EXECUTIVE SUMMARY SPOTLIGHT

2022 Mid-Year Outlook State of Protective Intelligence Report

THE PERSPECTIVE FROM PHYSICAL SECURITY LEADERS

Ontic Center for Protective Intelligence

Protecting companies and mitigating risk: Physical security is not on its own

Protecting corporate executives, employees, customers and assets is the responsibility of physical security leaders and human resources colleagues.

As American corporations experience an increased volume and wider range of threats driven by strong political, social and economic headwinds, it's no longer a question that physical harm and damage can be done through cyber means.

While physical security leaders will always need and be relied on for their deeper specialized expertise, the heightened threat landscape, technology adoption and consolidation mean the walls between lines of business are falling with the recognition that data-sharing raises the effectiveness of all.

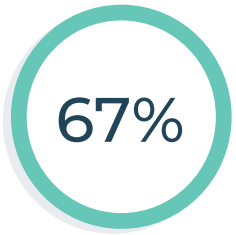
Among physical security executives, 61% say to date in 2022, their company received or investigated one or more threats per week, including 15% that received 2-5 per week.

DEFINITIONS AND VOLUME OF THREATS AND BUSINESS RISKS

(According to physical security leaders)

Threat description and % of physical security executives surveyed that said it expresses how their line of business defines and describes business threats

Number of threats and business risks physical security deals with annually



Hostile written, verbal or physical actions with the potential to compromise individuals' mental or physical well-being at the workplace or while on duty.

None	9%
1-2 per year	21%
3-5 per year	13%
6-10 per year	24%
11-25 per year	10%
26-50 per year	10%
+50 per year	10%

Extreme weather events that compromise the safety and integrity of infrastructure, including buildings, facilities and working conditions for executives and employees.

None	11%
1-2 per year	19%
3-5 per year	23%
6-10 per year	23%
11-25 per year	12%
26-50 per year	5%
+50 per year	5%

Actions or events that compromise company adherence to regulations and laws.

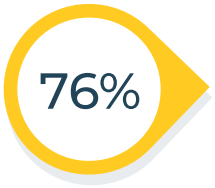
None	14%
1-2 per year	17%
3-5 per year	19%
6-10 per year	25%
11-25 per year	11%
26-50 per year	3%
+50 per year	8%

Threat assessment and management are critical, but it's unclear which department takes the lead.

Being able to identify potential trouble in the workplace that may be on the horizon is increasingly important as threats to businesses rise. Almost all physical security executives say that behavioral threat assessment or threat management training is important for their team to successfully execute their job (99% say it is important, including 65% who say it is very important).

Of the potentially violent and harmful threats their company received in 2022, physical security, cybersecurity and IT, human resources, and legal and compliance executives surveyed said most (32%), some (29%) and a few (22%) violent and harmful threats received surfaced because physical security observed an employee demonstrating suspicious behavior.

Though a majority of physical security executives agree (80%) that along with their department, cybersecurity and IT, human resources and legal and compliance professionals have also been adequately trained to assess threats — which includes reporting erratic behavior and warning signs that could lead to workplace violence — there is confusion over which department "owns" threat assessment and management.



Among physical security respondents, 76% said physical security is responsible for threat assessment and management while 70% said they should be responsible.

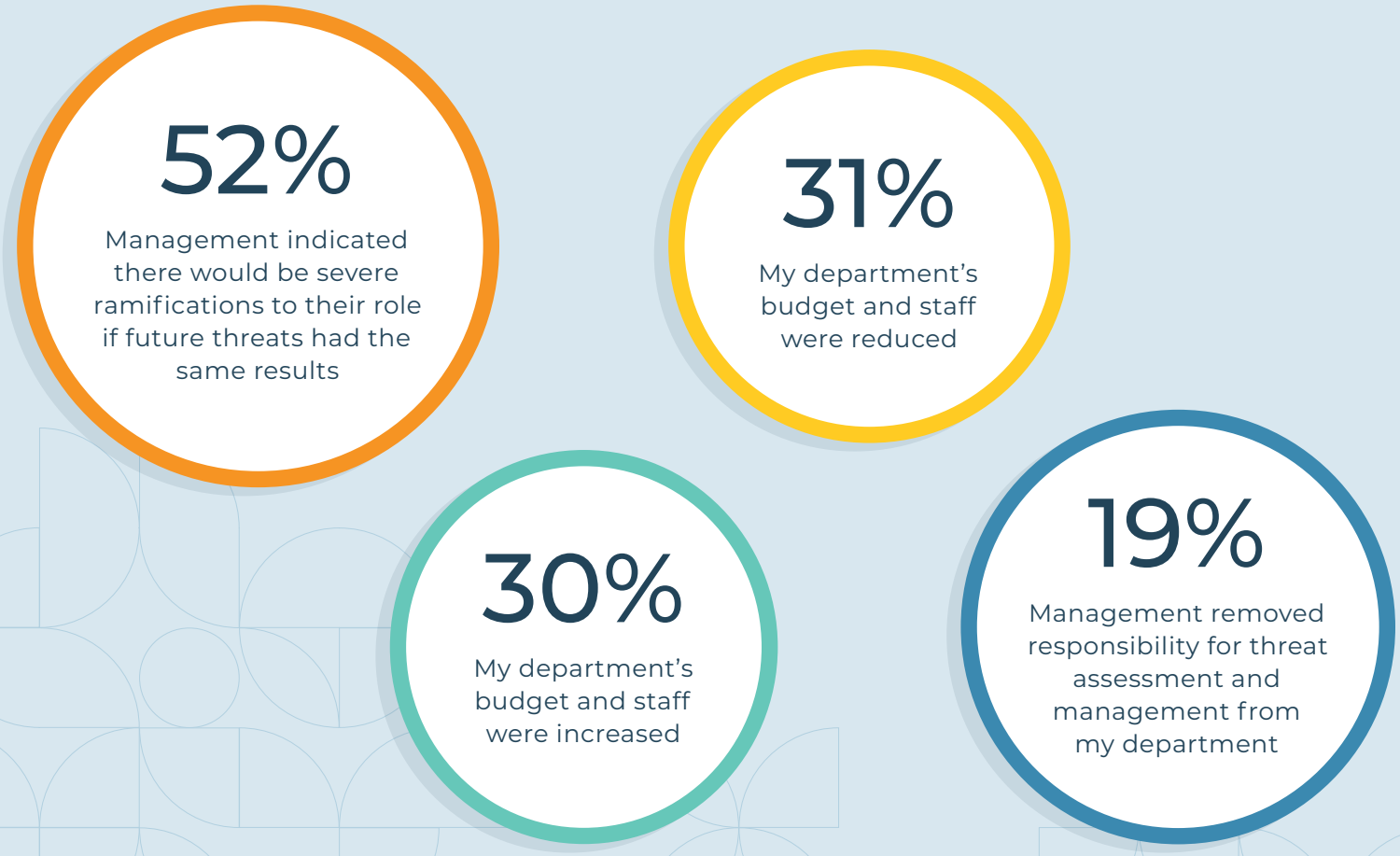
Most other respondents thought their own departments had and should have primary responsibility: 62% of human resources said they are responsible, 49% of cybersecurity and IT said they are responsible; and 47% of legal and compliance said they are responsible.

Implications for physical security

This disagreement — or confusion — among respondents is vital to try to remedy, as it could likely translate into confusion in threat investigations, assessment, and threat management planning and is a failure to meet the ASIS Standard for workplace violence prevention.

What's more, when physical security professionals are not able to identify threats before they cause harm or damage, there can be repercussions for their leaders and department. For more than half of physical security executives (52%) who have missed threats in 2022 (were not able to identify them before they caused harm or damage at their company), management indicated there would be severe ramifications to their role if future threats had the same results; 31% had their department's budget and staff reduced; 30% had budget and staff increased and over one-quarter (19%) had responsibility for threat assessment and management removed from their department by management.

IN 2022, WHEN THREATS WERE NOT ABLE TO BE IDENTIFIED BEFORE THEY CAUSED AN ISSUE:



Data-sharing and cross-functional collaboration can only benefit physical security

A strong majority of physical security executives (93%) say that their department is often assessing and investigating the same threat as their cybersecurity and IT, human resources, and legal and compliance colleagues, but independently from each other, including 54% who say this happens very often.

With this threat assessment and management redundancy and inefficiency at companies, and physical security leaders' multiple concerns in 2022, which range from keeping employees safe as they return to the office or work remotely, protecting the CEO and senior executives from harm while working at their private residence or traveling, to the increased volume of threat data and pressure to identify threats to save their company money and reduce liabilities, it follows that physical security leaders anticipate they will miss threats.

Data-sharing is key to all parties being informed and mitigating threats. In 2022, because of an inability to successfully collect, collate and share information across physical security, human resources, cybersecurity and IT, and legal and compliance departments, respondents said an employee was threatened and/or harmed while working at company facilities (38%), an insider abused authorized cyber access that led to property theft or supply chain damage (35%), a former employee threatened and/or harmed a current employee (34%) and an employee was threatened and/or harmed while working remotely (31%).

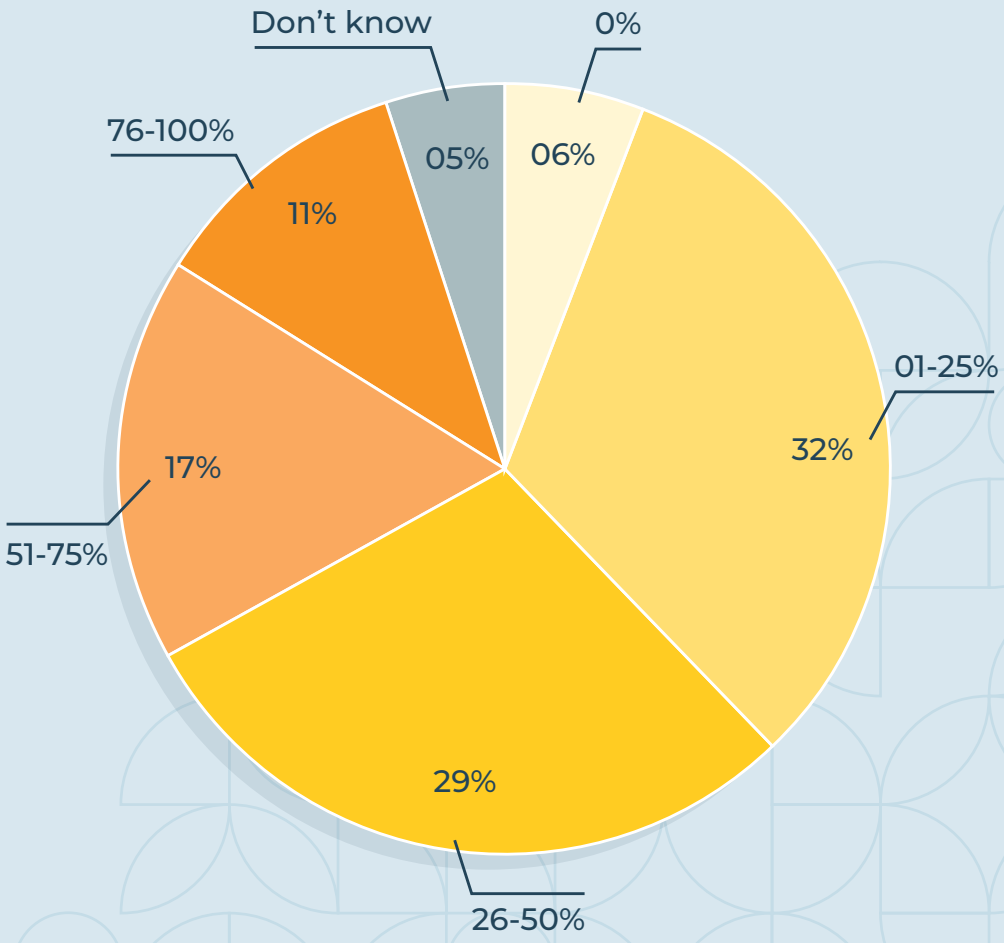
2022 PHYSICAL SECURITY PROGRAM CONCERNS

Tech consolidation and single universal software platforms to share data

A substantial percentage of threats that disrupted business continuity or resulted in harm or death at companies in 2022 could have been avoided if all functions surveyed shared and viewed the same intelligence in a single software platform. Nearly half (46%) of physical security executives said 26-75% of threats could have been avoided while 32% said 1-25% of threats could have been avoided and 11% said as high as 76-100%.

But the widespread movement to digitally transform physical security into a single platform continues to gain momentum. A majority (85%) of physical security executives agree their company is actively consolidating their multiple threat intelligence, data analysis and reporting solutions into a single software platform across physical security, cybersecurity and IT, human resources, and legal and compliance.

PERCENTAGE OF THREATS IN 2022 THAT DISRUPTED BUSINESS CONTINUITY, RESULTED IN HARM OR DEATH — BUT COULD HAVE BEEN AVOIDED — IF PHYSICAL SECURITY, HUMAN RESOURCES, CYBERSECURITY AND IT, LEGAL AND COMPLIANCE SHARED AND VIEWED THE SAME INTELLIGENCE IN A SINGLE SOFTWARE PLATFORM



EXECUTIVE SUMMARY SPOTLIGHT

2022 Mid-Year Outlook
State of Protective Intelligence Report

THE PERSPECTIVE FROM PHYSICAL SECURITY LEADERS

About the study

Ontic surveyed 400 executives across four different departments at U.S. enterprises who have responsibilities for protecting businesses: physical security, cybersecurity and IT, human resources, and legal and compliance.

Download the full report

To read the full 2022 Mid-Year Outlook State of Protective Intelligence Report, including the perspective from physical security, cybersecurity and IT, human resources, and legal and compliance leaders, visit ontic.co/stateofPI or download here: