EXECUTIVE SUMMARY SPOTLIGHT

2022 Mid-Year Outlook State of Protective Intelligence Report

THE PERSPECTIVE FROM CYBERSECURITY AND IT LEADERS

Ontic Center for Protective Intelligence

Cybersecurity and IT are on the first line for protecting companies, mitigating cyber-physical risk

Protecting corporate executives, employees, customers and assets is the responsibility of cybersecurity and IT leaders, along with their physical security, human resources, and legal and compliance colleagues.

As American corporations experience an increased volume 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 cybersecurity and IT leaders will always need and be relied on for their deeper specialized expertise, the heightened physical threat landscape and technology consolidation mean the walls between lines of business are falling with the recognition that data-sharing can raise the effectiveness of all.

DEFINITIONS AND VOLUME OF THREATS AND BUSINESS RISKS

(According to cybersecurity and IT leaders)

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

Number of threats and business risks cybersecurity and IT 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	4%
1-2 per year	16%
3-5 per year	18%
6-10 per year	24%
11-25 per year	24%
26-50 per year	7%
+50 per year	7%

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

None	1%
1-2 per year	11%
3-5 per year	19%
6-10 per year	29%
11-25 per year	24%
26-50 per year	3%
+50 per year	11%

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

None	4%
1-2 per year	13%
3-5 per year	31%
6-10 per year	30%
11-25 per year	17%
26-50 per year	2%
+50 per year	4%

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

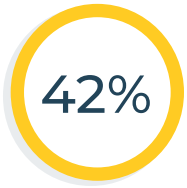
Being able to identify potential trouble in the workplace that may be on the horizon is increasingly important as threats to businesses rise. Almost all cybersecurity and IT executives say that behavioral threat assessment or threat management training is important for their team to successfully execute their job (96% say it is important, including 80% who say it is very important).

Of the potentially violent and harmful threats their company received in 2022, among cybersecurity and IT, physical security, human resources, and legal and compliance executives surveyed, 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.

Though a majority of **cybersecurity and IT executives agree (89%)** that along with their physical security, human resources, and legal and compliance colleagues they have 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.

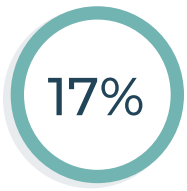
AMONG CYBERSECURITY AND IT RESPONDENTS

49% said their department is responsible for threat assessment and management



42% said they should be responsible

19% said human resources is responsible



17% said physical/corporate security should be responsible

Most other respondents thought their own departments had and should have primary responsibility: 76% of physical security said they are responsible, 62% of human resources said they are responsible, and 47% of legal and compliance said they are responsible.

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

While a majority of cybersecurity and IT were sure a range of policies, plans and procedures were in place at their company, many were not. Unclear policies and practices, and confusion about who takes the lead on important protective initiatives like threat assessment and threat management planning can lead to lack of accountability, miscommunication, incorrect assumptions and frustration — among the leaders who are supposed to be taking these actions and among those they 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.

POLICIES AND PRACTICES IN PLACE AT AMERICAN COMPANIES

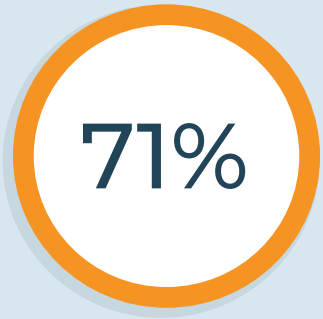
	Yes, I am sure they do	Not sure	No, I am sure they do not
My company conducts background checks as part of the hiring process as a way to mitigate risk, including the potential for property theft and workplace violence.	80%%	19%	1%
My company has clear policies and plans for keeping employees safe when they are performing work at home.	56%	38%	6%
My company has clear policies and plans to keep employees safe in our offices.	77%	23%	0%
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.	68%	27%	5%
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.	58%	36%	6%
My company has conducted workplace violence/threat assessments and implemented security measures at our worksites to mitigate liability for workplace violence.	73%	24%	3%
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.	61%	33%	6%
My company has clear policies and plans for keeping employees safe when they are performing work while on company-related travel.	69%	28%	3%

At public companies, protecting data and networks is part of a larger physical security risk landscape that's underreported.

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.

A majority (71%) of cybersecurity and IT leaders at public companies agree 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, while 65% say only recently their company started to include security threats such as cyber-physical, supply chain and remote work vulnerabilities as risk factors in its public filings. Sixty percent say their company does not include physical security threats that have the potential to cause harm to executives, employees, customers and/or damage to company property as risk factors in public filings.

AMONG CYBERSECURITY AND IT EXECUTIVES



A majority (71%) of cybersecurity and IT leaders at public companies agree 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.

65% say only recently their company started to include security threats such as cyber-physical, supply chain and remote work vulnerabilities as risk factors in its public filings.

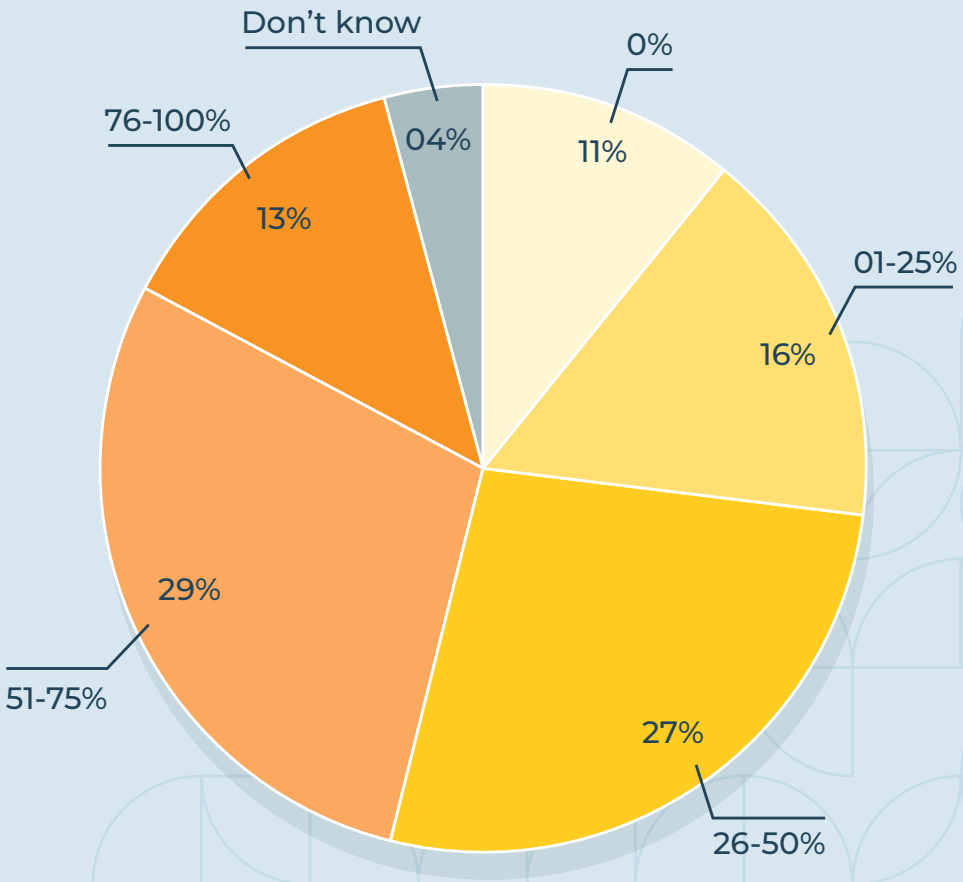
60% say their company does not include physical security threats that have the potential to cause harm to executives, employees, customers and/or damage to company property as risk factors in public filings.

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. More than half (56%) of cybersecurity and IT executives said 26-75% of threats could have been avoided while 16% said 1-25% of threats could have been avoided and 13% said as high as 76-100%.

A majority (89%) of cybersecurity and IT 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 CYBERSECURITY AND IT 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: