ONTIC

The Future of Security: Forecasts for 2025 and Beyond

Predictions and insights from the community

Table of Contents

Foreword from Ontic's CSO

The security landscape is evolving in both expected and surprising ways. For the Security Industry Forecasts for 2024 and Beyond report, we asked experts from across the industry to share their insights on the critical issues shaping security — from geopolitical tensions and emerging technologies to talent retention challenges. As we revisit these forecasts, it's striking how many predictions have come to pass or are well on their way to becoming realities. Looking ahead, we expect even more significant challenges as our industry grapples with new threats and evolving risks.

Before we delve into 2025 predictions, let's explore which predictions materialized from 2024's forecast, tangential key developments, and where our forecasts diverged.

What came true from Ontic's 2024 forecast?

One of the most accurate predictions from last year was the continued escalation of geopolitical risks. In 2024, conflicts in Ukraine and the Middle East grew more intense, with tensions also rising in other parts of the world. These developments reflected what many security professionals anticipated: a global environment marked by uncertainty, political instability, and an increasing need for organizations to adapt their security strategies. As expected, these geopolitical conflicts had significant downstream effects on corporate security, especially for companies with global operations.

Artificial intelligence (AI) and convergence predictions also aligned closely with reality. Last year, experts discussed the increasing integration of AI into security operations, forecasting that while AI tools would improve efficiency, human judgment would remain critical.

Over the past year, AI has enhanced capabilities like predictive analytics, threat detection, and intelligence gathering — particularly in Global Security Operations Centers (GSOCs). AI's ability to process vast amounts of data has enabled security teams to respond more rapidly to evolving threats. However, it is still a supplement rather than a replacement for human decision-making. This is an ongoing trend that is likely to continue shaping our industry in 2025 and beyond.

In terms of **insider risk**, the prediction that economic pressures — particularly inflation and rising interest rates — would exacerbate employees' financial stress has also come to fruition. In 2024, many organizations experienced an uptick in insider threats. Mitigation has become a top priority, with a renewed focus on monitoring, proactive threat assessment, and employee programs aimed at reducing vulnerabilities within the workforce.

Predictions about **talent shortages** and burnout materialized. With professional burnout rates climbing, security professionals faced evolving cyber-physical threats and the emotional strain of continuously reacting to risk. Organizations struggled to retain their top talent as job demands intensified.

Last year's forecast predicted that companies would need to take a more proactive approach to supporting mental health and wellness in the workplace, and that's precisely what many have done. However, rising demands for skilled professionals in physical and cybersecurity remain a major industry challenge.

Continued

Where did predictions diverge?

While many forecasts hit the mark, some areas deviated from expectations. For instance, the anticipated **convergence of cyber and physical security** has not advanced as much as some experts hoped. Though many organizations began implementing more integrated security strategies, they've faced challenges breaking down departmental silos. Despite recognizing the importance of convergence, navigating organizational culture and complexities in integrating diverse technologies has slowed progress.

In 2025, this convergence will remain a critical focus area as organizations work to dismantle silos and adopt more comprehensive security frameworks.

Another area where expectations diverged slightly was in **AI's role in misinformation**. Last year's forecast accurately predicted that AI would be used in disinformation campaigns, but the extent of this threat has grown beyond initial projections. State and non-state actors have leveraged generative AI to manipulate public opinion and create sophisticated misinformation campaigns. This has forced security teams to rethink their strategies for countering disinformation, placing greater emphasis on verifying the authenticity of information and developing new tools to combat AI-generated falsehoods.

New year, same risks?

As we look toward 2025, the risks we face will continue to evolve, and our responses must evolve with them. The security landscape is changing, shaped by events like the shocking killing of UnitedHealthcare's CEO, geopolitical tensions, economic pressures, and technological advancements. This year's forecast reflects the lessons we've learned and the opportunities ahead.

We invite you to explore this forecast and consider how these insights might help you prepare for the future. We also welcome any thoughts or feedback you may have. By staying agile and adaptable, we can turn these challenges into opportunities for growth and innovation.

We hope this year's forecast offers valuable insights. Stay safe, stay vigilant, and approach the future with agility and resilience — **Fortes fortuna adiuvat**.

Thank you,

Chuck Randolph

Chuck Randolph
Chief Security Officer
Ontic

Chapter 1: Executive Protection

Protecting executives will become a board-level issue

Following the shocking killing of UnitedHealthcare's CEO in December 2024, the importance of corporate executive protection entered the public discourse. Historically, corporate executives have resisted investing in such protection, as they often believe they are not at risk and have misconceptions about what executive protection means. However, experts predict that in the coming year, executive protection will emerge as a critical board-level concern. There will be a renewed focus on understanding the essential components of a robust executive protection program and prioritizing investments in the necessary technology, processes, and personnel.

Protecting executives will become a board-level issue

"The tragic shooting of the UnitedHealthcare CEO underscores the increasing threats faced by corporate leaders today. CEOs and high-profile executives are not only the faces of their organizations but are intrinsically linked to organizational stability. Their visibility inherently increases their risk, making them attractive targets for those with malicious intent. Executive protection (EP) is no longer a luxury; it is a strategic necessity.

Moving forward, I foresee that greater focus will be placed on the value of executive protection within organizations through the understanding that by protecting its leaders, an organization reinforces its commitment to resilience, safeguarding its reputation and the confidence of employees and stakeholders. With a heightened appreciation of the value and necessity of the executive protection function, resources, and funding will naturally expand to meet its growing needs."

Jonathan Wackrow
Chief Operating Officer
Teneo

"Corporate security organizations regularly face internal and external threats to their key leadership team. Identifying those who pose a "real threat" and taking the necessary precautionary steps to mitigate that risk is paramount. CSOs need an effective protective intelligence capability and tool set to help them identify and assess risk. The intelligence capability supports and enables the executive protection specialist(s) tasked with keeping key company officials safe. CSOs must also consider the threats and risks being communicated about their company and personnel on the deep dark web and maintain a capability either in-house or through a provider that excels in this area. Executive protection teams can be completely proprietary, completely sourced, or a mix of the two, depending on the risk profile associated with an organization. A strong executive protection program is crucial to business resilience and is a great way to showcase the value of corporate security investments."

Dave Komendat
President
DSKomendat Risk Management Services

Protecting executives will become a board-level issue

"Most CEOs rebuff the traditional close protection models, thinking they are either unnecessary, bad for business and optics, or undercut their reputation. Many executives deny that they are at risk or may have enemies. I've been in this business long enough to know that it takes tragedy to force change in our industry. It's always been that way. The shooting of UnitedHealthcare's CEO is a watershed moment for EP teams.

The threat landscape has changed to include the possibility of copycat attacks and doxxing of CEOs on social media. In the year ahead, the protection model will likely shift and adapt accordingly. We will see a shift toward a counter-surveillance model of protection — discreet shadowing and aggressive protective intelligence monitoring for threats. Technology solutions will help security teams stay in front of the avalanche of social media threat streams."

Fred Burton
Executive Director, Protective Intelligence
Ontic

"In the immediate aftermath of the murder of UnitedHealthcare's CEO, corporate executive protection became the "it" topic of the day. CEOs who once scoffed at any kind of protection will now be open to conversations with their security team. EP teams will have a committed interest in understanding the threat landscape and will turn to the threat assessment process that is most often used to prevent workplace violence to help them do this. They will identify individuals (or groups) of concern, investigate and gather as much information about the situation as possible, assess that information, and then put protective measures in place to protect their principal. It won't be about waiting for a threat to manifest itself, it will be more about doing something to ensure it doesn't.

Great EP teams will begin to understand that acts of violence targeting high-profile executives are not always directed at the individuals themselves. Often, these acts result from the executive's association with a prominent brand or industry. While it may not be immediately apparent or even understandable, these acts are typically motivated by something the individual feels or believes and should be approached with the necessary level of consideration."

Cindy Marble
Senior Director, Threat Assessment Management Operations
Ontic

Chapter 2: Intelligence

The impact of misinformation on risk analysis and reporting

Experts agree that the challenge of misinformation in intelligence is likely to intensify in 2025. Addressing the issue begins with understanding patterns in the campaigns designed to mislead the public, where they originate, and what signals indicate a legitimate concern for your organization. While AI has accelerated the spread of false claims and dangerous conspiracy theories, experts are split on whether AI-powered intelligence can solve the problem. In either case, in 2025, it's essential to focus on bolstering your intelligence skills, adopting better intelligence verification, and laser-focusing on the issues most likely to impact your organization.

The impact of misinformation on risk analysis and reporting

"Security teams struggling with the rise of misinformation and disinformation in 2025 will invest in research and intelligence analysts. In the aftermath of hurricanes Helene and Milton, we saw a sharp rise in disinformation that followed a familiar pattern: an attack on the truth designed to chip away trust in the institutions that drive our economy. It doesn't take much to see the implications for companies; whether they're targets or not, it's more important than ever for business leaders to understand what's possible. We will see more companies invest in research expertise. In other cases, security teams with these capabilities will begin integrating themselves into decision-making processes by proactively sharing information about risks."

Chuck Randolph
Chief Security Officer
Ontic

"Eagerness to adopt emerging technology permeates workplaces from the analyst level all the way to the CEO, and in 2025 we can expect experimentation and adoption of new technologies, including generative AI.

However, it's critically important to remember the human factor. Intelligence professionals will need to leverage tools such as artificial intelligence to increase data collection and processing efficiency while still demonstrating the indispensable value of human creativity. Intelligence professionals should adapt new tools into their work while ensuring they and their leadership convey to stakeholders the critical value of human subject matter experts to give companies security and essential insights."

Dr. Maria Robson-Morrow
Program Manager, The Intelligence Project, Belfer Center
Harvard Kennedy School

The impact of misinformation on risk analysis and reporting

"Corporate leaders will increasingly expect their security organizations to possess the skills and capabilities to provide early intelligence on issues and incidents that may potentially impact the business. Being caught 'off-guard' is not an acceptable position for a CSO, and it's incumbent that a security organization is able to proactively acquire and effectively communicate relevant threat information to company leadership in a timely manner."

Dave Komendat
President
DSKomendat Risk Management Services

"The rise of misinformation and disinformation has put a lot of pressure on companies to beef up their intelligence verification procedures. It's hard to know which of the issues coming through various feeds are true. At the same time, the volume of information is astounding.

There's been some talk of deploying AI to help solve this challenge, but given the propensity of some AI applications to provide misleading information, the technology isn't ready for prime time. Casting a wide net for intelligence isn't really feasible at the moment. To get a handle on the problem, companies will need to fine-tune their feeds to only focus on information directly impacting their environment. The guideposts of compliance and oversight are the new frontier here. Companies must focus on creating structures that ensure ethical and legal responsibility as they navigate complex issues like AI-driven disinformation."

Fred Burton
Executive Director, Protective Intelligence
Ontic

The impact of misinformation on risk analysis and reporting

"Advances in threat detection and risk monitoring technologies are changing how organizations approach risk management. Capabilities that surface information in near real time allow risk managers to detect an unfolding situation faster than ever. Data analytics and AI-driven insights help organizations to make conclusions and mitigate risks more effectively.

However, as the global risk environment changes and threat actors grow more diverse, it is crucial for organizations to develop comprehensive security risk management capabilities. This means investing in intelligence platforms in which tools are an important part of the intelligence cycle, especially for early warning and analysis, and support, or complement, expert analysts and professionals on the ground who need to verify and direct the process.

Navigating global friction, uncertainty, chaos, and danger requires careful integration of technology to manage workforce security, duty of care, and broader resilience."

James Robertson
Security Director
International SOS

Chapter 3: Investigations

A renewed focus on workplace violence and insider risk

As state-sponsored threats and social engineering attacks grow, experts emphasize that stronger investigations will be essential in 2025. Security professionals also foresee a renewed focus on workplace violence (WPV) prevention, particularly given recent legislation requiring employers to develop WPV programs. Empowering employees to identify early warning signs will likely also increase reports of potential risks, further boosting the need for thorough investigations — and solutions to streamline the process. Despite the rapid growth of AI startups and a market expected to surpass $820 billion by 2030,[1] many businesses could strengthen their security efforts to better protect their assets and IP. Experts say it's important to leverage tools like predictive analytics in your investigation workflows, helping your teams proactively mitigate insider risks.

[1] https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide#market-size

A renewed focus on workplace violence and insider risk

"In 2024, AI startups secured some of the largest funding deals in the history of venture capital. The most prominent among them are adding, if slowly, security risk management headcount to their growing companies. Many of these VC billions, however, are invested in talent and hardware-led companies with a lean approach to hiring and an even leaner approach to risk management. In some cases, these enormous investments create valuations exceeding $100 million per employee, on par with chip-making behemoth Nvidia and 20x that of Tesla. Yet almost none of these startups dedicate substantial resources to security.

This growing imbalance between investment value and the resources dedicated to safeguarding those investments will create significant security risks in 2025, not least in terms of insider risk. In an IP-driven industry, startups and their backers would be wise to ensure security keeps pace with growth."

Robin Welch Stearns
Chief Executive Officer
Pacific Resilience Group

"Gone are the days of "See something, say something." Instead, it's "See what? And say what?" In 2025, organizations are going to place more focus on employee training on the specific types of things that raise red flags. One factor that is driving this trend: an increasing number of employers fall under regulations or legislation that require them to build workplace violence prevention programs, which affect employers in New York and California, and hospitals around the country. Simply having a program isn't enough. Employers will need to focus on training that helps them understand what behaviors raise concerns and where to report them."

Cindy Marble
Senior Director, Threat Assessment Management Operations
Ontic

A renewed focus on workplace violence and insider risk

"In the year ahead, organizations and their respective security programs will place more focus on developing a security metrics program and will rely heavily on data-driven decision-making to anticipate and mitigate risks. As security threats become more sophisticated, predictive analytics will be key in helping organizations analyze large datasets to identify emerging trends in both digital and physical security threats. This will enable a more proactive response versus reactive incident and crisis management. Security organizations will also look to onboard a centralized database, such as incident management platforms that collect, manage, and analyze their security data.

With the availability of vast quantities of data in security programs — stemming from incidents, investigations, threat management, security tasks, intelligence, surveillance, and access control systems — security leaders are increasingly expecting frequent and comprehensive reviews of security metrics. This is driven by the growing role of data analytics in both cyber and physical security.

To take advantage of the predictive power of data analytics, security teams need to regularly assess key metrics to identify patterns, realign their focus, and adjust their mitigation tactics. Developing a rhythm to assess and present security metrics to security teams and organizational leaders will be critical. Lastly, security leaders will look to onboard security professionals with the knowledge and motivation to utilize data analytics in their practice and the ability to develop unique security metrics, make decisions, and take action based on the results."

Dr. Farhad Tajali
Author of Utilizing Data Analytics in the Field of Physical Security
Director, Global Security Systems and Data Analytics
Creative Arts Agency

A renewed focus on workplace violence and insider risk

"Insider threat programs need to expand to include other stakeholders — human resources, legal, IT, business operations — to better address security risks as business risks. There are two emerging trends supporting this reality: workforce education on WPV and the increased aggression of state actors.

On WPV to identify risks: The implementation of California's workplace violence legislation resulted in more of our clients asking for support in building a workplace violence program, which has led to an increase in person of interest investigations requiring inter-department collaboration.

Regarding corporations facing aggressive state actors: These threats are either made directly or by using proxies that threaten enterprise operations, which increases the need for stakeholder awareness.

Insider threat programs will need to educate and include stakeholders in the c-suite, board of directors, and the workforce to effectively identify, mitigate, and respond to these threats."

Karna McGerry
Vice President, Managed Services
Red5 Security

"As cyber security continues to become more effective in hardening firewalls, we are likely to see an increased effort by criminal groups to recruit, extort, or elicit insiders to gain access for criminal gain. Insider risk management teams would be smart to double down on employee awareness of elicitation."

Tim Kirkham
Managing Director, Global Head of Insider Threat and Fraud
Macquarie Group

Chapter 4: GSOC

Enhancing situational awareness and threat monitoring as geopolitical threats evolve

Security professionals predict that 2025 will bring a “great recalibration” for corporate security as employee travel and events return to pre-pandemic levels and companies consider permanent in-office or hybrid work policies. This shift, combined with global conflicts, U.S. political tension, and rising climate events, has broadened the threat landscape significantly. Many experts stress that establishing and supporting a GSOC is essential — even with budget cuts and restructuring. A centralized, comprehensive view of threats will be invaluable in navigating growing uncertainties.

Enhancing situational awareness and threat monitoring as geopolitical threats evolve

"In 2025, there will be a 'return to normal-ish' as security teams see their threat landscape expand to include the pre-pandemic perimeter alongside work-from-home issues. The effects of the pandemic are largely in the rearview mirror, and that's changing how we do business. More companies are having employees come into the office, and executive travel is up. But work-from-home arrangements are not going away.

Companies will need to protect employees in their offices and monitor executive travel with risk briefings, route awareness, and itinerary planning. These common pre-pandemic practices are actively being revived, but it's been a while since some teams have had to manage a significant volume of these issues."

Manish Mehta
Chief Product Officer
Ontic

"Employers have a 'duty of care' responsibility to all employees when it comes to travel and event security. Building a travel security program that provides timely threat and risk information for traveling employees is now an expectation. Companies must ensure that travelers are well prepared for the environment they are entering when traveling both domestically and internationally. Situational awareness is a travel imperative, and employees need accurate and up-to-date travel risk information pushed to their mobile devices to help them stay safe and secure.

Creating a documented event security program that evaluates risk and sets repeatable physical information and personnel security standards is an important way to manage event security risks. Whether the event is held on company property or offsite, having a defined program that incorporates pre-event intelligence, local law enforcement coordination (where appropriate), venue security planning, emergency and medical response planning are all fundamental requirements of a solid event security program."

Dave Komendat
President
DSKomendat Risk Management Services

Enhancing situational awareness and threat monitoring as geopolitical threats evolve

"In recent years, more organizations have recognized the value of establishing a GSOC, whether virtual or physical, and continue investing in it. This trend is directly linked to global events, including the situation in Ukraine and the tensions in the Middle East — and even reflected at home in the U.S. through protests on campuses and in major cities. These developments emphasize the need for a robust organizational presence. Additionally, increasingly severe natural disasters such as hurricanes, wildfires, and earthquakes drive the necessity for proactive measures to mitigate business risks.

Business travel is poised to surpass pre-pandemic levels in 2025, with more people on the move and traveling to risky global hotspots, heightening the demand for effective travel risk management. Looking ahead, we'll likely see continued, gradual GSOC investments in response to these global and domestic events."

Mike Gilbert
Vice President, Client Advocacy
Ontic

"In today's complex global business environment, where information moves at the speed of relevance, corporations require a 24/7/365 capability to see the world in real time and make sense of it. The challenge lies in anticipating potential disruptions that threaten assets, sensing emerging opportunities, navigating the complexity of the environment, and making timely, informed business decisions amid the daily noise and stimuli. There is a growing interest in transforming the traditional Security Operations Center (SOC) into an Operations and Intelligence Fusion Center—one that offers broader participation, greater value, and a higher return on investment across the enterprise, including business operations. Operations and Intelligence Fusion Centers offer firms an opportunity to innovate their operations and gain a competitive advantage."

Scott Morrison
Senior Director of Corporate Security
Tomahawk Security

Enhancing situational awareness and threat monitoring as geopolitical threats evolve

"While many have harkened a 'return to geopolitics' in recent years, geopolitics has always been an ever-present overarching force to account for in risk mitigation. This 'return' is really a renewed focus for corporations needing to provide context for many of the significant conflicts and varied economic developments occurring at a staggering pace.

Perhaps most significantly for the evolving threat intelligence landscape, we have seen an increased (or, at least, more easily identifiable) effect of geopolitical influences within the United States — whether it be cyber, economic policy, foreign government, transnational criminal, terrorist organization, etc. — over the last few years. This trend is likely to continue.

It will be interesting to see if U.S. corporations with minimal foreign footprints realize the need to mitigate potential risks stemming from this shift and devote needed attention and resources in a time of widespread corporate restructuring and cost reduction."

Lou Silvestris
Risk Intelligence & Investigations Manager, Protective Services
American Family Insurance

"We must never forget that we are dealing with determined adversaries. As practitioners, we must employ a zero-tolerance approach and not allow ourselves to become dismissive or apathetic to any of the potential security issues facing us. Intelligence is increasingly pointing toward threats escalating simultaneously; thus, security teams must employ a multi-front approach. Engaging individual pieces of a threat is no longer a viable mitigation strategy. Our communities' current climates demand that we think more expansively and encourage an approach to threat intelligence collection, dissemination, investigation, and ultimately 'bad actor' disruption that relies on partnership and collaboration. In the end, it's all about mitigating risk."

Bryan Flannery
President
Foresight Security Consulting

Enhancing situational awareness and threat monitoring as geopolitical threats evolve

"The Security field is continuing to evolve, and the stakes are higher than ever. With a number of major armed conflicts taking place simultaneously, the geopolitical operating environment presents multiple concurrent threats for companies to navigate. Complex risks to personnel, assets, and operations are at an all-time high, and with state-sponsored economic espionage and sabotage threats increasing across the globe, it is crucial that teams continue to level up and be ready to provide the solutions that senior executives need."

Lewis Sage-Passant, PhD
Global Head of Intelligence
Novo Nordisk

"In 2025, the critical importance of the GSOC will drive the industry to make strides in professionalization. One factor driving this shift is that the number of GSOCs is growing. Because they require 24/7 operations, GSOC staffing will remain challenging. To retain their people, GSOC leaders will need to focus on employee engagement, provide the right training, and offer additional incentives, such as pathways for advancement."

Fred Burton
Executive Director, Protective Intelligence
Ontic

Chapter 5: Security Management

The role of artificial intelligence and cross-team collaboration

Risks continue to be complex and interconnected, prompting security leaders to focus on integrating physical security and cybersecurity teams for more substantial strategic alignment. Organizations emphasizing cross-functional collaboration will build resilient defenses and enhance their incident response capabilities.

Experts also predict that corporate security teams will face the dual challenge of AI, striving to harness its powerful capabilities while mitigating its risks. While AI-driven solutions can enhance efficiency and effectiveness, concerns about data privacy, transparency, ethics, and potential misuse remain significant issues for security leaders.

The role of artificial intelligence and cross-team collaboration

"The risks faced by multinational corporations are increasingly interconnected; they sit across and between risk functions, and what starts as a physical security incident can quickly and unexpectedly impact cyber security, reputation, supply chain, or compliance risk, and vice versa. As a result, smart CSOs are looking for ways to work seamlessly across risk functions, from strategic to tactical levels.

The relationship between corporate security and cyber security is critical. Key touchpoints between the functions include insider risk, executive protection, information security, fraud prevention, intelligence, security operation centers, and security technology. It is increasingly difficult to deliver a truly comprehensive and effective response without collaboration

Alignment between corporate security and cybersecurity is organizationally agnostic. I have interviewed CSOs that run converged security models but complain about siloes within the function, as well as those that are not converged but have achieved highly effective partnerships with cyber security colleagues.

CSOs must identify ways to optimize the relationship with cybersecurity to derive maximum value for the corporation and a unified risk picture for the board, regardless of their organizational model. Outcomes trump org charts where risk management is concerned."

Rachel Briggs, OBE
Author of Connected Corporate Security: How to Manage Threats and Risks with a Unified Model and The Business Value of Corporate Security
CEO and Founder
The Clarity Factory

The role of artificial intelligence and cross-team collaboration

"The future of collaboration and convergence in physical security will be driven by the integration of advanced technologies, particularly AI, Internet of Things, and smart systems. AI-powered surveillance and data analytics will play a crucial role in enhancing threat assessment, enabling real-time analysis of vast amounts of security data to identify potential risks more accurately and proactively. By centralizing information from cameras, access control systems, analytics, and alarm sensors, security teams can collaborate more effectively, making faster, data-driven decisions.

AI's ability to recognize patterns and predict threats will lead to improved incident response and resource allocation. As physical security systems become increasingly interconnected, AI will also help automate routine tasks, allowing security personnel to focus on higher-priority issues. This convergence fosters a more adaptive, resilient, and efficient security environment, with the ability to respond swiftly to emerging threats and challenges."

Bill Davis
Senior Director of Physical Security
Ally Bank

"In 2025, we'll see security teams develop closer relationships with their IT teams to overcome roadblocks to modernization, particularly in case management. Many security teams are at an inflection point. Their current case management software is antiquated and often inflexible. They've resisted improvements because change management is difficult. Investigations are getting more complicated, with new sources of data and higher volumes of data. On the other hand, new case management systems facilitate deeper connections between data and, ultimately, better insights."

Manish Mehta
Chief Product Officer
Ontic

The role of artificial intelligence and cross-team collaboration

"The near future of collaboration and convergence in security will be shaped by the need to adapt to the changing ways organizations operate. Many employers are adopting dynamic, flexible work models, offering employees more autonomy, while others are focused on bringing their workforce back to the office. Regardless of these differing approaches, the importance of understanding and preparing for the next wave of threats and operational risks is more critical than ever.

As technologies like AI and automation continue to evolve, organizations must embrace solutions that provide a proactive, 360-degree view of the security landscape. The convergence of physical, cyber, and operational security functions will require systems capable of adapting to the complexities of a hybrid work environment. Real-time data sharing and seamless integration across platforms will be essential for identifying emerging threats and risks early, allowing businesses to respond swiftly and mitigate potential vulnerabilities. The roadmap to staying ahead involves fostering collaboration, investing in adaptive technologies, and maintaining a proactive stance on security."

Justus Abhulimen
Director, Corporate Security Operations & Intelligence
Twilio

"For 2025 and beyond, securing budgets for AI automation and integration will be imperative to driving efficiencies, enhancing decision-making, and keeping up with technological advancements. But first, spending time to build your AI strategy will be even more imperative for long-term sustainability and starts with understanding which tasks can be completely AI managed, AI enabled or AI assisted. This strategy creates the conditions for the elimination of low complexity, repetitive tasks and increasing human touch on higher, more sophisticated interactions, which will ultimately drive better business outcomes. Those who prioritize developing a strategy will be better positioned to make the case for investments in and implementation of AI."

Arian Avila
Vice President, Safety & Security Executive
Capital One

The role of artificial intelligence and cross-team collaboration

"The trend toward AI and machine learning will slow in the year ahead as many organizations that purchase software and integrate technology continue expressing concerns about the potential risks AI might reveal. However, the promise of AI is still that it can enhance security team effectiveness and speed up decision-making by combining internal and external data and synthesizing it into recommendations and actions.

Despite its potential, there is currently more fear than optimism, so vendors have a long way to go to increase buyer confidence."

Mike Gilbert
Vice President, Client Advocacy
Ontic

"Corporations and family offices are seeking to leverage large language models (LLMs) and AI. Leaders in the threat intelligence industry will need to navigate the societal impacts caused by AI and its human masters.

Risk managers should take into consideration the various risk areas caused or amplified by AI as its use within our social, business, and technological circles is dramatically changing the threat landscape. Key areas of concern include ethics, data privacy, security, financial impact, lack of transparency, socioeconomic inequality, and malicious instances of AI.

Public AI models are being open-sourced, and private AI instances are now a reality. Soon, individuals will carry around their own private AI in their pockets. Security leaders may need to bring in experts to get ahead of the curve, allowing organizations to benefit from the increased productivity of AI without jeopardizing their people, data, or operations."

Kris Coleman
Chief Executive Officer
Red5

The role of artificial intelligence and cross-team collaboration

"In 2025, the use of AI in physical security will transform security programs and incident management, enabling faster response to crisis and enhanced decision making. This change will be made possible by the availability of more reliable security data, ingested and analyzed by various AI-powered applications. These applications will provide real-time analysis of threat and intelligence monitoring, video surveillance, and access control systems, enabling quicker identification of potential threats such as persons of interest, unauthorized access, suspicious behavior, gunshot detection and gun recognition, environmental hazards, and natural disasters, identifying the potential impact to organizations and their assets quickly. These applications will continuously learn from patterns, enhance data accuracy, and reduce false positives.

Using AI and LLM within GSOC environments will greatly enhance knowledge management capabilities, providing operators faster access to large volumes of information, such as standard operating procedures and playbooks. Therefore, AI will play a critical role in decision-making, allowing faster and more precise crisis responses.

Additionally, using autonomous AI-powered agents could significantly enhance the efficiency and effectiveness of support for security staff and the employee population by automating tasks, providing real-time insights, and reducing human error. Autonomous agents can handle repetitive tasks, such as low-level incidents or employee requests, including answering common security and safety questions, responding to employee inquiries quickly and in real-time, and escalating unresolved inquiries to a service ticket as needed. The 'autonomous security agent' can act as a force multiplier, supporting the security program, employees, and the organization."

Dr. Farhad Tajali
Author of Utilizing Data Analytics in the Field of Physical Security
Director, Global Security Systems and Data Analytics
Creative Arts Agency