EXECUTIVE SUMMARY SPOTLIGHT

2022 Mid-Year Outlook State of Protective Intelligence Report

THE PERSPECTIVE FROM LEGAL AND COMPLIANCE LEADERS

Ontic Center for Protective Intelligence

Legal and compliance leaders meet expanding enterprise risk as threats to American companies increase

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

As American corporations experience an increased volume of threats driven by strong political, social and economic headwinds, legal and compliance executives are increasingly responsible for business continuity and resilience, and managing a variety of these threats.

DEFINITIONS AND VOLUME OF THREATS AND BUSINESS RISKS

(According to legal and compliance leaders)

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

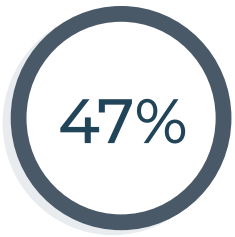
Number of threats and business risks legal and compliance deals with annually

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	13%
3-5 per year	25%
6-10 per year	27%
11-25 per year	24%
26-50 per year	4%
+50 per year	4%

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

None	2%
1-2 per year	17%
3-5 per year	21%
6-10 per year	21%
11-25 per year	28%
26-50 per year	6%
+50 per year	4%



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

None	2%
1-2 per year	16%
3-5 per year	17%
6-10 per year	21%
11-25 per year	19%
26-50 per year	11%
+50 per year	13%

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

Legal and compliance executives are 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.

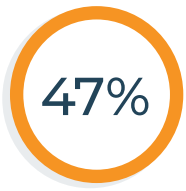
That said, unclear policies and practices, and confusion about who takes the lead on important protective initiatives like threat assessment and threat management planning can lead to lack of accountability, miscommunication, incorrect assumptions and frustration — among the leaders who are supposed 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.	53%	44%	3%
My company has clear policies and plans for keeping employees safe when they are performing work at home.	53%	44%	3%
My company has clear policies and plans to keep employees safe in our offices.	53%	45%	2%
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.	54%	41%	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.	48%	49%	3%
My company has conducted workplace violence/threat assessments and implemented security measures at our worksites to mitigate liability for workplace violence.	52%	45%	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.	52%	43%	5%
My company has clear policies and plans for keeping employees safe when they are performing work while on company-related travel.	54%	44%	2%

WHO IS AND SHOULD BE RESPONSIBLE FOR THREAT ASSESSMENT AND MANAGEMENT

(According to legal and compliance respondents)



47% said their department is responsible

43% said they should be responsible

16% said physical/corporate security is responsible

19% 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 49% of cybersecurity and IT said they are responsible.

Enterprise risk and critical business resilience

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.

79% 79% agree their company has a program to specifically identify employees with greater access to critical information, IP or key executives than the rest of the organization.

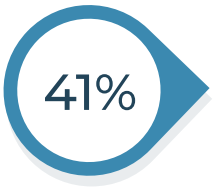
65% 65% agree their company downplays risk to emulate a safe environment.

Repercussions for legal and compliance

When legal and compliance professionals are not able to identify threats before they cause harm or damage, there can be repercussions for their leaders and department. For close to half of legal and compliance executives (47%) 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.

45% had their department's budget and staff reduced.

Close to one-third (30%) had responsibility for threat assessment and management removed from their department by management.



41% had budget and staff increased.

At public companies, risk factors are expanding concurrent with the threat landscape.

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 (58%) of legal and compliance 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.

73% 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.

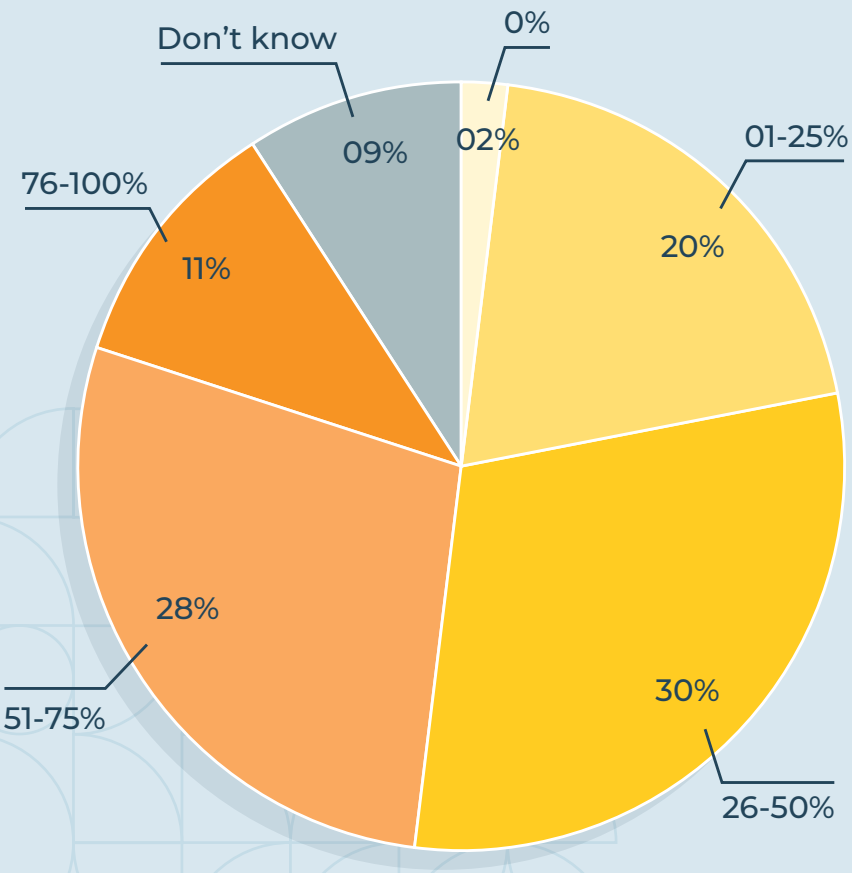
62 percent say their company does not include physical security threats that have the potential to cause harm to executives, employees, customers and/or damage to company property as risk factors in public filings.

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 (58%) of legal and come compliance executives said 26-75% of threats could have been avoided while 20% said 1-25% of threats could have been avoided and 11% said as high as 76-100%.

A majority (81%) of legal and compliance 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 LEGAL AND COMPLIANCE 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: