being proactive and training employees will create a culture of fear.

Such a passive stance means workforces have little training and would not know what to do if an active shooter was at one of their facilities. On the other hand, not all companies take this approach, as 38% surveyed say they have an Active Shooter/Active Assailant Plan in place and employees receive regular training.

Still, an inability to imagine the unimaginable — physical harm happening at their company — rings true for close to one-third of those surveyed, which also results in an inability to value employee training and preparedness to deal with such crises. Less than one-third surveyed say their companies do workplace violence training from time to time but do not have a formal program.

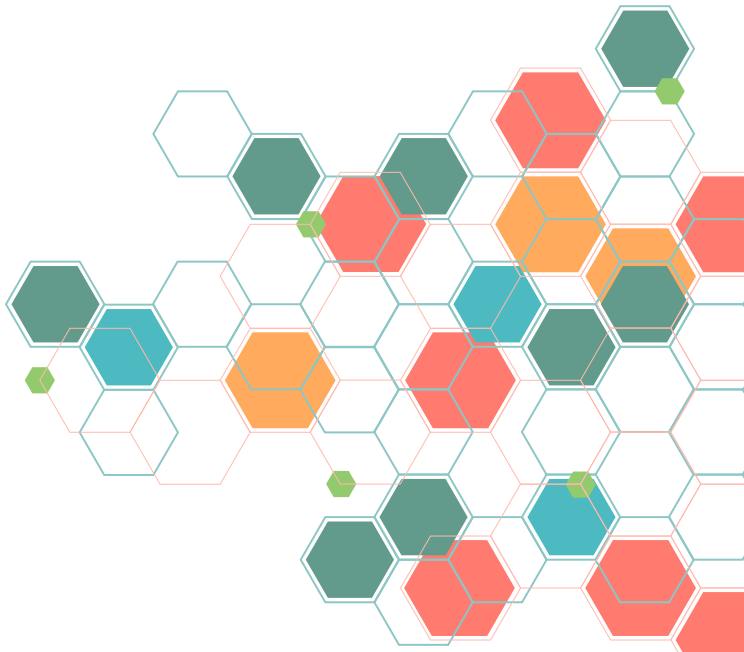
My company believes training employees so they are better prepared for potential workplace violence will create a culture of fear, wants to take a reactive strategy and does not see the ultimate risk to business continuity by inaction.

EMPLOYEE PREPAREDNESS TO ADDRESS PHYSICAL THREATS AND POTENTIAL WORKPLACE VIOLENCE AT AMERICAN COMPANIES, ACCORDING TO PHYSICAL SECURITY, LEGAL AND COMPLIANCE EXECUTIVES

A conundrum for HR, physical security and legal professionals: violent employees

An estimated two million Americans are victims of workplace violence, according to OSHA.[4] The American National Standard for Workplace Violence Prevention and Intervention (ASIS & SHRM, 2011; ASIS, 2020) defines workplace violence broadly to include bullying, verbal harassment and intimidation. But all too often, previously observed behaviors, voiced concerns, hostile social media posts and other warning signs tied to a perpetrator of violence come to light after a tragedy has occurred.

There are dozens of widely reported examples from the past year: a pediatrician in Austin, Texas was murdered at her office; a lone gunman opened fire inside a supermarket in Boulder, Colorado, killing 10 and an armed gunman shot 14 people, one of them fatally, in a Kroger supermarket in Collierville, Tennessee. The shooter was a former employee dismissed from his job earlier that day. A transit employee who gunned down nine co-workers and killed himself at a Northern California rail yard was known to be "highly disgruntled" long before carrying out the shooting rampage, according to news reports. U.S. customs and border officers had detained the man five years before as he returned from the Philippines and in his possession were books about terrorism, fear and manifestos… professions of hatred of his workplace.



4 - OSHA

Policies and practices that operationalize violence prevention are needed, particularly given the potential emotional and psychological impact, which can ultimately hurt overall business performance. Threats, harassment and bullying — precursors to physical violence — may lead to lower employee morale, increased turnover, absenteeism and mental health service costs.

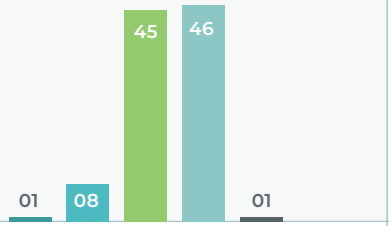
Oftentimes training doesn't go far enough and internal attitudes about how companies may be perceived can hamper their ability to keep people safe and for businesses to rebound from crisis. Initiatives can be sidelined by inconsistencies and departments working at cross-purposes. According to the survey, 91% of respondents agree that at their company, physical security, legal and HR are trained to address situations should the firing or furloughing of an employee turn violent. But, 87% agree their company does not have a process or tools to alert the same departments or staff if, after they have been furloughed or fired, former employees who have exhibited violent tendencies return to the premises.

While a strong majority (88%) agree that at their company, physical security, legal and HR are notified and typically present when an employee will be furloughed or fired, alarmingly, 86% agree that in the past year violence or harm has occurred when an employee was furloughed or fired because these actions are not being taken consistently.

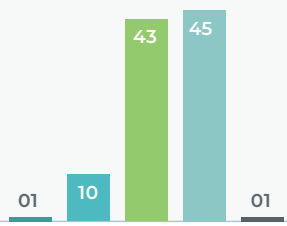
Physical security, legal and HR professionals have received threat assessment training, recognize and report erratic behavior and warning signs to prevent workplace violence, 86% agree. But, 87% also agree their company has workplace violence fatigue — that threats or harmful incidents occur so often that employees are used to erratic and violent behavior and don't report these as warning signs until it's too late. Further hindering efforts to keep people safe, 86% agree their company downplays risk to emulate a safe environment, as opposed to taking the steps to monitor and proactively prevent workplace violence incidents.

WORKPLACE VIOLENCE, THREAT ASSESSMENT TRAINING, CROSS-FUNCTION COMMUNICATIONS AND REPORTING

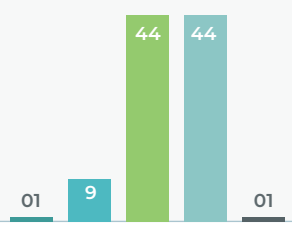
% Strongly disagree | % Somewhat disagree | % Somewhat agree | % Strongly agree | % Don't know



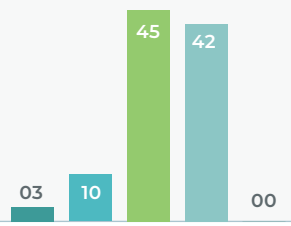
At my company, physical security, legal, and HR are trained to address situations should the firing or furloughing of an employee turn violent.



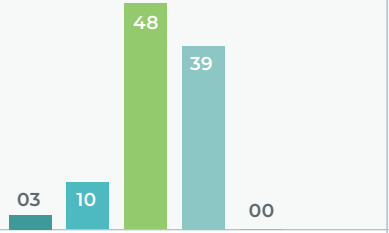
At my company, physical security, legal, and HR are notified when an employee will be furloughed or fired.



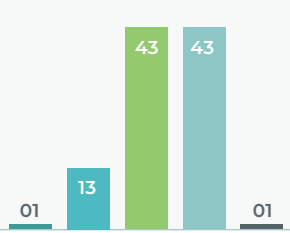
At my company, physical security, legal, and HR are typically present when furloughing or firing of an employee takes place.



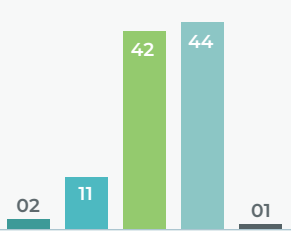
If former employees who have exhibited violent tendencies return to the premises after they have been furloughed or fired, my company does not have a process or tools to alert physical security, legal, HR or staff.



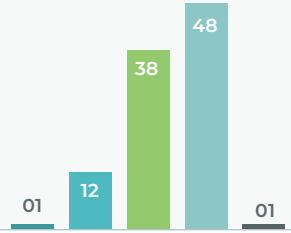
Our company has workplace violence fatigue — threats or harmful incidents occur so often that employees are used to erratic and violent behavior and don't report these as warning signs until it's too late.



Physical security, legal and HR professionals have received threat assessment training, recognize and report erratic behavior and warning signs to prevent workplace violence.



In the past year violence or harm has occured when an employee was furloughed or fired because we do not consistently notify physical security, legal and HR in advance of the action nor are they present when the dismissal takes place.

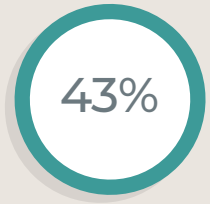


My company downplays risk to emulate a safe environment, as opposed to taking the steps to monitor and proactively prevent workplace violence incidents.

Fewer than half of respondents take action after employees are threatened or harmed

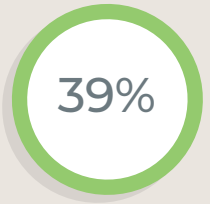
After employees were threatened or harmed by former employees or others while working remotely or at company facilities, 43% of those surveyed notified HR, legal and security; 40% notified the local police and requested enhanced patrol coverages while 39% enhanced company security coverages for the employee both in the office and at their home. Enhanced intelligence collection around the threat was done by 36% of respondents.

ACTIONS TAKEN AT AMERICAN COMPANIES AFTER AN EMPLOYEE WAS THREATENED AND/OR HARMED*

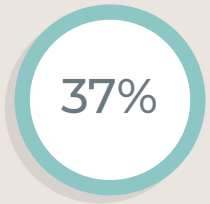


Notified HR, Legal and Security

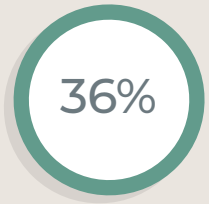
Notified the local police and requested enhanced patrol coverages



Enhanced company security coverages for the employee in the office and/or working from home

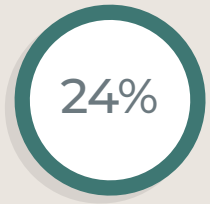


Notified Security



Enhanced intelligence collection around the threat

Notified Legal



Notified HR

*Working remotely or at company facilities or perpetrated by a former employee

Physical security and cybersecurity — prioritizing both to varying degrees

Integrating digital physical security operations with cybersecurity is an area of investment in 2022 for nearly half (48%) of all surveyed and 37% are investing in the buildout/fusion of a cyber-physical Security Operation Center. For 36%, integrating digital physical security operations with cybersecurity was a top priority at the beginning of 2021 and continues to be for 2022. For 30% of respondents, it is a new priority for 2022. Given the growing convergence of physical security and cybersecurity threats, these are prudent business strategies. As noted earlier in this report, 40% of respondents said an insider abused cyber access that led to property theft or supply chain damage as a result of intelligence failures in 2021.

How companies are managing the potential for and actual cyber-physical security violations after they occur, however, is all over the board — some approaches are highly constructive and impactful, and other approaches could be perceived as doing the right thing but are in effect just "band-aids". Close to two-thirds (64%) of the respondents who had an insider abuse authorized cyber access said their company contracted with a cyber-consulting firm to conduct a damage assessment following abuse by an insider with authorized cyber access that led to property theft or supply chain damage and 30% notified the FBI. Concerned about the risk of negative brand impact, though, 39% said their company "kept things quiet."

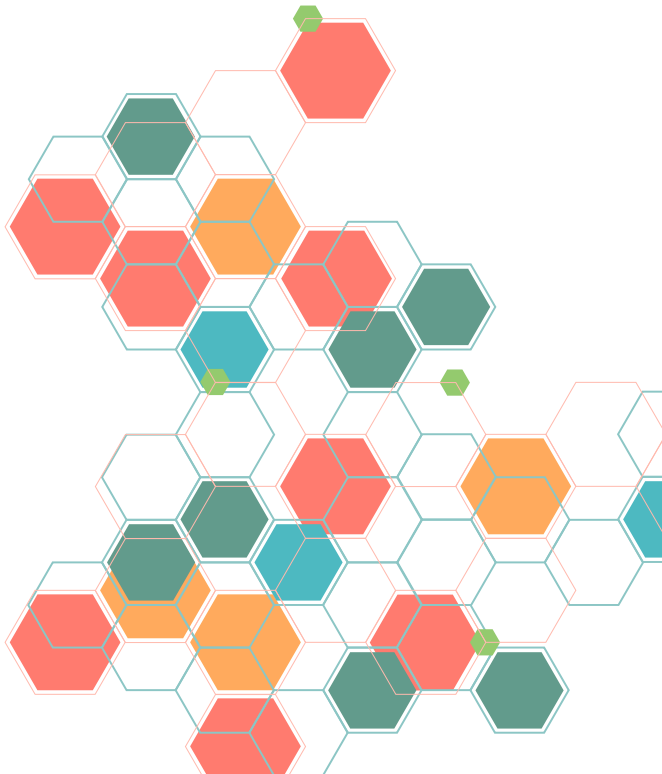
ACTIONS TAKEN AT AMERICAN COMPANIES AFTER AN INSIDER ABUSED AUTHORIZED CYBER ACCESS*

*that led to property theft or supply chain damage

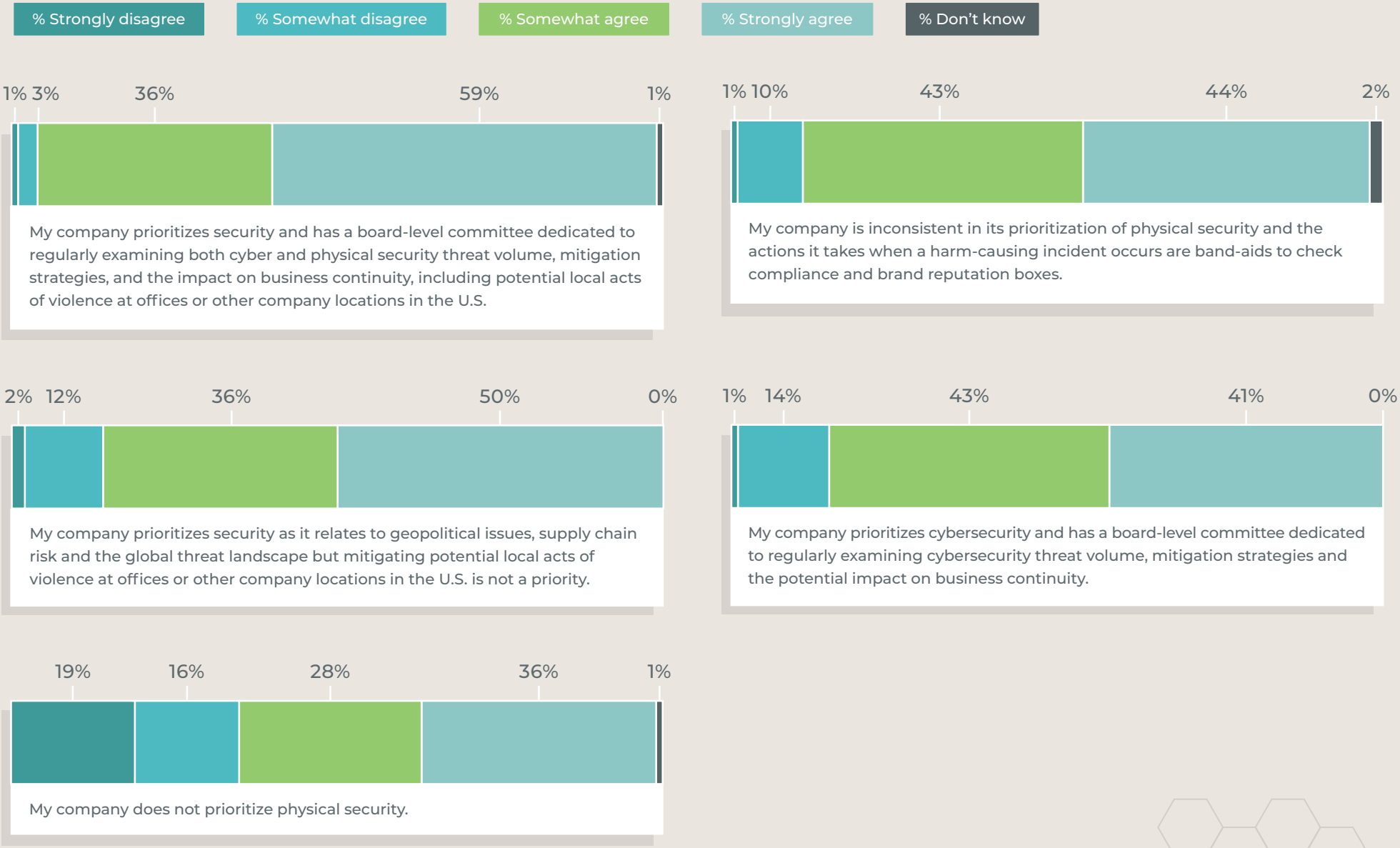
	2022 Total	Physical Security	Legal / Compliance
Our company notified the FBI.	30%	29%	33%
Our company contracted with a cyber consulting firm to conduct a damage assessment.	64%	60%	73%
Our company kept things quiet due to the risk of negative brand impact.	39%	38%	40%

Almost universally (95%), respondents say their company prioritizes security and has a board-level committee dedicated to regularly examining both cyber and physical security threat volume, mitigation strategies, and the impact on business continuity, including potential local acts of violence at offices or other company locations in the U.S. The question is whether regular reviews by organizations' most powerful advisors and prominent executives lead to effective, consistent protective plans and actions.

Survey results indicate they may not, as a strong majority agree (87%), their company is inconsistent in its prioritization of physical security and the actions it takes when a harm-causing incident occurs are band-aids to check compliance and brand reputation boxes. What's more, 86% agree, including 50% that strongly agree, their company prioritizes security as it relates to geopolitical issues, supply chain risk and the global threat landscape, but mitigating potential local acts of violence at offices or other company locations in the U.S. is not a priority. Significantly, 64% agree their company does not prioritize physical security.

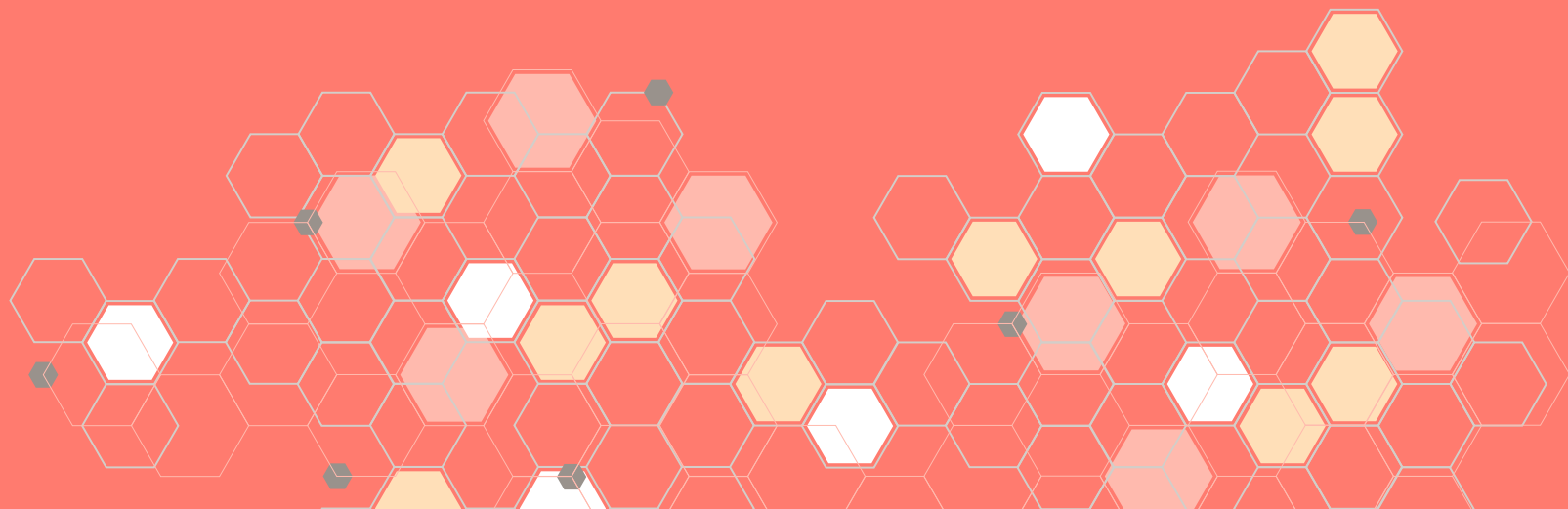


INCONSISTENT CYBER-PHYSICAL SECURITY PRIORITIES AT AMERICAN COMPANIES



Section 04

PHYSICAL SECURITY CONVERGENCE, CONSOLIDATION AND INVESTMENT



INVESTMENT PRIORITIES FOR PHYSICAL SECURITY OPERATIONS

2022 VERSUS THE BEGINNING OF 2021

- % not a top priority at the beginning of 2021, but is for 2022
- % was a top priority at the beginning of 2021, and still is for 2022

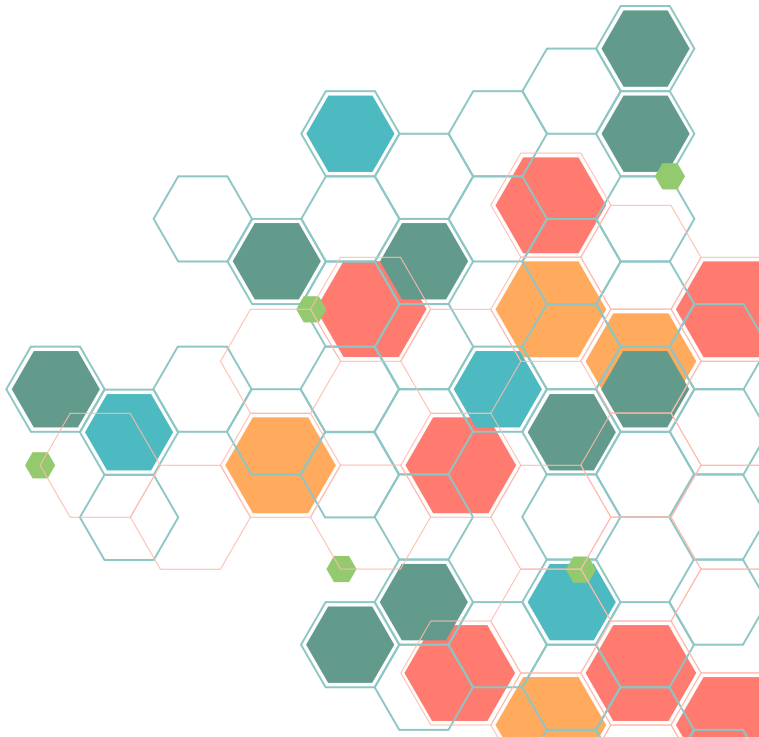
2022 AREAS OF INVESTMENT FOR PHYSICAL SECURITY OPERATIONS INTEGRATION

- 50% Access control systems with software to identify physical threat actors
- 48% Digital physical security operations with cybersecurity
- 43% Visitor management system with software to identify threat actors
- 41% Digital physical security operations with HR
- 37% Buildout/fusion of a cyber-physical Security Operation Center
- 37% Fixed license plate reading cameras with software to identify threat actors
- 32% Hiring Protective Intelligence analysts

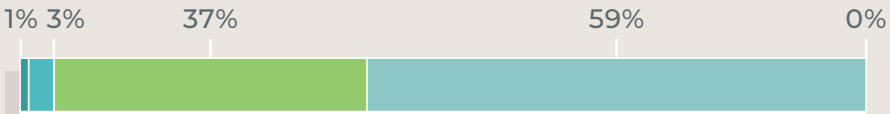
Cyber and physical security convergence, integration into one software platform underway

As people continue to work remotely in 2022, 91% of physical security, legal and compliance executives agree, it is more important than ever for their company to dedicate financial resources to physical security technology solutions at the same level. Most agree (96%) including 59% who strongly agree, that cybersecurity and physical security must be integrated or else both cyber and physical threats will be missed.

In 2021 the lack of unified digital protective intelligence resulted in missed threats and physical harm to employees, customers and human assets for their company, 84% of respondents agreed, up from 71% in the prior year. If all members of the physical security team could view threat data in a single system-of-record software platform, 87% agree their company would be able to better avoid crises.



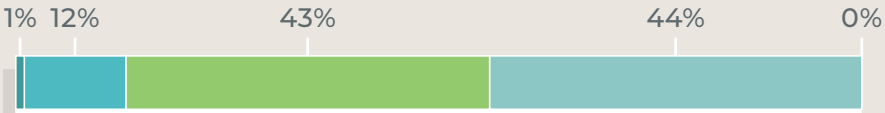
PHYSICAL SECURITY, LEGAL AND COMPLIANCE EXECUTIVES AGREE



Cybersecurity and physical security must be integrated or else both cyber and physical threats will be missed.

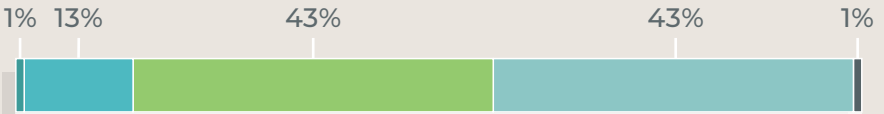
Investment in technology to advance physical security effectiveness and mitigate violent threats is necessary for the future of my company.

For 2022, my company is actively consolidating our multiple threat intelligence, monitoring and alerting solutions into a single software platform that enables holistic data analysis and reporting across physical security, cybersecurity, HR, legal and compliance.

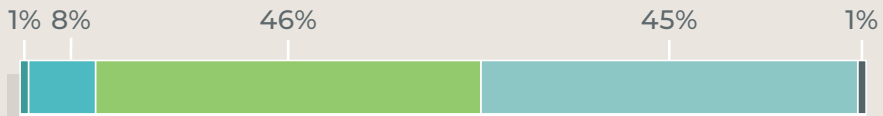


My company would be able to better avoid crises if all members of the physical security team could view threat data in a single system-of-record software platform.

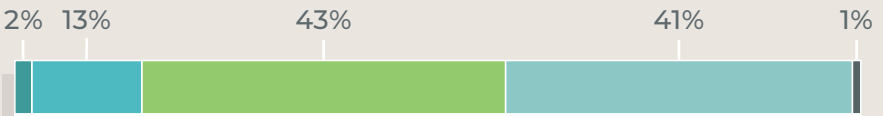
My company is actively adopting multiple new threat intelligence, monitoring and alerting solutions for physical security, cybersecurity, HR, legal and compliance but has no strategy for holistic data analysis and reporting.



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



As people continue to work remotely in 2022, it is more important than ever for my company to dedicate financial resources to physical security technology solutions at the same level as cyber security.



In the past year, the lack of unified digital protective intelligence — an investigative and analytical process used by protectors and physical security professionals to proactively identify, assess and mitigate threats to protectees — has resulted in missed threats and physical harm to employees, customers and human assets for my company.

A WIDESPREAD MOVEMENT TO PHYSICAL SECURITY SOFTWARE IS UNDERWAY

For the future of their company, a strong majority agree (89%), investment in technology to advance physical security effectiveness and mitigate violent threats is necessary.

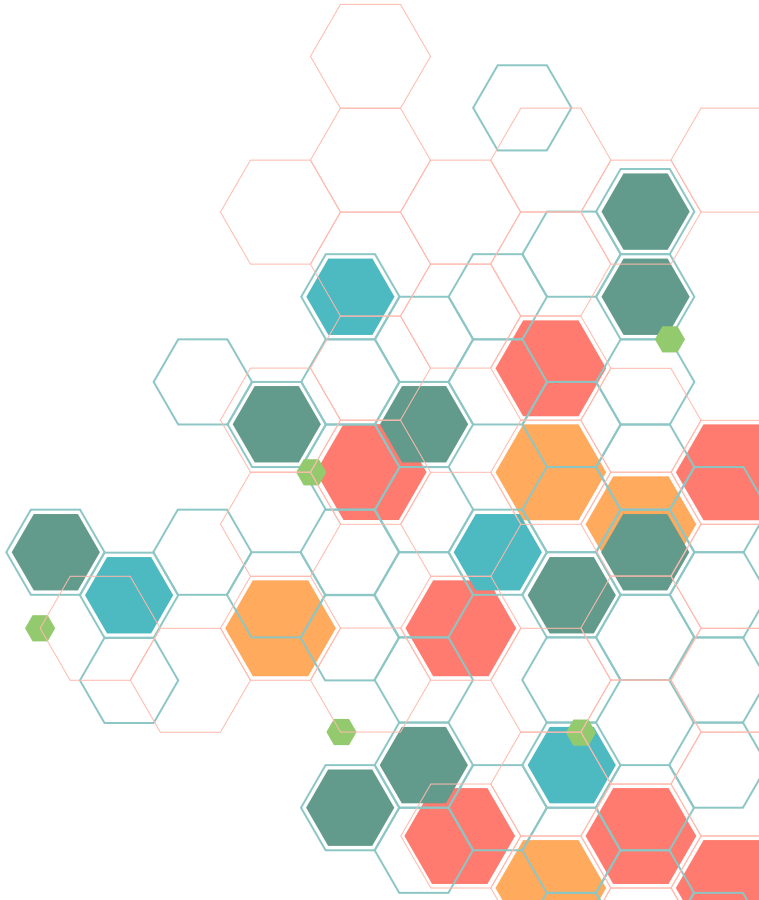
In a new and significant development, this study shows that in 2022 a widespread movement is underway at American businesses to digitally transform physical security into a single software platform. Almost universally, 95% of respondents say, U.S. companies in 2022 are actively consolidating their multiple threat intelligence, monitoring and alerting solutions into a single software platform that enables holistic data analysis and reporting across physical security, cybersecurity, HR, legal and compliance.

About the study

A total of 359 respondents completed the survey, which was conducted November 29-December 21, 2021. These included chief security officers, chief legal officers, chief compliance officers, general counsels, physical security directors, corporate attorneys and physical security decision-makers at U.S. companies with over 5,000 employee in the automotive, banking and financial services, consumer goods, education, energy, government, healthcare, insurance, media and entertainment, pharmaceutical, retail, technology, telecommunications, travel and hospitality industries.

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 multiple industry sectors including financial services, technology, retail, entertainment and consumer products. 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.

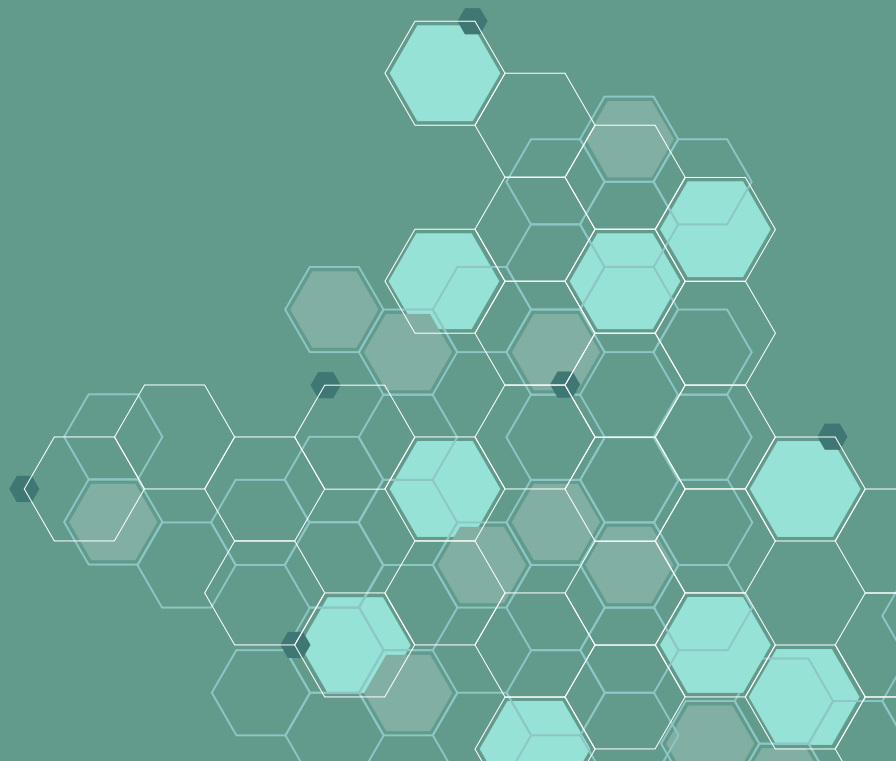


About Ontic

Named the top industry innovator in the Frost Radar™: Digital Intelligence Solutions, 2021, Ontic is the first protective intelligence software company to transform how Fortune 500 and emerging enterprises 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 provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals through its Center for Protective Intelligence and Center of Excellence, the latter of which also offers program development and training services in behavioral threat assessment, threat management, and violence prevention for major corporations, educational institutions and government agencies.

For more information please visit www.ontic.co
For inquiries related to the study, contact info@ontic.co



ONTIC | Center for Protective Intelligence

2022 STATE OF PROTECTIVE INTELLIGENCE REPORT

For further insights, please download these additional State of Protective Intelligence Reports