2022 Mid-Year Outlook State of Protective Intelligence Report

THE PERSPECTIVE FROM PHYSICAL SECURITY, CYBERSECURITY AND IT, HUMAN RESOURCES AND LEGAL AND COMPLIANCE LEADERS

Ontic Center for
Protective Intelligence

Strong political, social and economic headwinds persist as the United States heads into the fall of 2022. Corporations continue to experience an increased volume of threats and many of the communities where they reside are rattled. The increasing frequency of mass shootings contributes to growing security concerns — at Robb Elementary School in Uvalde, TX; during a parade in Highland Park, IL; at a medical building next to Saint Francis Hospital in Tulsa, OK; in downtown Philadelphia, PA; the worst attack on New York City's subway system in decades; a Tops supermarket in a predominantly Black section of Buffalo, NY and the Irvine Taiwanese Presbyterian Church in Laguna Woods, CA. In many of these cases, prior known and sometimes reported violent behaviors and actions by the shooter, often on social media, came to light after the event occurred.

Civil unrest continues in the wake of recent Supreme Court decisions, and inflation hovers alongside potential recession fears. While employment and demand for talent remain high, some sectors have experienced layoffs. As companies navigate return to in-person work as COVID recedes, they also have to keep track of new variants that have the potential to drive spikes in cases and fuel undercurrents of concern. The House Select Committee investigating the events of January 6 and looming midterm elections are contributing to political uncertainty as geopolitical events such as the war in Ukraine impact supply chains and food production.

In June, The Department of Homeland Security issued a National Terrorism Advisory System (NTAS) Bulletin, its sixth since the beginning of 2021, regarding the continued heightened threat environment across the U.S.

> "In the coming months, we expect the threat environment to become more dynamic as several high-profile events could be exploited to justify acts of violence against a range of possible targets. Threat actors have recently mobilized to violence due to factors such as personal grievances, reactions to current events, and adherence to violent extremist ideologies, including racially or ethnically motivated or anti-government/anti-authority violent extremism. Foreign adversaries—including terrorist organizations and nation state adversaries—also remain intent on exploiting the threat environment to promote or inspire violence, sow discord, or undermine U.S. democratic institutions. We continue to assess that the primary threat of mass casualty violence in the United States stems from lone offenders and small groups motivated by a range of ideological beliefs and/or personal grievances."

© Ontic Technologies, Inc. 2022

EXECUTIVE SUMMARY

Protecting corporate executives, employees, customers and assets is primarily the responsibility of physical security, cybersecurity and IT, human resources and legal and compliance leaders. Their mutual concerns regarding their companies' physical security programs in 2022 are many:

- An increased volume of threat data
- Keeping employees safe as they return to the office but also work remotely
- Threat data being held in departmental silos is hampering effective company-wide threat and risk management
- Greater pressure to identify threats to save the company money and reduce liabilities
- Management's heavier focus on global risk and supply chain security compared to local security issues

About two-thirds of those surveyed said that, to date in 2022, their company received or investigated one or more threats weekly, including one-quarter that are on track to receive or investigate up to 260 threats annually. For those responsible for protecting businesses, not being able to identify threats before they cause harm or damage can have severe ramifications for their roles. And while physical security, cybersecurity and IT, human resources and legal and compliance leaders believe they are adequately trained in threat assessment, a majority anticipate in the next six months they will miss up to half the threats at their company due to the volume of threats, lack of data sharing, and poor communication, among other reasons.

The four departments surveyed are assessing and investigating the same threats independently from each other. This significant redundancy and inefficiency, fortunately, is being addressed because a universal movement at U.S. companies to actively consolidate their multiple threat intelligence, monitoring and alerting solutions into a single software platform continues. This transformation is enabling holistic data analysis for deeper visibility, speedy decision-making and clear communications across these functions and the enterprise when it's most critically needed.

© Ontic Technologies, Inc. 2022

An increasing number of threats is permeating a wider range of areas that will only become greater. That physical harm can be facilitated through cyber means is no longer a question. Nor is the ability of technology to unite all threat intelligence in one shared platform, or to train leaders and employees to identify and assess threats before they cause harm and devastation. To function in this new turbulent normal, to grow and thrive, organizations must cultivate a culture of security. Information, action, communication, training and habit can mitigate business and mission-critical threats and liabilities, preserve business integrity and ensure critical resilience.

The Ontic Center for Protective Intelligence commissioned its 2022 mid-year outlook survey to examine how physical security challenges and opportunities have been unfolding halfway through the year, where they are headed and the potential impact on business continuity and resilience. The survey was conducted from June 8 – July 1, 2022.

A TOTAL OF 400 RESPONDENTS AT U.S. COMPANIES WITH OVER 5,000 EMPLOYEES WERE SURVEYED, INCLUDING:

- Chief Security Officers
- Chief Human Resources Officers
- Chief Legal Officers
- Chief Compliance Officers
- Chief Information Security Officers
- Chief Technology Officers
- Chief Information Officers
- Director-level or equivalent decision-makers

INDUSTRIES COVERED:

- Automotive
- Banking and Financial Services
- Consumer Goods
- Education
- Energy
- Government
- Healthcare
- Insurance
- Media and Entertainment
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Travel and Hospitality

© Ontic Technologies, Inc. 2022

OUR MID-YEAR STUDY SURFACED THESE KEY TAKEAWAYS

1

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

Though there's universal agreement that identifying concerning behavior, obtaining intelligence that a threat may be on the horizon, making an assessment and taking action to mitigate such threats is very important, there are differences regarding who has or should have primary responsibility for threat assessment at companies. This could likely result in further confusion in threat investigations, assessment and planning.

2

Threats are vast, growing, unrelenting and will be missed

In the next six months, a significant number of threats are anticipated to be missed at American companies. Nearly one-third anticipate they will not be able to identify 1-25% of threats before they cause harm or damage, close to one-third anticipate missing 26-50% and more than one-quarter anticipate missing 51% or more.

3

Threats to businesses are defined in many ways, not just events that compromise IT and network security

Threats encompass hostile written, verbal or physical actions against others at work, events that compromise a company's adherence to regulations and laws, extreme weather events that impact the safety and integrity of buildings and working conditions and extreme rhetoric or hate speech on social media.

4

'Emperor's new clothes' security strategies, workplace violence fatigue prevail

Companies emulate a safe environment by downplaying risks and have not addressed the potential for workplace violence. Many have workplace violence fatigue, which could result in failure to follow up on threats and other troubling behaviors that should be investigated, assessed and managed to reduce risk.

© Ontic Technologies, Inc. 2022

5

Communication silos and redundant threat assessments will be mitigated by universal software technology

Communication silos continue, and different departments are assessing the same threat individually, increasing the likelihood that security decisions are being made without full information. But U.S. companies are also actively consolidating their multiple threat intelligence, monitoring and alerting solutions into a single software platform. Survey data shows it can't happen fast enough: about half said 51% or more of threats that disrupted business continuity resulting in harm or death at their company in 2022 could have been avoided if physical security, human resources, cybersecurity and IT, and legal and compliance shared and viewed the same intelligence in a single software platform.

6

People-centered functions are in the first line for protection and risk mitigation

Human resources executives are increasingly co-owning and responsible for business continuity and resilience. While physical security, cybersecurity and IT, human resources and legal and compliance leaders will always need and be relied on for their deeper specialized expertise, the heightened threat landscape, technology adoption and consolidation mean walls are falling with the recognition that data-sharing raises the effectiveness of all.

PRO·TECT·IVE IN·TEL·LI·GENCE

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

CONTENTS

2022 Mid-Year Outlook
State of Protective Intelligence Report

07 Section 01
THREATS AMERICAN COMPANIES ARE RECEIVING: WHAT THEY ARE, WEEKLY AND ANNUAL VOLUME, WHO DEALS WITH THEM

13 Section 02
ATTITUDES, STANCES, RHETORIC AND BACKLASH

16 Section 03
THREAT ASSESSMENT AND MANAGEMENT: POLICIES, PRACTICES, TRAINING AND OWNERSHIP

24 Section 04
COMMUNICATION SILOS PERSIST, BUT CROSS-FUNCTIONAL 'TASK FORCES' ARE EMERGING

31 Section 05
PHYSICAL SECURITY CONVERGENCE, CONSOLIDATION GAINING MOMENTUM

© Ontic Technologies, Inc. 2022

SECTION 01

THREATS AMERICAN COMPANIES ARE RECEIVING: WHAT THEY ARE, WEEKLY AND ANNUAL VOLUME, WHO DEALS WITH THEM

© Ontic Technologies, Inc. 2022

While physical security, cybersecurity and IT, human resources, and legal and compliance all deal with threats and business risks, how each function defines them can differ. When asked which of six statements express how their line of business defines and describes threats and business risks at their company, each function selected every statement, but at different levels.

Among physical security, cybersecurity and IT and legal and compliance executives, within each function, close to two-thirds selected the same single statement. But around two-thirds of human resources leaders selected four of the six statements — indicators that they define threats across an organization in broad and diverse ways, and align and overlap with multiple colleagues' functions.

- **Threat definition** *"Hostile written, verbal or physical actions with the potential to compromise individuals' mental or physical well-being at the workplace or while on duty"* – selected by 67% of physical security and 66% of human resources executives; 55% of legal and compliance and 45% of cybersecurity and IT executives;
- **Threat definition** *"Actions or events that compromise company adherence to regulations and laws"* – selected by 69% of human resources and 63% of legal and compliance executives; 54% of cybersecurity and IT and less than half (49%) of physical security executives;
- **Threat definition** *"Negative actions or events that compromise the security of your company's IT and network systems"* – selected by 70% of cybersecurity and IT, and 68% of human resources executives; 47% of legal and compliance, 36% of physical security executives;
- **Threat definition** *"Extreme weather events that compromise the safety and integrity of infrastructure, including buildings, facilities and working conditions for executives and employees"* – selected by 63% of human resources and 61% of legal and compliance; 57% of physical security and 48% of cybersecurity and IT executives;

Interestingly, human resources was the only function where a majority (58%) selected *extreme rhetoric, hate speech on social media, in writing or conversation,* despite growing consensus among threat assessment experts that such behavior indicates a potential pathway to violence.

The volume of threats or business risks each line of business says they deal with over the course of a year varies by type. Notably, just over one-fifth (21%) of physical security executives say they do not ever deal with extreme rhetoric or hate speech on social media. This may be because, at many companies, monitoring and flagging concerning issues on social media is owned by marketing.

© Ontic Technologies, Inc. 2022

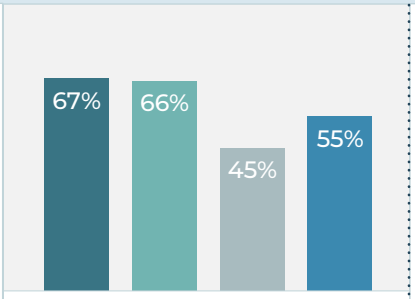
DEFINITIONS AND VOLUME OF THREATS AND BUSINESS RISKS *(According to lines of business)*

Total Respondents | Physical Security Respondents | Human Resources Respondents | Cybersecurity and IT Respondents | Legal and Compliance Respondents

THREAT DESCRIPTION AND % SURVEYED THAT SAID IT EXPRESSES HOW THEIR LINE OF BUSINESS DEFINES THREATS AND BUSINESS RISKS

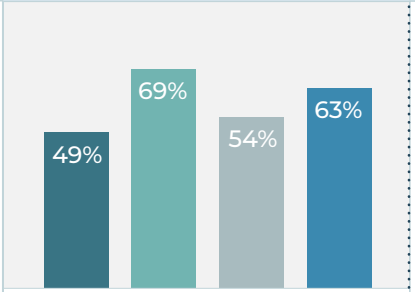
NUMBER OF THREATS AND BUSINESS RISKS LINE OF BUSINESS DEALS WITH ANNUALLY

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



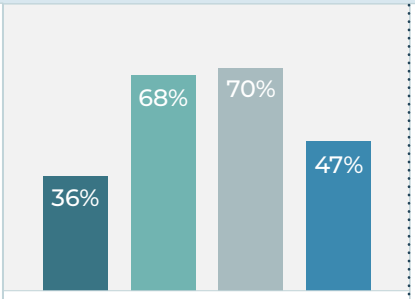
None	5%	9%	2%	4%	4%
1-2 per year	15%	21%	9%	16%	13%
3-5 per year	20%	13%	24%	18%	25%
6-10 per year	28%	24%	35%	24%	27%
11-25 per year	18%	10%	18%	24%	24%
26-50 per year	6%	10%	5%	7%	4%
+50 per year	7%	10%	8%	7%	4%

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



None	3%	14%	0%	1%	2%
1-2 per year	14%	17%	12%	11%	17%
3-5 per year	25%	19%	37%	19%	21%
6-10 per year	28%	25%	34%	29%	21%
11-25 per year	18%	11%	9%	24%	28%
26-50 per year	3%	3%	1%	3%	6%
+50 per year	8%	8%	6%	11%	4%

Negative actions or events that compromise the security of your company's IT and network systems.



None	6%	16%	6%	4%	2%
1-2 per year	19%	27%	22%	13%	16%
3-5 per year	22%	12%	25%	31%	17%
6-10 per year	26%	24%	29%	30%	21%
11-25 per year	14%	10%	10%	17%	19%
26-50 per year	6%	4%	4%	2%	11%
+50 per year	6%	6%	3%	4%	13%

© Ontic Technologies, Inc. 2022

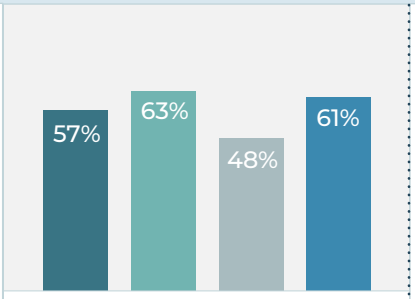
DEFINITIONS AND VOLUME OF THREATS AND BUSINESS RISKS *(According to lines of business)*

Total Respondents | Physical Security Respondents | Human Resources Respondents | Cybersecurity and IT Respondents | Legal and Compliance Respondents

THREAT DESCRIPTION AND % SURVEYED THAT SAID IT EXPRESSES HOW THEIR LINE OF BUSINESS DEFINES THREATS AND BUSINESS RISKS

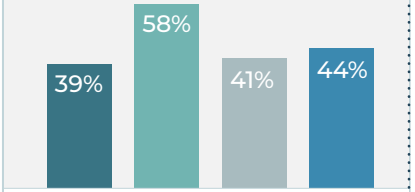
NUMBER OF THREATS AND BUSINESS RISKS LINE OF BUSINESS DEALS WITH ANNUALLY

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



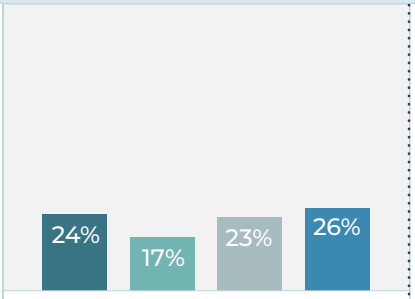
None	4%	11%	3%	2%	2%
1-2 per year	19%	19%	22%	21%	13%
3-5 per year	22%	23%	19%	19%	28%
6-10 per year	29%	23%	33%	27%	33%
11-25 per year	16%	12%	19%	15%	16%
26-50 per year	5%	5%	2%	6%	7%
+50 per year	4%	5%	2%	10%	2%

Extreme rhetoric, hate speech on social media, in writing or conversation.



None	7%	21%	2%	5%	2%
1-2 per year	12%	13%	21%	2%	9%
3-5 per year	19%	13%	21%	17%	25%
6-10 per year	33%	26%	33%	32%	41%
11-25 per year	18%	10%	19%	32%	11%
26-50 per year	5%	10%	3%	5%	5%
+50 per year	4%	5%	2%	5%	5%

Geopolitical risks.



None	13%	33%	6%	9%	4%
1-2 per year	17%	21%	12%	17%	15%
3-5 per year	28%	21%	29%	22%	38%
6-10 per year	20%	13%	29%	17%	23%
11-25 per year	13%	4%	12%	26%	12%
26-50 per year	3%	4%	0%	4%	4%
+50 per year	4%	4%	12%	4%	0%

© Ontic Technologies, Inc. 2022

Security concerns are many: threats are vast, growing, unrelenting and will be missed.

With a multitude of concerns ranging 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 respondents anticipate they will miss threats.

2022 PHYSICAL SECURITY PROGRAM CONCERNS *(Respondents asked to select all that apply)*

- 37% Keeping our employees safe as they return to the office
- 34% The increased volume of threat data
- 34% Increased pressure to identify potential threats in order to save my company money and reduce liabilities
- 32% Management is predominantly focused on global risk and supply chain security issues so mitigating location-specific physical threats is not a priority
- 32% Keeping our employees safe as they work remotely
- 31% Increased physical threats and company backlash related to geopolitical, activism and social issues
- 30% Threat data is held in different departmental silos and not shared so it is difficult to effectively manage the volume of threat data across the company
- 30% Cyber-related insider threats that also share physical security implications
- 29% Protecting our CEO and senior executives from harm when working from their private residence or while traveling
- 28% Identifying employees with extremist views and mental health issues
- 27% COVID variant spikes and the impact on employee mental health
- 27% Potential threats from former employees
- 26% Leadership is predominantly focused on cybersecurity and believes it does not strongly tie to physical security risks
- 26% Preventing an active shooter event at one of your locations
- 22% Increased physical threats to my CEO and senior executives and company posted on social media

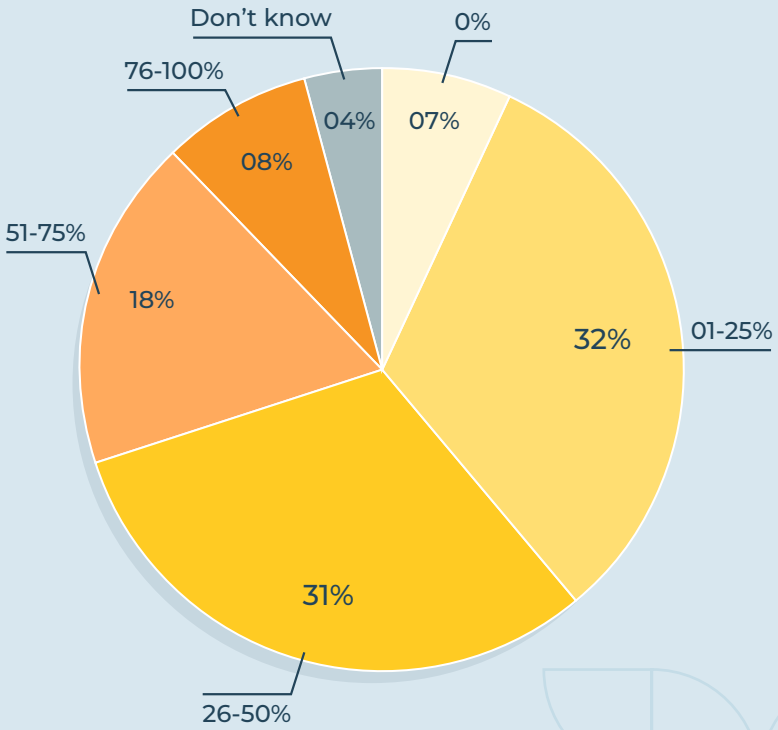
© Ontic Technologies, Inc. 2022

In the next six months it is anticipated that a significant number of threats will be missed at American companies. About one-in-four (26%) anticipate missing at least 51% of threats, while another 31% anticipate missing 26%-50% of threats, and 39% anticipate missing 25% of threats or fewer.

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%).

The actions companies take in the wake of threats and violence can have a lasting impact on culture, morale, behaviors and keeping all safe in the future. While more needs to be done more consistently at businesses, 63% of those who had one of the above such incidents said after an employee was threatened and/or harmed at one of its locations or while working remotely, their company reassessed and revised their existing Threat Assessment Management Team or something similar to eliminate vulnerable gaps. Sixty-two percent implemented a Threat Assessment Management Team or something similar for the first time as well as active shooter training exercises. Staff was trained in how to Stop the Bleed (39%), additional security personnel were hired at the location (35%) and 5% closed the location altogether.

PERCENTAGE OF THREATS ANTICIPATED TO BE MISSED AT BUSINESSES IN THE NEXT 6 MONTHS



© Ontic Technologies, Inc. 2022

SECTION 02

ATTITUDES, STANCES, RHETORIC AND BACKLASH

© Ontic Technologies, Inc. 2022

Heightened threats tied to corporate stances on political and social issues.

Only 12% of physical security executives expected COVID-19 recovery, managing permanent hybrid/remote, office work structures and safety protocols to be among their biggest 2022 challenges when queried for the 2022 State of Protective Intelligence Report. Midway through the year, we now find that COVID-19 and health protocols are atop a list of issues that have resulted in threats at U.S. companies, according to 62% of physical security leaders surveyed. The reason for those threats related to COVID-19 and health protocols — 59% across all surveyed audiences — is primarily because their company issued vaccine and testing requirements (83%). These findings reiterate those of previous State of Protective Intelligence studies — the potential for a company to receive threats exists whether they take a public stance on an issue or refrain.

Diversity, equity and inclusion issues have resulted in threats to their company for 33% of those surveyed, with the majority of threats occurring (79%) because their company and CEO expressed support for racial diversity and the LBGTQ+ communities, while 22% say threats occurred because support for the same was not expressed by their company and CEO.

Issues around return to office mandates (28%), permanent hybrid work (25%), and sustainability and climate change (21%) also resulted in threats to American businesses, the latter because their CEO and company publicly stated and implemented sustainability, decarbonization goals and initiatives (78%). Issues around return to office mandates (28%), permanent hybrid work (25%), and sustainability and climate change (21%) also resulted in threats to American businesses, the latter because their CEO and company publicly stated and implemented sustainability, decarbonization goals and initiatives (78%) or have not implemented any sustainability, decarbonization goals and initiatives (24%).

Hot button issues also resulted in threats at U.S. companies, including the war in Ukraine (16%), because their CEO and company expressed support for Ukraine (66%), did not take a stance (32%), their company has operations in Russia and no plans to leave (24%), and had operations in Russia and exited the country (21%).

Gun control issues also drove threats (16%) because their company took a stance and severed ties with the NRA (66%), or continued its alliance with the NRA (29%).

Finally, even prior to the overturning of Roe v. Wade when this survey was conducted, it was an issue that drove threats (9%) because the CEO and company had taken a stance supporting abortion rights (54%), taken a stance against abortion rights (43%) or not taken a stance at all (14%).

© Ontic Technologies, Inc. 2022

ISSUES RESULTING IN THREATS TO AMERICAN COMPANIES

59% COVID-19 and health protocols

	WHY?
83%	My company has issued vaccine and testing requirements
22%	My company has not issued vaccine and testing requirements

33% Diversity, equity and inclusion

	WHY?
79%	My CEO and company have expressed support for racial diversity and the LGBTQ+ communities
19%	My CEO and company have not expressed support for racial diversity and the LGBTQ+ communities
05%	Not sure

28% Return to office mandate

25% Permanent hybrid work

21% Sustainability and climate change

	WHY?
78%	My CEO and company have publicly stated and implemented sustainability, decarbonization goals and initiatives
24%	My CEO and company have not publicly stated and implemented sustainability, decarbonization goals and initiatives
05%	Not sure

16% The war in Ukraine

	WHY?
66%	My company has taken a stance and severed its ties with the NRA
32%	My CEO and company have not expressed support for Ukraine
24%	My company has operations in Russia and no plans to leave
21%	My company has operations in Russia and has exited the country
02%	Not sure

16% Gun control

	WHY?
66%	My company has taken a stance and severed its ties with the NRA
29%	My company continues its alliance with the NRA
11%	Not sure

9% Roe vs Wade

	WHY?
54%	My CEO and company have taken a stance supporting abortion rights
43%	My CEO and company have taken a stance against abortion rights
14%	My CEO and company have not taken a stance
03%	Not sure

11% None of these

© Ontic Technologies, Inc. 2022

Some numbers add up to more than 100% because respondents selected both types of threats.

SECTION 03

THREAT ASSESSMENT AND MANAGEMENT: POLICIES, PRACTICES, TRAINING AND OWNERSHIP

© Ontic Technologies, Inc. 2022

Threat assessment training is vital to job success

Being able to identify potential trouble in the workplace that may be on the horizon is increasingly important as threats to businesses rise. In fact, there is consensus across department functions – with the highest agreement from human resources – and unanimity among all survey respondents that behavioral threat assessment or threat management training is important for their team to successfully execute their job (98% say it is important, including 71% who say it is very important).

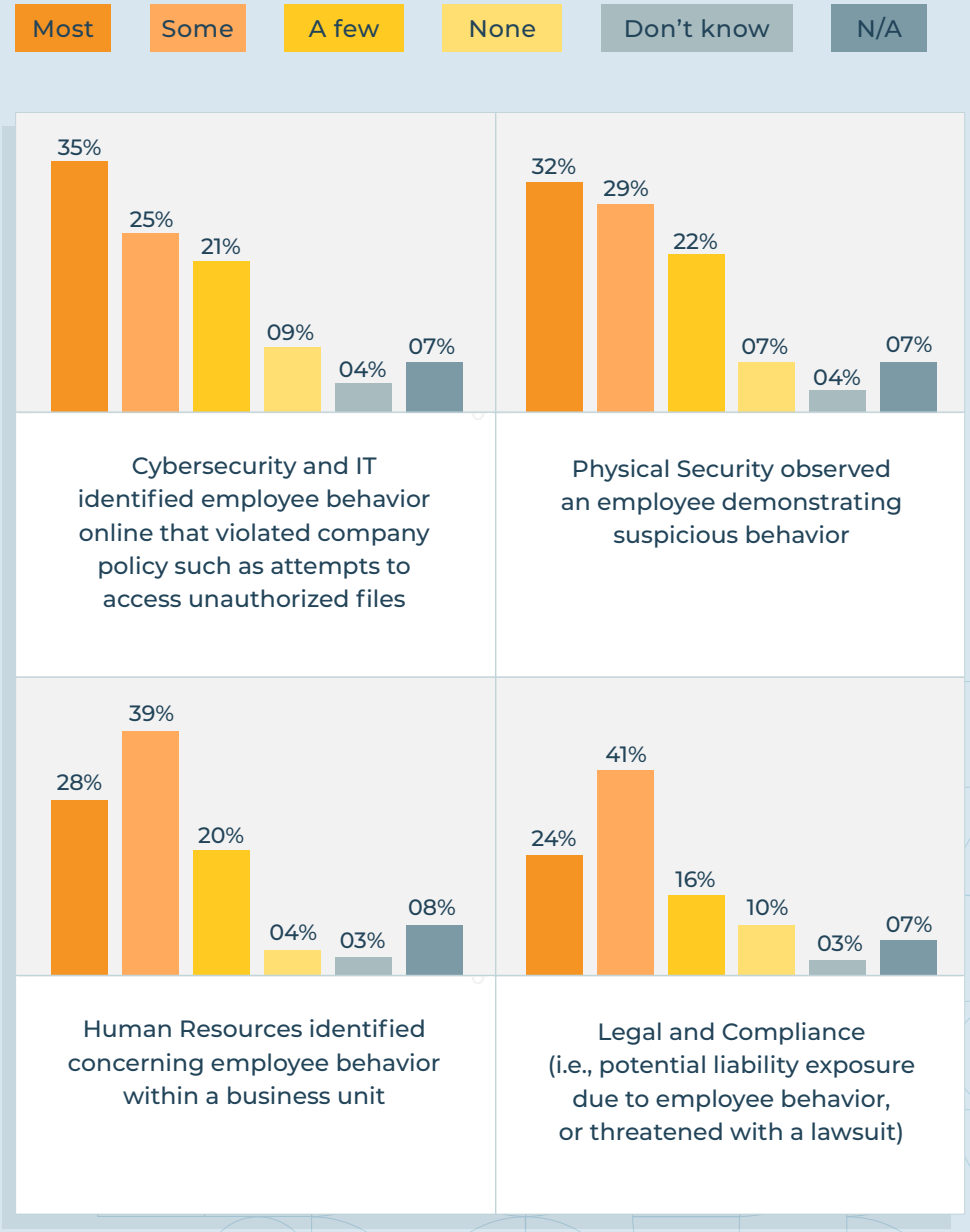
IMPORTANCE OF BEHAVIORAL THREAT ASSESSMENT TRAINING TO SUCCESSFUL JOB EXECUTION

© Ontic Technologies, Inc. 2022

A majority agree (84%) their company's physical security, human resources, cybersecurity and IT, and legal and compliance professionals have been adequately trained to assess threats, which includes reporting erratic behavior and warning signs that could lead to workplace violence. Of the potentially violent and harmful threats their company received in 2022, many surfaced using behavioral threat assessment strategies.

For example, 35% said that most of the violent and harmful threats surfaced because cybersecurity and IT identified employee behavior online that violated company policy such as attempts to access unauthorized files; another 25% said "some" threats surfaced this way as well. In addition, most (32%), some (29%) and a few (22%) violent and harmful threats received surfaced because physical security observed an employee demonstrating suspicious behavior while most (28%), some (39%) and a few (20%) threats were surfaced through human resources identification of concerning behavior. Most (24%), some (41%) and a few (16%) threats related to potential liability exposure due to employee behavior, or threat of a lawsuit were surfaced by legal and compliance.

VOLUME AND HOW VIOLENT AND HARMFUL THREATS HAVE BEEN SURFACED AT U.S. COMPANIES IN 2022



© Ontic Technologies, Inc. 2022

However positive it may be that threat assessment training for these business functions is taking place, survey data suggests confusion remains among physical security, cybersecurity and IT, legal and compliance, and HR over who has primary responsibility for behavioral threat assessment functions and over who should have primary responsibility. Most respondents thought their own departments had and should have primary responsibility. This disagreement — or confusion — among respondents is vital for corporate security to be aware of and 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.

THREAT ASSESSMENT AND THREAT MANAGEMENT TRAINING

IS responsible | **SHOULD BE** responsible

	Physical Security Respondents		Human Resources Respondents		Cybersecurity and IT Respondents		Legal and Compliance Respondents	
Physical security / Corporate security	76%	70%	13%	09%	16%	17%	16%	19%
Executive protection	03%	04%	04%	05%	06%	13%	08%	05%
Human resources	07%	07%	62%	68%	19%	15%	11%	10%
IT/Cybersecurity	09%	13%	07%	11%	49%	42%	6%	10%
Legal and compliance	02%	01%	07%	02%	04%	02%	47%	43%
Enterprise risk management	02%	02%	05%	05%	04%	11%	10%	12%
Employee assistance program	00%	02%	02%	00%	01%	00%	01%	00%
Don't know	01%	01%	00%	00%	01%	00%	01%	00%

© Ontic Technologies, Inc. 2022

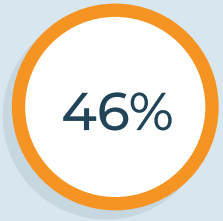
Challenges still exist among employee populations, as almost two-thirds (64%) of respondents agree that at their company employees do not report erratic and violent behavior or other warning signs in a timely manner.

Given that 63% agree their company downplays risk to emulate a safe environment, it's also not surprising that, when it comes to their company's approach to employee preparedness to address physical threats and potential workplace violence, more than half (54%) of respondents do not have a mechanism in place that allows employees to anonymously report issues and 43% rely on employees to take the "if you see something, say something" approach to security, whether they are working from home or on-site at a company location.

Slightly over one-third (35%) say they do training for workplace violence from time to time but do not have a formal program in place, while one-third (33%) say they have a hybrid work structure so workplace violence training is not a priority since employees are not at company locations full-time. At the same level, one-third of respondents say their company believes that workplace violence training may create a culture of fear, wants to take a reactive strategy and does not see the ultimate risk to business continuity by inaction. One quarter (25%) say their company does not believe it will be a target for significant physical harm and does not value employee training and preparedness for dealing with such crises, while 21% say their company has never addressed the potential for workplace violence and employees would not know what to do if an active shooter was at their facilities. On a positive note, however, 39% of those surveyed said they have an Active Shooter/Active Assailant Plan in place and employees receive regular training.

© Ontic Technologies, Inc. 2022

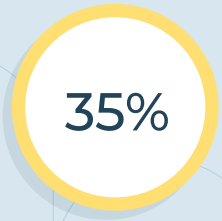
COMPANY APPROACHES TO EMPLOYEE PREPAREDNESS TO ADDRESS PHYSICAL THREATS AND POTENTIAL WORKPLACE VIOLENCE



My company has a mechanism in place that allows employees to anonymously report issues

We rely on employees to take the “if you see something, say something” approach to security, whether they are working from home or on-site at a company location

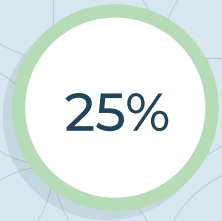
We have an Active Shooter / Active Assailant Plan in place and our employees receive regular training



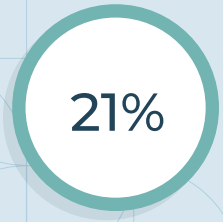
We do training for workplace violence from time to time but do not have a formal program in place

We have a hybrid work structure so workplace violence training is not a priority since employees are not at company locations full-time

My company believes that workplace violence training may create a culture of fear, wants to take a reactive strategy and does not see the ultimate risk to business continuity by inaction



My company does not believe we will be a target for significant physical harm and does not value employee training and preparedness for dealing with such crises



My company has never addressed the potential for workplace violence and employees would not know what to do if an active shooter was at our facilities

None of these

© Ontic Technologies, Inc. 2022

If protectors are not sure company policies, plans and practices exist, how effective can they be?

While the majority of those surveyed were sure that a range of policies, plans and procedures were in place at their company, for each policy a significant contingent remained unsure. The amount who were not aware of each policy ranged from one in five (19%) to nearly half (49%).

Legal and compliance executives are the most unsure about what policies and practices are in place at their company. This could be because legal and compliance executives' criteria for what they consider a set policy or practice may be more finite than that of their physical security, human resources, and cybersecurity and IT colleagues. That said, among the latter functions, the survey reveals they are also not sure what policies and practices are in place.

Unclear policies and practices can lead to confusion, lack of accountability, miscommunication, incorrect assumptions and frustration — among leaders who are supposed to be responsible for executing the policies and practices, as well as among those the initiatives are intended to protect. When everyone is not working from the same playbook, viewing the same data and receiving the same information, potential risks and threats can be missed.

© Ontic Technologies, Inc. 2022

POLICIES AND PRACTICES IN PLACE AT AMERICAN COMPANIES

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	67%	65%	68%	80%	53%
Not sure	33%	34%	32%	19%	44%
No, I am sure they do not	1%	1%	0%	1%	3%

My company conducts background checks as part of the hiring process as a way to mitigate risk, including the potential for property theft and workplace violence.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	59%	63%	64%	56%	53%
Not sure	37%	34%	32%	38%	44%
No, I am sure they do not	4%	3%	4%	6%	3%

My company has clear policies and plans for keeping employees safe when they are performing work at home.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	66%	67%	66%	77%	53%
Not sure	33%	33%	29%	23%	45%
No, I am sure they do not	2%	0%	5%	0%	2%

My company has clear policies and plans to keep employees safe in our offices.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	63%	66%	64%	68%	54%
Not sure	33%	32%	35%	27%	41%
No, I am sure they do not	3%	2%	1%	5%	5%

When a potentially violent employee has been dismissed, my company has a process for notifying across physical security, IT/cybersecurity, human resources, legal and compliance functions.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	58%	63%	62%	58%	48%
Not sure	39%	33%	37%	36%	49%
No, I am sure they do not	4%	4%	1%	6%	3%

My company keeps employees safe by having workplace violence insurance to cover expenses it might incur from incidents, such as hiring security and public relations consultants, survivors' death benefits and business interruption costs.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	63%	69%	59%	73%	52%
Not sure	35%	30%	38%	24%	45%
No, I am sure they do not	3%	1%	3%	3%	3%

My company has conducted workplace violence/threat assessments and implemented security measures at our worksites to mitigate liability for workplace violence.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	59%	67%	55%	61%	52%
Not sure	36%	28%	38%	33%	43%
No, I am sure they do not	6%	5%	7%	6%	5%

When a potentially violent employee is due to be dismissed, my company conducts a behavioral threat assessment (or uses an external expert to do so) prior to termination / dismissal.

	% Total	% Physical Security	% Human Resources	% Cybersecurity and IT	% Legal and Compliance
Yes, I am sure they do	63%	60%	68%	69%	54%
Not sure	35%	37%	30%	28%	44%
No, I am sure they do not	3%	3%	2%	3%	2%

My company has clear policies and plans for keeping employees safe when they are performing work while on company-related travel.

© Ontic Technologies, Inc. 2022

SECTION 04

COMMUNICATION SILOS PERSIST, BUT CROSS-FUNCTIONAL 'TASK FORCES' ARE EMERGING

© Ontic Technologies, Inc. 2022

Enterprise risk and critical business resilience: What are the components? Who's responsible?

Putting in place strategies to prepare for and lessen the effects of threats a business may face — and ultimately mitigating risk — is as important as corporate compliance or ensuring internal policies, procedures and behaviors, as well as external regulations, are met. Clarity around roles and responsibilities, communications, collaboration, processes and reporting, and special training to be able to address volatile situations, can mean the difference between a catastrophic event destroying a business or the event being averted. This is critical to long-term business resilience.

Nearly all those surveyed are responsible for ensuring compliance requirements are met and that risk is mitigated by protecting their company in a panoply of ways. These include protecting company executives, employees and customers from violent and disastrous events that could threaten business resilience; protecting the company from lawsuits and ensuring it adheres to regulatory requirements to avoid business disruption and financial losses; protecting the company from hostile, aggressive and harmful employee behavior and protecting the company's computer systems and data.

© Ontic Technologies, Inc. 2022

% Total | % Physical Security | % Human Resources | % Cybersecurity and IT | % Legal and Compliance

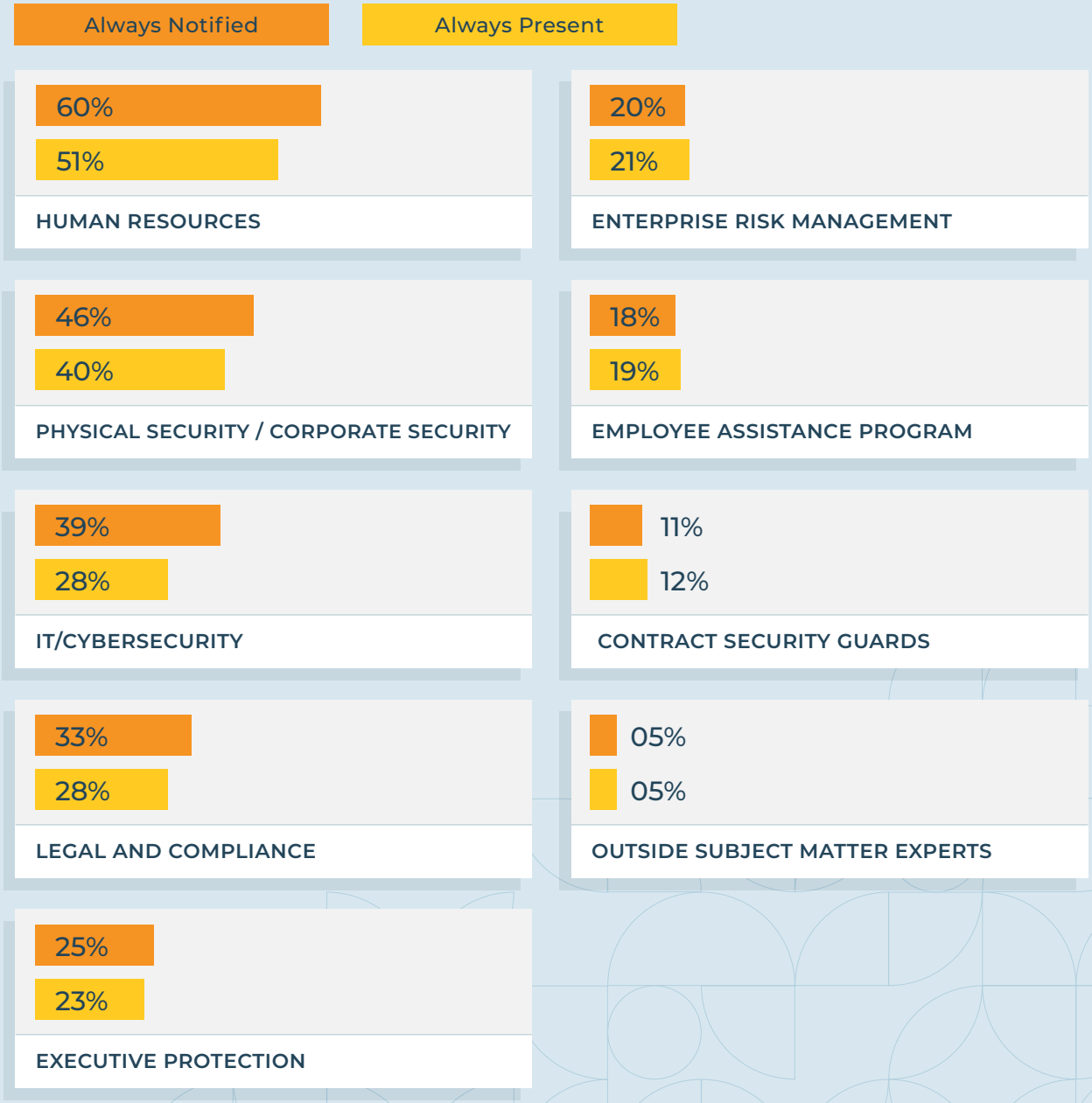
	ENSURING COMPLIANCE REQUIREMENTS ARE MET					MITIGATING RISK				
Protect my company's executives, employees and customers from violent and catastrophic events that could threaten business resilience.										
Yes, DIRECT responsibility	78%	86%	85%	63%	77%	70%	81%	80%	53%	67%
Yes, INDIRECT responsibility	20%	13%	15%	29%	22%	25%	17%	18%	37%	28%
No, not a responsibility	3%	1%	0%	8%	1%	5%	2%	2%	10%	5%
Protect my company's computer systems and data.										
Yes, DIRECT responsibility	62%	53%	56%	80%	58%	64%	52%	65%	79%	58%
Yes, INDIRECT responsibility	32%	34%	40%	19%	33%	30%	32%	32%	20%	34%
No, not a responsibility	7%	13%	4%	1%	9%	7%	16%	3%	1%	8%
Protect my company from lawsuits and ensure it adheres to regulatory requirements to avoid business disruption and financial losses.										
Yes, DIRECT responsibility	68%	63%	81%	56%	70%	68%	64%	77%	58%	72%
Yes, INDIRECT responsibility	24%	23%	17%	30%	27%	24%	20%	22%	29%	24%
No, not a responsibility	8%	14%	2%	14%	3%	9%	16%	1%	13%	4%
Protect my company from hostile, aggressive and harmful employee behavior.										
Yes, DIRECT responsibility	72%	83%	80%	58%	67%	68%	84%	73%	53%	61%
Yes, INDIRECT responsibility	23%	16%	19%	30%	28%	27%	15%	26%	34%	34%
No, not a responsibility	5%	1%	1%	12%	5%	5%	1%	1%	13%	5%

© Ontic Technologies, Inc. 2022

Employee firings don't have to go wrong

What happens when an employee who is furloughed or fired turns violent? Who at the company is notified ahead of when this action is going to take place, and what kind of training do they have to address such a situation? Our survey shows that companies have a long way to go to ensure such workplace violence doesn't occur.

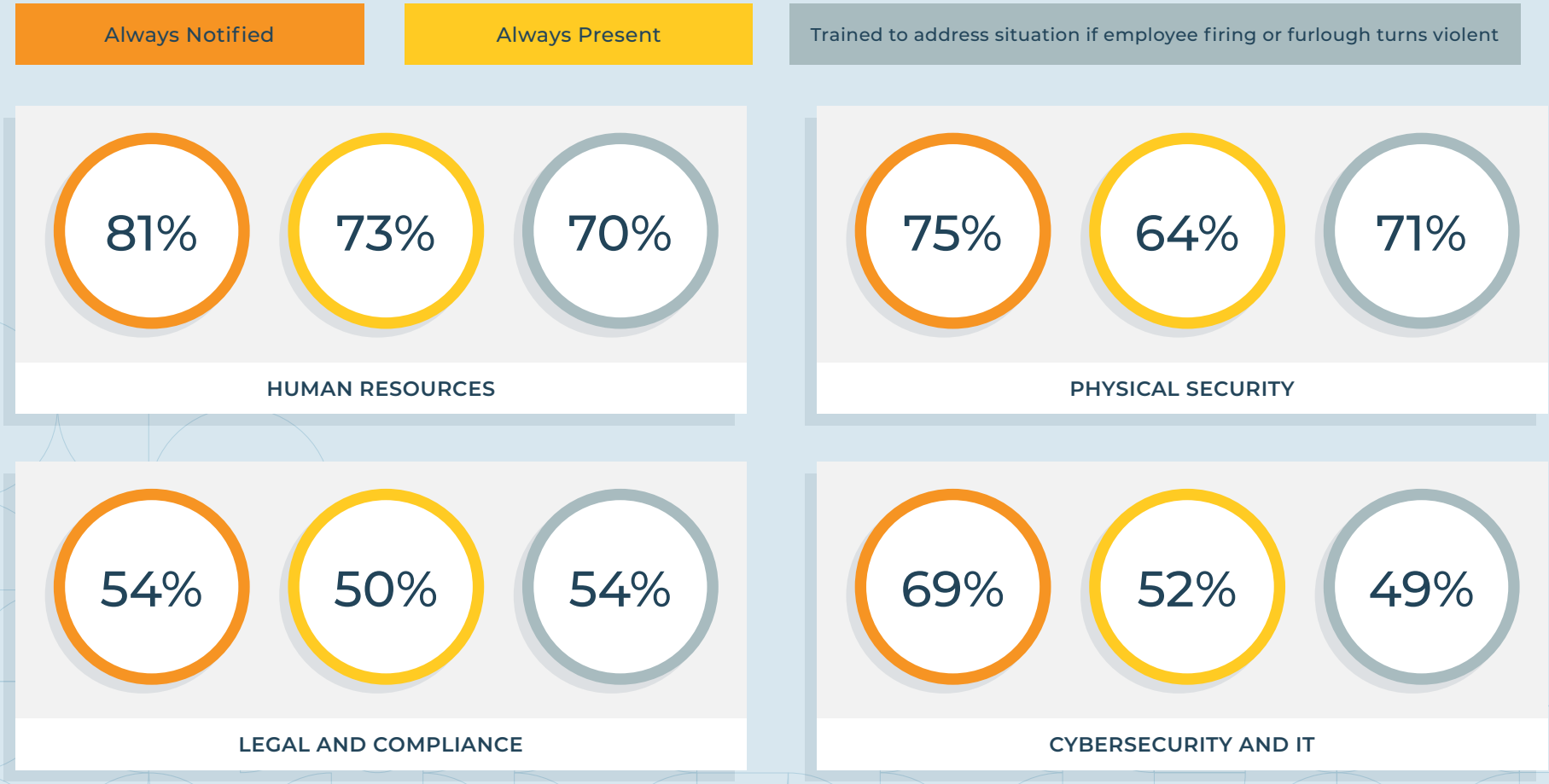
WHEN AN EMPLOYEE WILL BE FURLOUGHED OR FIRED AT MY COMPANY, MY DEPARTMENT IS... *(All respondents)*



© Ontic Technologies, Inc. 2022

When an employee will be furloughed or fired, among HR executives surveyed, 81% say they are always notified, 74% say they are always present and 70% say they are trained to address the situation if it turns violent. Among physical security executives, 75% say they are always notified, 64% say they are always present and 71% say they are trained to address the situation if it turns violent. Among legal and compliance executives, 54% say they are always notified, half or 50% say they are always present and 54% say they are trained to address the situation if it turns violent. Cybersecurity and IT executives say they are always notified (69%), always present (52%) and close to half (49%) say they are trained to address the situation if it turns violent.

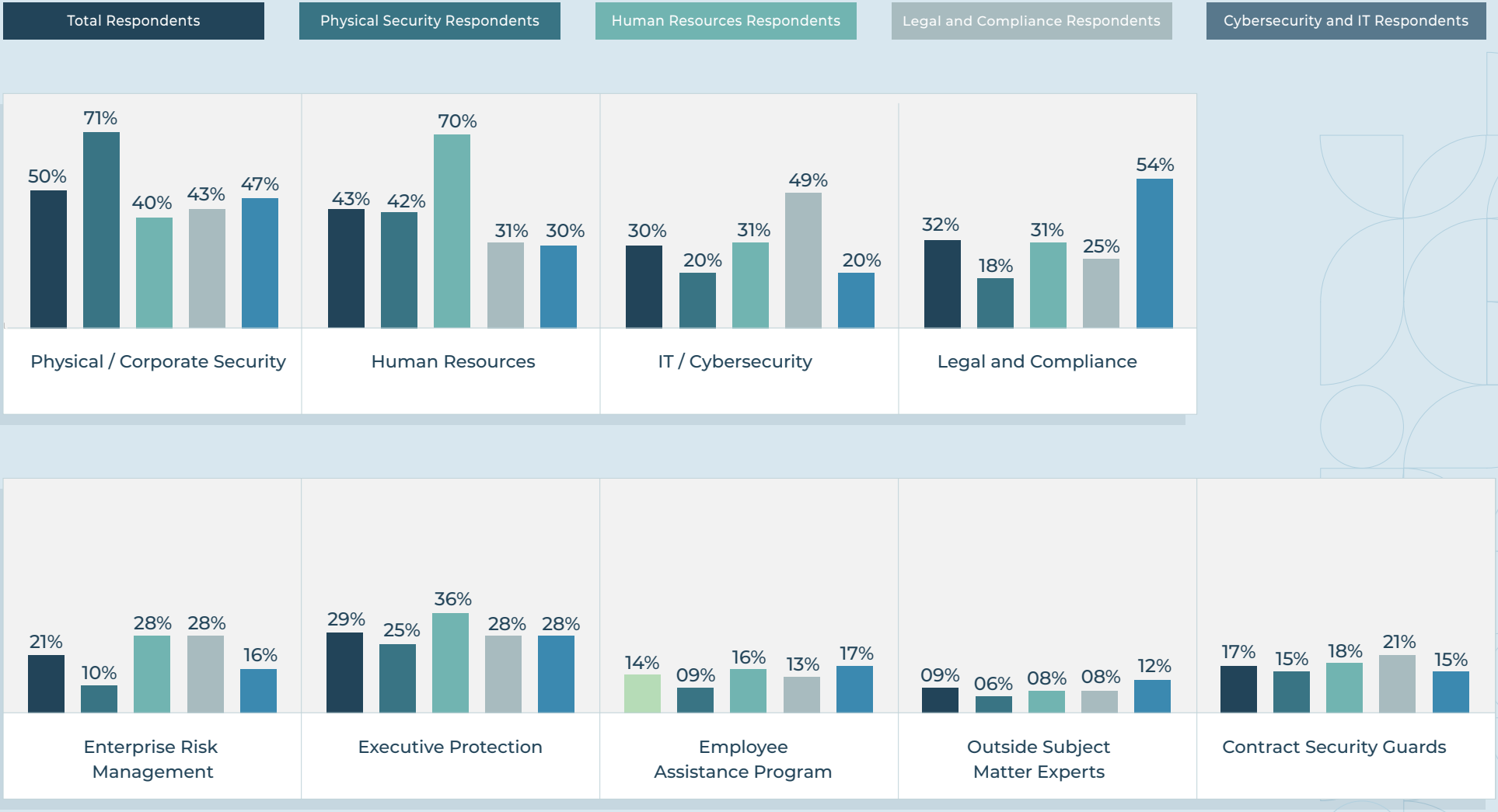
WHEN AN EMPLOYEE WILL BE FURLOUGHED OR FIRED AT MY COMPANY THESE DEPARTMENTS ARE...



© Ontic Technologies, Inc. 2022

Even minor lapses in established communications or processes can result in disaster. Indeed, 75% of human resources, 72% of legal and compliance, 66% of physical security and 60% of cybersecurity and IT respondents agree that in the past year, violence or harm occurred at their company when an employee was furloughed or fired because of a failure to notify their department in advance.

DEPARTMENTS TRAINED TO ADDRESS SITUATION IF EMPLOYEE FIRING OR FURLOUGH TURNS VIOLENT



© Ontic Technologies, Inc. 2022

SNAPSHOT: THREATS AND PUBLIC COMPANY RISK FACTORS

THREATS, RISK FACTORS AND PUBLIC FILINGS

Public companies are required to publish a 10-K so investors have fundamental information about a company in order to make informed investment decisions. Within a 10-K filing, risk factors include information about the most significant risks that apply to the company or its securities. Given the volume of threats corporations face and the potential for those to result in harm or damage to executives, employees and assets, financial instability or an inability to continue operations, disclosing such risks is critical for corporate transparency.

AMONG 110 PUBLICLY TRADED COMPANY EXECUTIVES SURVEYED:

78% AGREED

Their company's investment in security operations (e.g. funding, planning and policy development) is based directly on risk factors disclosed in its public SEC filings, including the 10-K risk factors

77% AGREED

The risk factors in their company's public SEC filings, such as the 10-K, barely skim the surface in terms of the scope and volume of security threats they investigate and receive

64% AGREED

Including security threats such as cyber-physical, supply chain and remote work vulnerabilities as risk factors in its public filings is something their company only recently started to do

54% AGREED

Physical security threats (threats that have the potential to cause harm to executives, employees, customers and/or damage to company property), are not included by their company as risk factors in public filings

© Ontic Technologies, Inc. 2022

SECTION 05

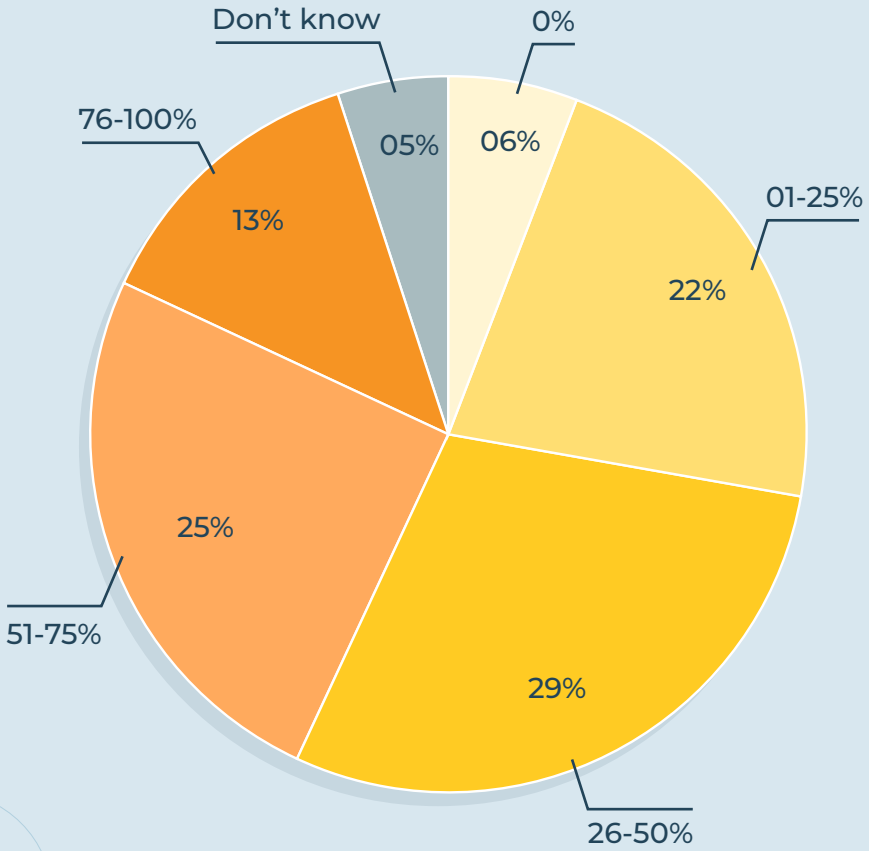
PHYSICAL SECURITY CONVERGENCE, CONSOLIDATION GAINING MOMENTUM

© Ontic Technologies, Inc. 2022

Tech consolidation and single universal software platforms

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. Over half (54%) said 26-75% of threats could have been avoided while 22% said 1-25% of threats could have been avoided and 13% said as high as 76-100%.

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



© Ontic Technologies, Inc. 2022

For close to half of those surveyed (47%) who missed threats (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; 37% had their department's budget and staff increased; 34% had budget and staff reduced and over one-quarter (26%) had responsibility for threat assessment and management removed from their department by management.

But, as first noted in the 2022 State of Protective Intelligence Report, the widespread movement to digitally transform physical security into a single software platform continues to gain momentum. A majority (87%) of respondents 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.

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

© Ontic Technologies, Inc. 2022

About the study

A total of 400 respondents completed the survey, which was conducted from June 8 – July 1, 2022. These included chief security officers, chief human resources officers, chief legal officers, chief compliance officers, chief information security officers, chief technology officers, chief information officers and physical security decision-makers at U.S. companies with over 5,000 employees in the automotive, banking and financial services, consumer goods, education, energy, government, healthcare, insurance, media and entertainment, pharmaceutical, retail, technology, telecommunications, and travel and hospitality industries.

About the Ontic Center for Protective Intelligence

The Center is a trusted resource for those in the security, safety and protection communities. It's a place to share strategies and best practices, insights on current and historical trends and lessons learned through dialogue, discourse and alternative analysis from some of the industry's top practitioners.

About Ontic

Ontic is a protective intelligence software innovator transforming, expanding and changing how Fortune 500 and emerging enterprises protect employees, customers and assets from physical security threats. Ontic's SaaS platform helps preserve business continuity and build long-term organizational resilience by collecting and connecting data to create a comprehensive view of potential threats and take necessary actions to mitigate risks. Ontic also provides threat assessment, threat management and strategic intelligence services that include expert training, guidance and program development using best practices and proven protocols. Ontic was named 2022 Global Entrepreneurial Company of the Year by Frost & Sullivan and the top industry innovator among a dozen other vendors in the Frost Radar™: Digital Intelligence Solutions, 2021.

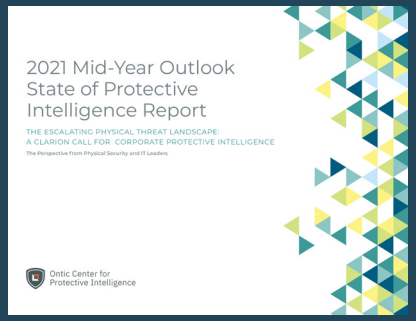
For more information please visit ontic.co
or follow us on Twitter or LinkedIn

For inquiries related to the study, contact contact@ontic.co

© Ontic Technologies, Inc. 2022

ONTIC

Center for Protective Intelligence

2022 MID-YEAR STATE OF PROTECTIVE INTELLIGENCE REPORT

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