2021 State of Protective Intelligence Report

A MANDATE FOR PROACTIVE PROTECTIVE INTELLIGENCE IN THE ERA OF EXPONENTIAL PHYSICAL SECURITY THREATS

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

ONTIC

Ontic Center for Protective Intelligence

EXECUTIVE SUMMARY

In the face of a global pandemic, remote working from home has for many replaced corporate offices, leaving previously on-the-go corporate heads more vulnerable as they lead from their residences, and a more complex, expanded geographic scope of employees needing protection. At the same time, economic and geopolitical challenges are fueling rises in physical threats to companies. Though corporate physical security has lagged in investing in and adopting modern tools and technologies — particularly compared to cybersecurity — big changes are afoot, accelerated by COVID-19.

Corporate leaders face greater fiduciary scrutiny and personal liability for business continuity, coupled with a growing recognition their organizations are increasingly targets they must protect from harm. A proactive, always-on, data and intelligence-driven function powered by universal, accessible technology has never been more important for corporations, and a physical security digital transformation movement is underway.

Ontic commissioned a survey of 300 chief security officers, chief legal officers, chief compliance officers and physical security decision-makers at U.S. companies with over 5,000 employees, to understand their current physical security operations, what keeps them up at night, the challenges and opportunities they foresee in 2021, and the pressing need for physical security modernization through technology.

In this report, we explore these findings in more detail and expand on other notable results — to fully illuminate the severity of the physical threat landscape, its far-reaching human and business costs, and the watershed opportunity security leaders have to act judiciously, be emboldened to adopt a proactive protective intelligence strategy and help radically transform physical security — and our world — for the better.

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

OUR SURVEY SURFACED THESE KEY TAKEAWAYS:

1. **AMID DRAMATIC RISES** in physical threats, corporate leaders are under unprecedented financial, reputation and liability pressures to keep employees and customers safe from physical harm. Unmanaged physical threats increase corporate risk, can be financially crippling and negatively impact business continuity.

2. **IN THE PAST YEAR,** the lack of unified protective intelligence has resulted in missed threats and physical harm to company employees, customers and human assets. To instill confidence (and proof), physical security, legal, compliance and risk executives are doing everything possible to keep their people and assets safe from physical harm.

3. **DRIVEN BY COVID-19,** which will continue to be a challenge in 2021, modernization solutions have been accelerated and physical security operating budgets are expected to expand. To better avoid crises, however, physical security needs a technology-driven industry standard for actively identifying, investigating, assessing, monitoring and managing physical security risks — and it is way overdue.

CONTENTS

Section 01

THE CURRENT THREAT ENVIRONMENT AND MAJOR CONCERNS

Physical threats are rising and increasingly unmanageable, putting unprecedented financial, reputational and liability pressures on business leadership and security teams.

Companies are experiencing a dramatic increase in physical threat activity as compared to last year, and that physical threat activity has also dramatically increased compared to the beginning of 2020. This rapid change and expansion of the physical threat landscape has created an exponential increase in data and pre-incident indicators that have become unmanageable. What's more, in relation to digital transformation of physical security and physical threat management, company leadership is under more pressure than ever before, from a financial, corporate reputation and liability standpoint, to keep their employees safe from physical harm.

This translates to even greater pressure for those on the front lines. Underscoring this, physical security concerns keeping executives up at night range from keeping remote workers safe and identifying potential threats to reduce company liabilities or save money, to managing threat data volume.

SECURITY, LEGAL AND COMPLIANCE EXECUTIVES AGREE

80%

In relation to digital transformation of physical security and physical threat management, my company leadership would agree they are under more pressure than ever before, from a financial, corporate reputation and liability standpoint, to keep their employees safe from physical harm.

78%

This dramatic change and expansion of the physical threat landscape has created an exponential increase in data and pre-incident indicators that are unmanageable.

71%

Physical threat activity at my company has dramatically increased compared to the beginning of 2020.

69%

My company is experiencing a dramatic increase in physical threat activity as compared to last year.

WHEN YOU THINK ABOUT YOUR COMPANY'S PHYSICAL SECURITY, WHAT KEEPS YOU UP AT NIGHT?

43% Keeping our employees safe as they work remotely

43% Identifying potential threats in order to reduce my company's liabilities

43% Effectively managing the volume of threat data

34% Identifying potential threats in order to save my company money

31% Increased physical threats and company backlash related to racial justice activism or political unrest

31% Protecting our CEO from harm when working from their private residence or while traveling

31% Management is solely focused on cybersecurity

30% Preventing an active shooter event at one of our locations

27% Justifying my position as cyber-physical security operations increasingly merge

27% Staff layoffs and dangerous threats from former employees

26% Our company tries to de-escalate potential threats with financial settlements

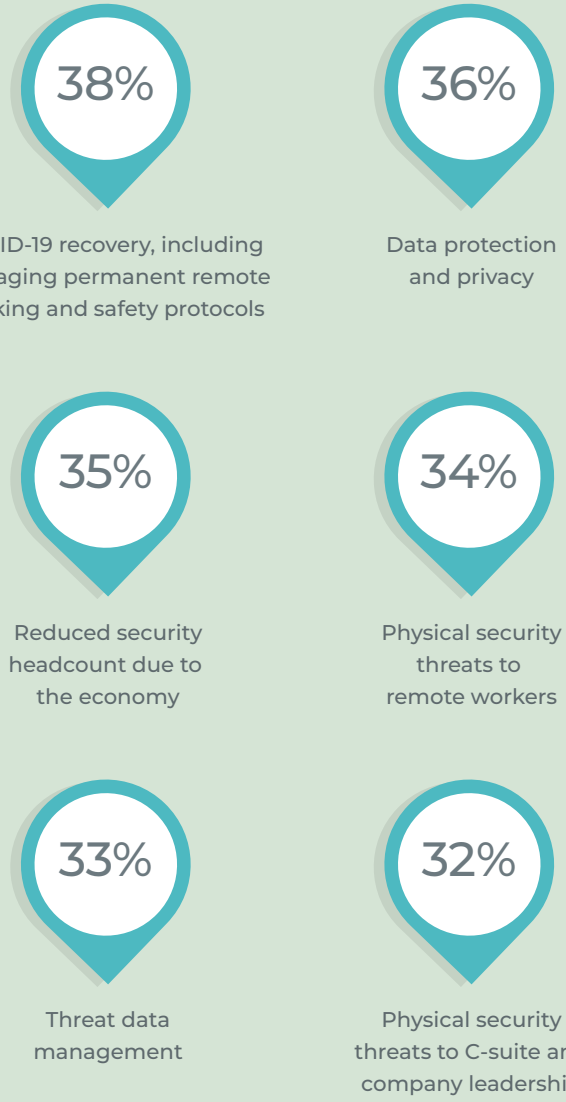
As they prepare to take on what they see as their biggest physical security challenges in 2021, which range from managing new safety protocols, remote workers and physical threats to them as COVID-19 recovery continues; addressing data privacy and security issues; protecting their C-suite and company leadership; potential reductions in security teams due to economics and managing threat data, the overriding sentiment is that physical security needs a technology-driven industry standard for actively identifying, investigating, assessing, monitoring and managing physical security threats, and it is way overdue.

Missed threats and harm have resulted from lack of protective intelligence; catastrophic financial, reputation, and business continuity implications are major concerns.

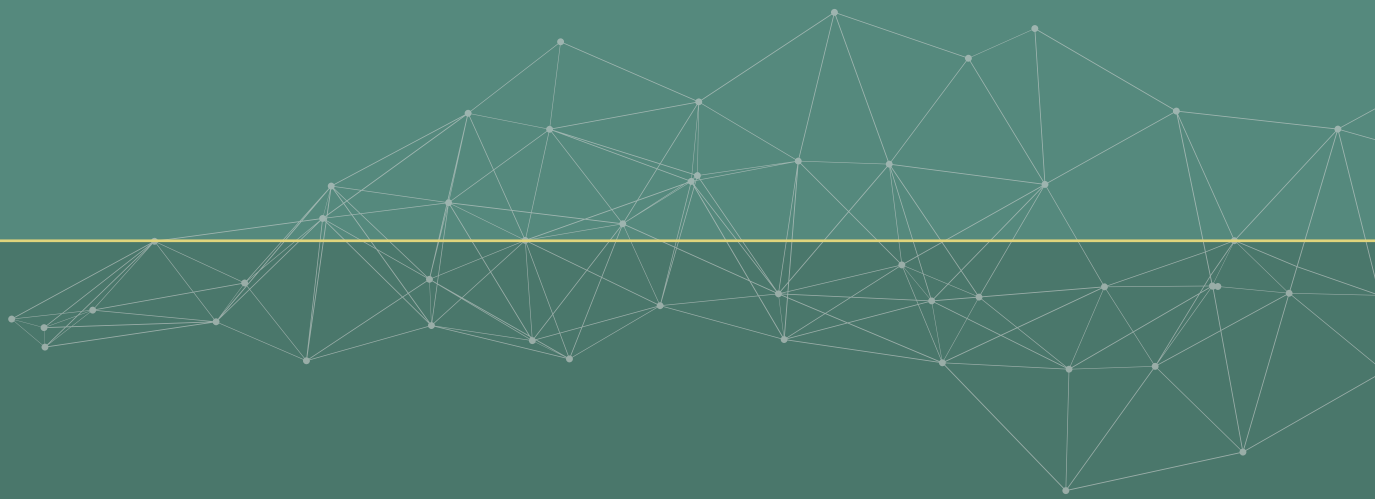
Business continuity is at the heart of these physical security concerns, and 69% say their leadership would agree it will be impossible for their company to recover financially and reputation-wise were a fatality to occur as a result of missed physical threats. But the reality is they are already teetering on the brink of inadequately protecting many aspects of their businesses.

Alarmingly, **71% of respondents agree that in the past year the lack of unified protective intelligence has resulted in missed threats and physical harm** to their company's employees, customers and human assets. So it's not surprising that **84% agree their 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 platform.**

LOOKING AHEAD: BIGGEST PHYSICAL SECURITY CHALLENGES IN 2021

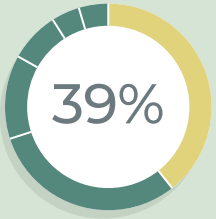


91% of respondents agree that physical security needs a technology-driven industry standard for actively identifying, investigating, assessing, monitoring and managing physical security threats.



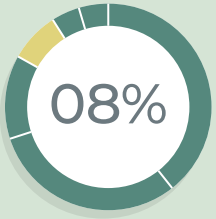
WHEN IT COMES TO PHYSICAL SECURITY THREAT MANAGEMENT, GOOD ENOUGH IS INADEQUATE

Corporate management of physical threats and mitigating damage from threat actors varies, as does how those surveyed describe their company's current approach:



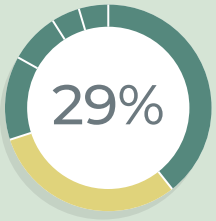
Prevention is better than the cure

We take a proactive, always-on technology-driven approach to managing physical threats so we can detect and mitigate bad actors before damaging incidents occur.



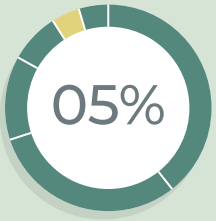
Moving at a snail's pace

We are addressing physical threats through a hodgepodge of disparate manual and digital solutions.



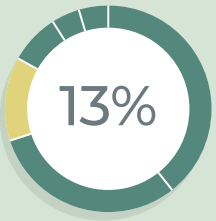
Good enough

Our efforts remain analog, manual and reactive because management does not understand the return on investment, brand reputation and compliance and risk issues.



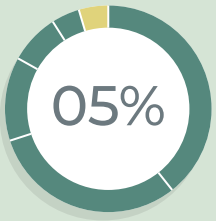
All talk, no action

What is said publicly to stakeholders does not reflect their focus or attention internally.



Whack-a-mole

We react, notify and address threats after they're randomly discovered and it's an ongoing chaotic battle.



Fiefdoms hamper progress

Business units are so focused on protecting their individual budgets and priorities that it makes collaboration and innovation impossible.

Section 02

PHYSICAL SECURITY INVESTMENT PRIORITIES AND COVID-19

Driven by COVID-19, a majority have accelerated physical security modernization plans, shifted investment priorities and expect 2021 operating budgets to increase.

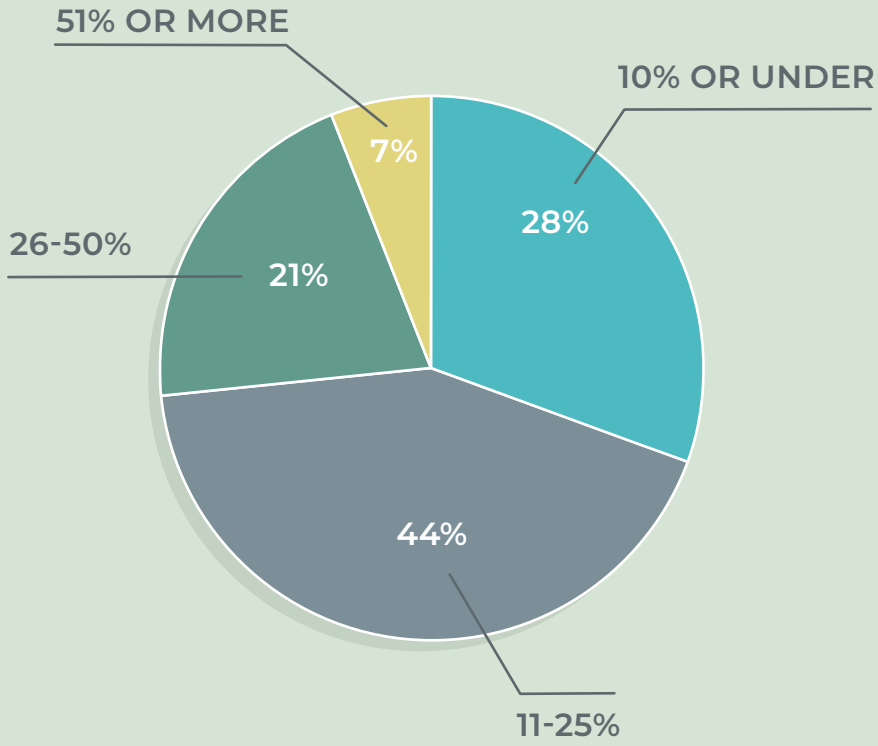
The COVID-19 pandemic, which may be contributing to an increase in physical threat activity, has accelerated physical security modernization plans and positively impacted expected 2021 physical security operating budgets. Most agree (82%) and half (50%) strongly agree that as people continue to work remotely, it is more important than ever for their company to dedicate financial resources to physical security technology solutions at the same level as cybersecurity.

Among those that anticipate an increase, nearly all (97%) attribute an increase in their company's 2021 physical security operating budget at least partially to COVID-19, with 63% citing most or all of the increase due to the pandemic. In the face of the COVID-19 pandemic, 3 out of 4 respondents (78%) feel better prepared to handle physical security for their company as compared to the beginning of the year. In fact, 39% say COVID-19 has caused them to accelerate their timeline for physical security solutions modernization.

Of those surveyed, (80%) expect their company's 2021 physical security operating budget to increase.

EXPECTED INCREASES IN 2021 PHYSICAL SECURITY OPERATING BUDGETS

(Among respondents expecting a physical security operating budget increase)



COVID-19 impact

When asked what vulnerabilities the COVID-19 pandemic has revealed in their company's physical security operations, **common themes were lack of preparedness, remote working challenges and how cybersecurity deficiencies impacted physical security.**

Real-time monitoring and threat reporting, threat assessment training, cyber-physical integration and remote mobile capabilities top immediate and long-term investment priorities.

For more than half of Security, Legal and Compliance leaders (52%), real-time monitoring and threat reporting for their management team is one of their top immediate investment priorities for physical security operations, followed by threat assessment training for their team (51%) and integrating digital physical security operations with cybersecurity (48%).

For 39% of respondents, implementing remote/mobile capabilities and hiring protective intelligence analysts and experts rank among their top five immediate physical security operations investment priorities.

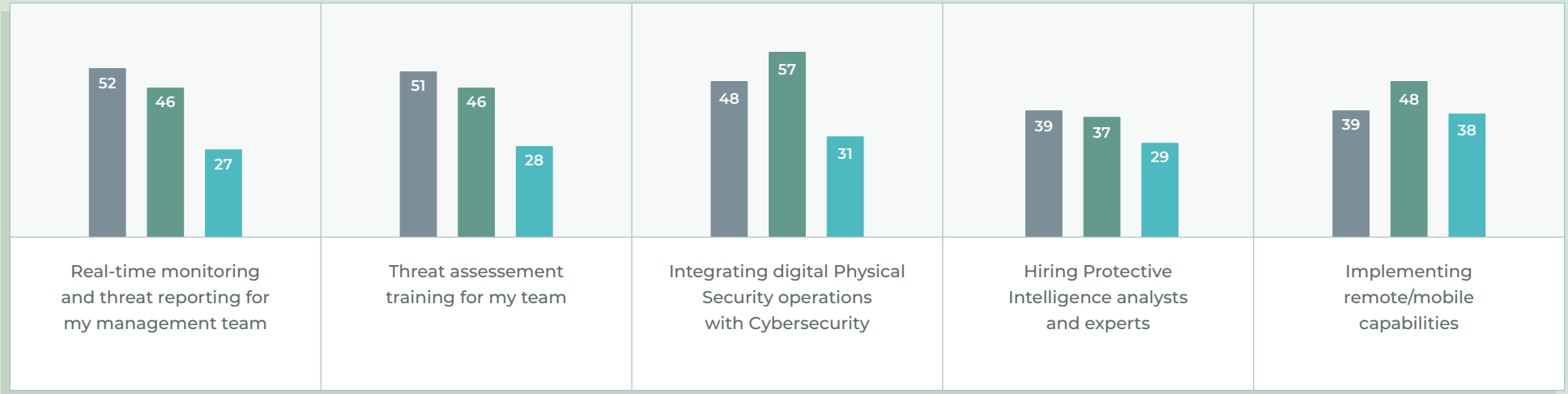
Notably, implementing remote/mobile capabilities (38%), integrating digital physical security operations with cybersecurity (31%), real-time monitoring and threat reporting for management and insider threat monitoring tools and training (27%) were not top investment priorities at the beginning of the year for respondents, but are now.

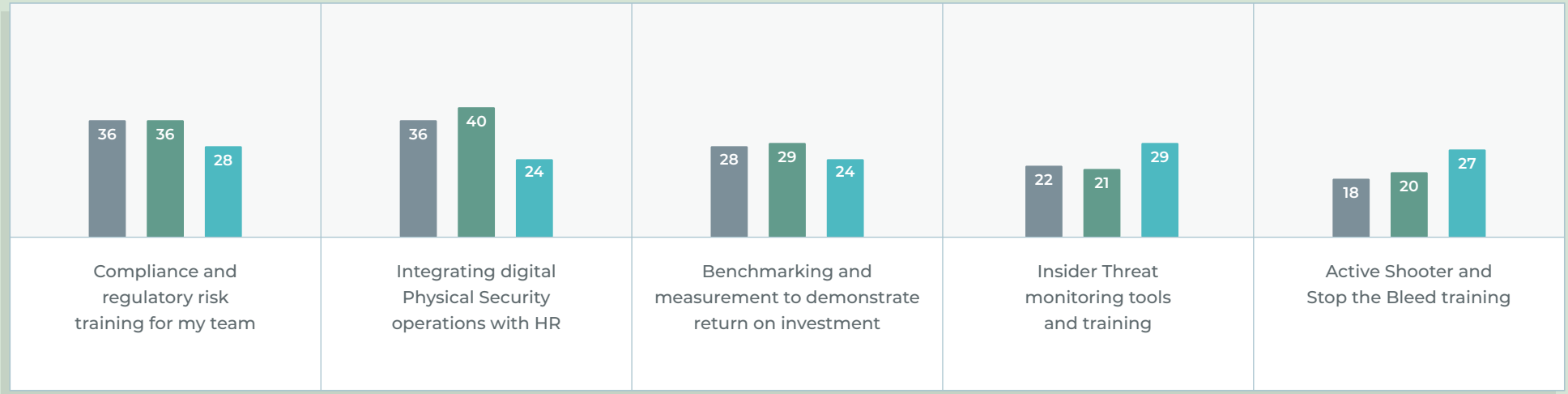
Looking out on the horizon, respondents' top five long-term investment priorities for physical security operations look largely the same, with slight shifts.

Integrating digital physical security operations with cybersecurity is the top long-term investment priority for 57% of those surveyed, followed by implementing remote/mobile capabilities and real-time monitoring and threat reporting for their management team (48%), threat assessment training for their team (46%); real-time monitoring and threat reporting for my management team (46%) and hiring Protective Intelligence analysts and experts (37%). Integrating digital physical security operations with HR (40%) is also a top long-term investment priority.

IMMEDIATE AND LONG-TERM PHYSICAL SECURITY OPERATIONS INVESTMENT PRIORITIES

% Immediate | % Long-term | % Not a top priority at the beginning of the year but is now





Section 03

COMPLIANCE, RISK AND REGULATIONS

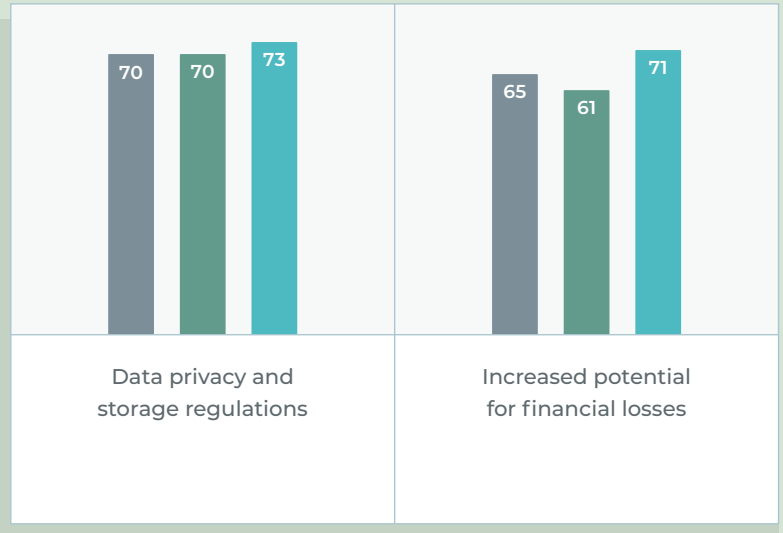
Data privacy, greater need for corporate self-protection, potential for financial loss and personal liability of C-suite permeate compliance, risk and regulation issues.

Physical security strategies can be greatly impacted by corporate compliance, risk and regulation issues, and seven out of 10 of those surveyed (70%) cite data privacy and storage regulations as among the top 3, followed by increased potential for financial losses (65%), and that corporations have now become targets and can no longer rely on others for protection (54%).

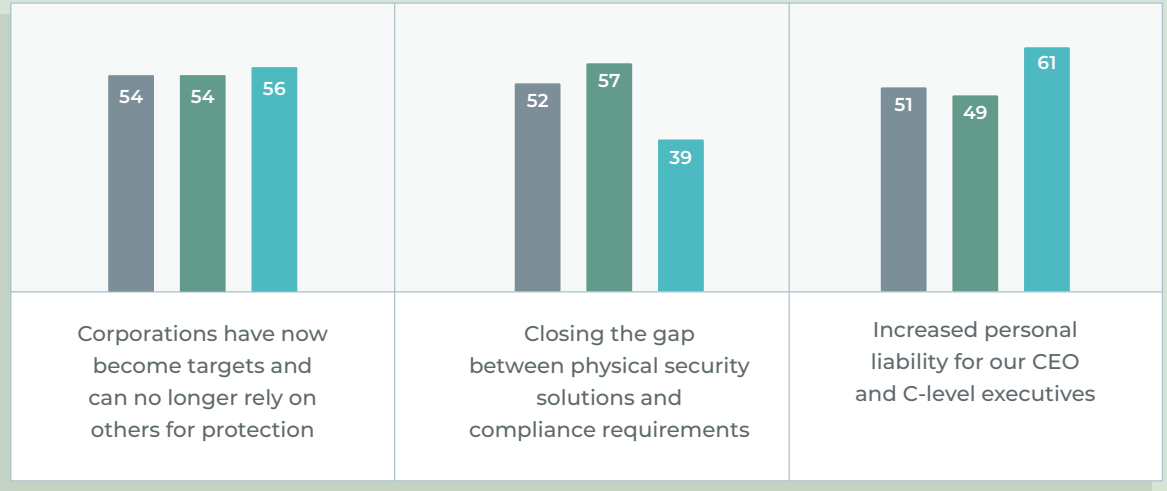
Additionally, the top 5 immediate priorities for integration and cross-functional communication with physical security operations include management reporting/ alerting (76%), cybersecurity alignment (75%), changing the Chief Information Security Officer (CISO) reporting structure to encompass cyber, physical security, HR and legal/compliance (66%), compliance (62%) and implementation of a company-wide crisis plan (53%).

TOP COMPLIANCE, RISK OR REGULATION ISSUES IMPACTING PHYSICAL SECURITY STRATEGY

% All respondents | % Security leaders | % Legal and Compliance leaders



Among Legal and Compliance leaders more than seven out of 10 (71%) rank increased potential for financial losses as a top 3 compliance, risk or regulation issue impacting physical security strategy.



Section 04

THE PROTECTIVE INTELLIGENCE IMPERATIVE

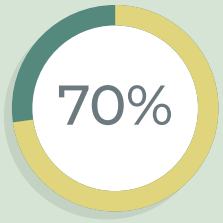
Now is the best time to invest in physical security digital transformation, critical for protecting companies financially, culturally, brand-wise — and for their future.

A strong majority of those surveyed agree (90%) — half strongly agree (51%) — that now is the best time to invest in physical security digital transformation, and unmanaged physical threats increase corporate risk, can be financially crippling and negatively impact business continuity (84% agree).

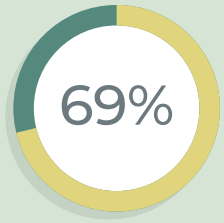
Security leaders who do not adopt a digital mindset, 81% agree, will quickly be business irrelevant. Nearly nine in 10 (87%) agree digitally transforming their physical security solutions would play a critical role in protecting their company financially, culturally and brand-wise, while **87% agree investment in technology to advance physical security effectiveness and mitigate violent threats is necessary for the future of their company.**

PHYSICAL SECURITY IMPLEMENTATION PRIORITIES

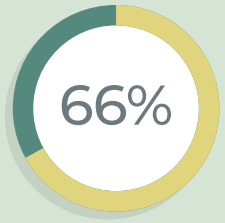
About two-thirds or more are interested in implementing an array of technology-driven solutions and physical security initiatives to better protect their companies including:



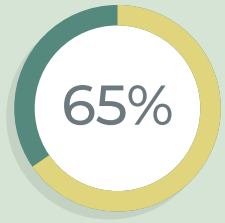
Automating potential threat identification and pre-incident indicators



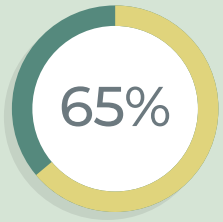
The ability to connect all aspects of threat management journey



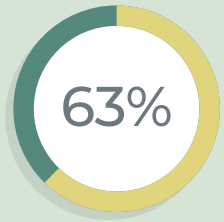
Protective intelligence analysts



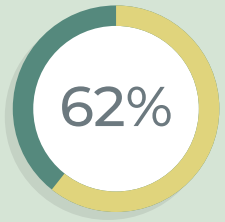
Cyber-physical security operation center, compliance projects, training for legal/liability initiatives



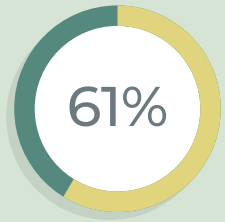
Compliance projects



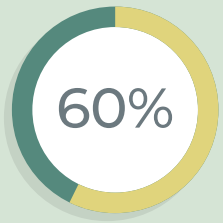
Software-as-a-service (SaaS)-based threat management platform



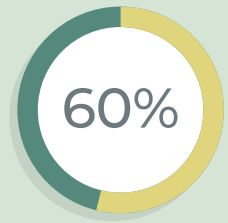
Investigation protocols and processes



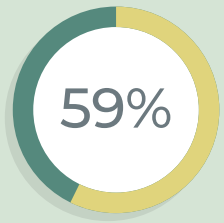
Always-on threat actor monitoring, and mobile threat management



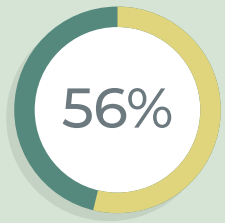
Mobile threat management



Event notification system



Threat assessment training



Identity authentication

The benefits of digital transformation

When asked what they believe is the greatest benefit from digital transformation of physical security, most **common themes were increases in overall security, more efficient processes and earlier detection of threats.**

"The greatest benefit from the transformation of physical security is that it has been more efficient and reduces the tedious manual working job."

"It will keep physical security relevant and effective in the modern era."

"Now, more than ever, physical security is a huge issue for many organizations the world over. It's not just in the United States, where we regularly see active shooter situations, but also internationally, where similar dangerous attacks occur. There's a real concern when it comes to locking down and protecting a corporate campus from would-be attackers."

"Understanding when and where attacks might come from and what can be done to prevent and mitigate damage."

"The complexity of managing current threats often gets in the way, leaving less time to focus on proactive threat management. Digital transformation empowers these operators with systems that contextualize data to identify threats before they occur, mitigate risks and better ensure life safety."

"The greatest benefit is reducing the human component of it. Not necessarily reducing jobs but automating processes to ensure human lives are more protected from threats."

"One of the greatest benefits is ... a faster and easy compilation of information for my department to evaluate and always be one step ahead of any eventuality."

"All data is compiled, categorized and shared in real time and the time from when a potential threat is noticed until it is acted upon is decreased."

"People and businesses are able to assess and attest to many physical threats while maintaining social distancing and without having a liability on our hands."

"Better communication between departments, better compliance, faster reactions, and detecting threats more efficiently."

"To keep ourselves updated with the smallest potential threat that can cause any harm to business or employee."

About the study

A total of 300 respondents completed the survey, which was conducted between October 13-30, 2020. These included chief security officers, chief legal officers, chief compliance officers, general counsels, corporate attorneys and physical security decision-makers at U.S. companies with over 5,000 employees. For inquiries related to the study, contact us via email at info@ontic.ai.

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, pharmaceutical, entertainment, consumer products and more. 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 about Ontic please visit www.ontic.ai.

ONTIC | Center for Protective Intelligence

2021 STATE OF PROTECTIVE INTELLIGENCE REPORT