ONTIC

WHITEPAPER

Security Industry Forecasts for 2023 and Beyond

PERSPECTIVES FROM THE COMMUNITY

As we close out 2022 and look forward to new challenges in 2023, the Ontic Center for Protective Intelligence has put together this forecast documenting some of the trends and ideas we believe will shape our industry and the business world in the coming year. In this document, we hope you will find ideas to help you understand the current security environment you're operating in and anticipate critical changes before they impact your operations.

In recent years as we've confronted multiple large-scale, high-impact crises, it's become abundantly clear that those who protect must understand a wide range of disciplines and global situations to anticipate the evolving risk environment and mitigate threats. While our forecast has a heavy focus on security issues – including insider threats, safety in the workplace, political polarization, and the convergence between cyber and physical security disciplines – we've also included discussions of adjacent fields like geopolitical conflict, technology, leadership burnout, and the importance of soft skills in security.

I wanted to share two big-picture thoughts. First, I'm proud that Ontic has put together such a diverse and experienced group of professionals, both inside the company and across our network of clients and friends, who have been willing to share their thoughts and ideas to benefit the larger community. That diversity of thoughts and expertise informs everything we do to help protectors understand and counter challenges. Second, the great diversity of thought leadership we've assembled often creates different viewpoints on challenging situations and the way forward. Rather than distill all of these thoughts into a single voice, we believe it's important to portray how our differing viewpoints and experience may lead us to have differing opinions about how situations will evolve. Learning more from these professionals and understanding the trends they're witnessing from their perspectives will help us all to be more effective at anticipating and mitigating risks in our own domains.

We welcome feedback and comments.

Thank you,

Fred Burton

Fred Burton
Executive Director,
Ontic Center for Protective Intelligence

TURN THE PAGE TO DIVE DEEPER INTO EACH THEME THAT ROSE TO THE TOP

Nurturing and Retaining Talent

With physical threats only increasing in volume and sophistication, compounded by the third year of a global pandemic, security professionals are seemingly burnt out and worn thin. We are witnessing leadership that is impaired to lead in addition to a shortage of security and safety professionals. So, how can our industry overcome these staffing challenges while combating fatigue?

There will be a substantial shortage of physical security and public safety professionals – the 'foot soldiers' that protect others in both the public and private sectors – leaving organizations to fill the gaps. Demand for these professionals will grow due to increasingly violent incidents, but a decline in interest in the profession will cause a serious hiring gap. Organizations must be prepared to fill the gap, both by paying higher prices for trained and qualified protection professionals, while also shifting their paradigm to address the threat using protective intelligence. Hiring of protective intelligence analysts with criminal analysis expertise, greater use of technology and early threat warning data, and deployment of plainclothes security professionals who proactively act on that information can fill the void.

FRED BURTON
Executive Director, Ontic Center for Protective Intelligence

In 2023, corporate security practitioners must find ways to overcome staffing challenges while navigating emerging challenges because of the growing mistrust in government and corporate entities. Remaining agile while implementing security protocols that are reliable, relevant, resilient and repeatable will be critical to success. Successful practitioners will have developed the optimal mix of intelligence, technology and technical competencies to control the environment.

WILLIAM PLUMMER
CSO, RaySecur

In 2023, there will be significant increase in fatigue and burnout among department leadership and C-suite personnel, primarily due to nearly three years of navigating stresses from the pandemic, on top of global unrest and other large-scale issues. This increase in fatigue and burnout will lead to 'impaired leadership' in many aspects of organizations, including C-suite, security departments, and other departments in the organization. Security teams will likely experience this in a few ways: retirement or departure of security leadership; turnover in C-suite leadership that will require establishing new working relationships with incoming C-suite personnel; and/or, navigating relationships with department leadership and C-suite leadership that are less reliable or more fractured than previously experienced. Security professionals can be aware of this potential impact and prepare for the need to hire new security personnel and/or find ways to work with colleagues (in any department) who are impaired in their ability to perform their responsibilities.

MARISA RANDAZZO
Executive Director of Threat Management, Ontic

Attracting, developing, and retaining next-generation talent will be a key risk mitigation for corporate and institutional resilience – in our increasingly chaotic global operating picture. Analytic technical acumen is now in high demand. Risk mitigators now know what fair pay and life balance look like. An increasingly competitive labor market provides opportunity for proven players.

FRANCIS D'ADDARIO
Emeritus Faculty Lead, Strategic Innovation, Security Executive Council

Addressing Geopolitical Challenges

It's clear now that many companies are assessing geopolitical security risks, wondering how to protect their supply chains, how to comply with sanctions and how to manage reputational risk associated with these events. As we reflect on this past year, it's no wonder that increased physical threats and company backlash related to geopolitical, activism and social justice issues were reported by 25% of physical security leaders as a program concern.

This raises the question: what are security professionals worried about looking into the future as geopolitical conflict continues to unfold?

Organizations will need to continue to monitor and respond to all the current major global issues that will persist into 2023 such as the Russia-Ukraine War, continued aggression by China, climate change driven severe weather, supply and transport disruptions, along with global stress and unrest driven by continued inflation and food insecurity. Protective leaders should plan for potential issues such as a new and more challenging COVID variant, nation-state aggression, territorial disputes and political instability. Success in navigating this dynamic global environment where the frequency and severity of threats and events seem to be ever-increasing will require: 1) more continuous risk monitoring (current and evolving) and assessment; 2) balancing current response activities with proactive preparedness; and 3) staying abreast of changing organizational objectives and enhancing your risk-related communications with management.

BRUCE MCINDOE
President, McIndoe Risk Advisory, Founder, iJET/WorldAware

Worries over a possible invasion of Taiwan and North Korean aggression are valid, but the main attraction is seeing just how long China can maintain its zero-COVID stance. People there still live with the constant threat of sudden lockdowns and business closures, now years into the global pandemic when much of the world has returned to normal. The impact of China's pandemic measures are significant, and the longer the government persists, the more it risks triggering economic instability at home and across the region. Businesses reliant on China are glancing in India's direction more as they worry about rising costs and a challenging COVID situation. Remember, it's not just the housing market and domestic consumption. With zero-COVID, there aren't millions of Chinese tourists flying to Japan, Korea, and Australia to spend their money.

Regionally, expect the U.S. to enhance military cooperation among its closest allies. There will be a renewed focus on rebuilding damaged relationships with partners, a la the Philippines, as it also attempts to edge countries like Vietnam and Thailand further away from China's sphere of influence.

STUART DEAN
Owner, Value Outlook, Former Geopolitical Analyst, Microsoft

In 2023, geostrategic issues will drive investment and budget decisions. These decisions will be risk-based and security teams will need to have the comprehensive risk data to back-up funding requests. Corporate security teams will need to prove the value of nothing happening in security and how in risk, there is also always opportunity. Geopolitical issues will continue to spur movement away from having executive protection teams physically on the ground in every region. Because there will be fewer boots on the ground, companies will have an even greater need for intelligence-driven, operations led, threat informed activity through holistic intelligence software solutions.

CHUCK RANDOLPH
Vice President of Security and Intelligence, Ontic

2023 is likely to see an increasing demand for security teams to help contextualize and navigate the turbulent geopolitical risk landscape that has dominated 2022. The global landscape is undergoing radical shifts, and understanding how these changes will impact operations and plans will be crucial for companies with international exposures. Security teams now have an opportunity to provide an added value to corporations, as expert advisors on these complex environmental challenges such as geopolitical disruption to supply chains, and political risks associated with expansion into new territories. Security teams should increasingly have a seat at the table for strategic corporate decisions in order to mitigate the dangers in this complex new operational landscape. Against the backdrop of all of this change, however, security teams will still need to demonstrate a continued mastery of the day-to-day basics. Political polarization and economic challenges will drive increased tactical threats and insider risks in the coming year, and companies cannot lose sight of the dangers they pose.

LEWIS SAGE-PASSANT
Global Strategic Intelligence Manager, Salesforce

Europe faces three significant challenges in the coming 12 months. The war in Ukraine, energy security and inflation. Although it has made significant progress in retaking territory, a decisive Ukrainian battlefield victory is unlikely in the short-term and a prolonged conflict in the coming months is the most likely scenario.

ROSS HILL
Director of Intelligence, AT-RISK International

Comprehensive 'Protective Intelligence' policies, procedures and programs will be more essential than ever in 2023 for governments and organizations. An increasingly polarized 'post-pandemic' world coupled with the 'weaponization of politics' will likely continue to promote a permissive environment for increased incidences of intentional or targeted violence in the coming year. Specifically, in addition to the now all too familiar acts of extreme violence such as active assailant (mass shooting) incidents, I predict we will see a potential resurgence of more traditional targeted attacks such a kidnapping and political assassinations in 2023 and beyond.

DAVID BENSON
Owner, DJ Benson & Associates

When considering how to identify and mitigate risk in Asia, corporate security and risk teams should keep in mind the Taoist concept of Yin and Yang. For thousands of years, two circling fish, each clearly in black and white, have represented the coexistence of separate and opposite truths. Using this Yin/Yang imagery, readers might wish to take all of the regional (and global) strategic risks mentioned by other contributors in this publication and group them in an area no larger than the white Yang fish, because they really only represent half of the challenge. For the black Yin fish, readers may wish to consider risks associated with their own teams' construction, mandate, and activity. Taoism teaches the importance of self-reflection and looking at both the details and the big picture from all angles. In Asia, I worry weak and unbalanced security and risk teams are not adequately empowered or resourced to address the risks of the multi-polar post-pandemic recessionary moment.

JAMES TUNKEY
Chief Operating Officer, I-OnAsia

Mobile devices will continue to be a major form of communications for data, voice, video and messaging. The threat of intercepting voice, video, and messaging will increase, both from criminals for financial gain, nation state actors for espionage, or other unauthorized third parties.

Tools are now readily available to intercept mobile communications, and the availability of low orbital satellites increased the ability to identify, track and target individuals in near real time. Protecting information on a mobile device, whether originating, received or stored, will require as much attention as protecting the enterprise. This will include identifying apps that broadcast the users location (even when turned off) and implementing strong encryption for communication channels.

We will continue to see nation states infiltrate software companies as employees or owners, and will need to rethink trust when it comes to third party applications.

DON SORTOR
Senior Vice President, Global Integrity

Addressing Violence in the Workplace

The 2022 Mid-Year Outlook State of Protective Intelligence Report showed that 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. Whether working from home or on-site, more than half (54%) of respondents reported they don't have a mechanism in place that allows employees to anonymously report issues.

Identifying possible violent threats in the workplace that may be on the horizon is becoming more important as threats to businesses rise. But what preventative measures can leaders take? What trainings, assessments and other tools can businesses use to reduce stress, risk, conflict and overall potential threats as they relate to workplace violence?

As corporations look forward to 2023 and providing a safe work environment for all employees, the impact of domestic violence and sexual harassment prevention training cannot be overlooked. A 2018 national survey of domestic violence survivors found that 83% of survivors reported that their trauma disrupted their ability to work. Another study has found an average cost to employers of US $22,500 per employee in lost productivity and employee turnover due to sexual harassment.

Active threat training is not the same as helping employees understand, recognize, articulate, and have self-confidence to prevent the escalation of early warning signs of inappropriate behaviors. What many employees are missing is the foundation on which to apply these learnings. Employees need to be taught to think differently, to see differently, to articulate behaviors in ways that give HR and security teams actionable information to deal with inappropriate behaviors that threaten safe work environments.

KELLY SAYRE
Founder & President, The Diamond Arrow Group

In Q3 and Q4 of 2022 we saw an increased reduction in corporate security positions as talk of a recession loomed. With a little over a year of distance from the pandemic, more companies returning to the office, and still struggling community resources I believe 2023 will inevitably bring an increase in preventable Workplace Violence incidents. From the reactivity of aggressive pushing and shoving to a targeted attack of tragic violence, leaders should begin bolstering their workplace violence prevention efforts now by creating and maintaining Behavioral Threat Assessment Teams that work cross-culturally to include security, HR, and legal. Leveraging a company's desire to best serve its employees, security professionals and practitioners should be outspoken evangelists for holistic security programs. Preventative measures like reporting mechanisms, policies, and multi-disciplinary threat assessment and management teams should be parts of the comprehensive programs all organizations strive for. Prevention of targeted violence is certainly the goal, but better care for people can be the standard by which we achieve it.

BRYAN FLANNERY
President, Foresight Security Consulting

Employees are still carrying 2+ years of stress as they return to the office, which will increase the risk of both physical and verbal conflict with others. In many ways, the pandemic stunted our ability as a society to socialize and tactfully navigate interactions with others in difficult or potentially emotional situations. The declining ability for people to effectively communicate and navigate the potentially awkward ramifications of returning to the office will result in increased stress and conflict in the workplace.

Companies that are more mindful of the need for work-life balance for employees, and become more flexible regarding work-from-home policies, PTO, and family leave, will likely see a reduction in employee conflict and threatening behavior. For nearly three years, people have grown accustomed to working from home, which allowed them to spend more time with family and participate in activities that a rigid in-office work schedule did not previously allow. Coming out of 2+ years of pandemic-related stress does not mean that employees will automatically go back to "normal." Many employees will benefit from increased flexibility in where, when and/or how they perform their jobs. Company leadership that recognizes this need for their employees (and managers, leadership too) will likely see a decrease in potential conflict and decrease in employee turnover as well. Security teams must also be mindful of this shift and adjust their employee policies and processes accordingly, looking for creative solutions (such as job sharing) where possible.

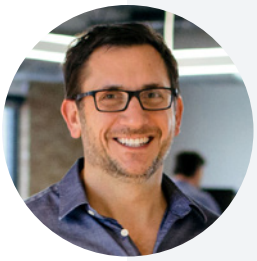
MARISA RANDAZZO
Executive Director of Threat Management, Ontic

The social impacts of the pandemic, resulting isolation, and financial impacts on individuals will be felt for many years to come. We have seen and will continue to see the long-term impact of these stressors on the global population, which in some cases have reframed their overall perspective on what they value in the world. The global trust barometer produced by Edelman for several years has illustrated an overall increase in distrust of our politicians and the media, with corporate CEOs now entering the distrust arena.. With the reductions in force and offshoring of jobs, the level of trust in these organizations will likely also diminish. Leaving populations to seek the truth through their own social collective, which could include online platforms potentially populated with misinformation. All of these factors will likely lead to increases in the current trends of targeted violence in schools and workplaces. We should also anticipate the targeting of executives and political figures globally. Lastly, the re-emergence of organized criminal activity targeting high-net-worth individuals, their families, homes, and assets are sure to increase. Evidenced by increased gang and carter activities domestically and abroad.

CHUCK TOBIN
President & CEO, AT-RISK International

Proving the Value of Security

It's more critical than ever before for organizations to prioritize security and ensure teams have the recognition they need to unlock the resources necessary for an effective corporate security program. So how do security teams get the budget, respect, and support they need?



Soft skills are more critical than ever for physical security professionals in 2023, as the industry continues to undergo a sea change accelerated by technology. Hard skills, such as tactical driving or shooting, and law enforcement or military experience were once foundational requirements in the security industry. Today, soft interpersonal and communication skills, and people from diverse experiences including academia, technology and research, are increasingly important. Security professionals must be able to cull and distill information on potential threats across multiple lines of business and communicate to management the value of protecting their organization in a more holistic way. Refined soft skills will help security professionals accomplish these things.

THOMAS KOPECKY
President & Chief Strategy Officer, Ontic

Permacrisis. Collier's 2022 word of the year is a call to 2023 action: an unprecedented time to turn ongoing crises into new opportunities. As leaders continue to feel and show the strains of responding to new and old threats, we are challenged to find alternatives, to transform reaction into action, to build a shared language and culture of trust. Successful and safe organizations will be those that acknowledge weariness, embrace vulnerability and understand trust is a security force multiplier.

MELISSA MUIR
Director of Human Resources and Organizational Development, City of Shoreline

There will be a no-contest showdown among security SaaS platforms. Those attempting to connect disparate platforms from a wide range of sources will continue to see gaps and increased vulnerabilities. Their limitations will be easily "unmasked" by robust, native-built, seamlessly-engineered and comprehensive solutions that provide a clearer, wider and more accurate picture of the threats facing their organizations.

Companies will prioritize a shared understanding of risk to safeguard the business. Teams across the organization will need to break down cultural, technology and operating silos for more effective collaboration and a clearer operating picture of their security landscape. Security leaders will face pressure to prove business value, and the best way to do this is to have a complete picture of both organizational vulnerabilities and threats in a single platform. Leadership will begin to prioritize and invest in technology that eliminates these barriers and increases cross-team communication and data collection and analysis, to foster a more comprehensive risk mitigation strategy.

MANISH MEHTA
Chief Product Officer, Ontic

Mitigating Insider Threats

In the 2022 Mid-Year Outlook State of Protective Intelligence Report, 30% of respondents reported cyber-related insider threats that also share physical security implications as a program concern. As the different parts of the workforce adopt a new hybrid model, remain remote, or return to office, security teams are tasked with staying one step ahead of potential insider threats that are introduced by the work environment.

Interest in the metaverse and virtual reality will elevate how the human and physical world are inextricably connected to the cyber and virtual... and in an expected way – insider threats. Security breaches are not 100% avoidable, but manageable. Companies will increasingly recognize that there are always people on the other side of a cyber attack, including potential nefarious insiders within their organization. To protect the enterprise, you have to get to those real-life bad actors. CISOs and CSOs should focus greater resources and attribution data on the physical access to their systems to better understand their virtual and real-world vulnerabilities, the potential for corporate espionage and to mitigate risk.

LUKAS QUANSTROM
CEO & Co-Founder, Ontic

The CISO and CSO can combine forces to fight insider threats like they've never been fought before as they acknowledge that insider threats are not solely digital, and humans are always involved. Mitigating these threats are not the sole responsibility of either department. Taking it one step further to also secure data from human resources and legal will be a start, though this collaboration must ultimately become a corporate mandate.

Human resources and security teams will have to work more closely together in 2023. Two main trends are combining to exacerbate insider threat risk. Hybrid work has removed a level of control from companies over data and device usage during work. It's very easy for an employee to use their smartphone to take a picture of sensitive info on a computer screen. Similarly, companies feel pressure to foster a culture of openness and transparency that often encounters friction when combined with a security mindset. Watch for increased collaboration and cooperation between HR, legal, and security teams to monitor and prevent IP theft and other insider threats.

THOMAS KOPECKY
President & Chief Strategy Officer, Ontic

The 2023 insider threat landscape will continue to evolve and change. Organizations can expect to see increases in volume and severity. Economic factors, combined with geopolitical and social unrest, in addition to hybrid work environments, will drive threat actors to use complex activities and recruitment strategies to achieve their goals.

Organizations should expect to see an increase in sophisticated attack strategies and tactics. Similar to the Uber breach in September 2022, actors will use tiered tactics such as a phishing attack followed up with socially engineered calls directly to unsuspecting victims. This tactic makes the "ask" from the actor seem urgent, legitimate and realistic.

Intensified use of social media to express personal grievances and discontent about employers will encourage like-minded individuals to become malicious insiders to achieve their personal goals. Social media also allows more sophisticated actors to target disgruntled employees and employ forced recruitment tactics such as bribery and extortion.

Insider threat is the responsibility of every employee at every level. As threat actors evolve, so must organizational insider threat programs. Insider threat programs should focus on incorporating a holistic approach including a comprehensive insider framework, communication throughout the entire organization, enhanced human centric training focused on the behavioral psychology of insiders and effective cyber tools. This holistic approach will offer a positive, proactive approach to anticipating and preventing insider threats.

JANET LAWLESS
CEO/Founder, Center for Threat Intelligence

Adopting a Holistic Security Strategy

While the industry has been talking for some time about cyber-physical convergence, as we look to 2023 and beyond, experts are realizing that the duty of care for an organization's security expands far beyond the physical security team. Breaking down silos and accepting the shared responsibility of risk will be fueled by universal software technology and consolidated threat intelligence. Collaboration of these departments also enables holistic data analysis for deeper visibility, speedy decision-making and clear communications across multiple functions.

The increasing complexity of new and emerging security risks, compounded by strained resources, whether staffing, budgetary, or otherwise, are the two biggest factors driving change across the industry. Succeeding in this environment requires a behavioral shift from viewing threats in isolation and grasping for one-size-fits-all solutions. For 2023 we can expect forward-thinking organizations strategically adapting security approaches to fit business needs and circumstances. This means taking a hard look at the data first in order to tailor holistic risk mitigation strategies that are informed by timely and accurate intelligence. The execution of these strategies will rely on advanced technologies, increasingly adopted from other industries, to complement the capabilities and enhance the effectiveness of existing security teams.

ALEX SAPPOK, PH.D
CEO, RaySecur

We will begin to see more cybersecurity experts embrace physical security. This will be in the form of a rise of security practitioners who have knowledge of both the cybersecurity and physical security industries. This convergence of security-related knowledge will also lead more businesses to create a Chief Risk Officer role to address security holistically.

CHUCK RANDOLPH
Vice President of Security and Intelligence, Ontic

In 2023, cyber-physical convergence will be a focus for security teams. As the threat landscape becomes more complex and increasingly interconnected, organizations need to build a bridge between their physical and cybersecurity intelligence to better understand, navigate and address potential threats. Accomplished through frequent inter-team meetings and technology, collaboration among these two sectors is going to be key for mitigating risk to an organization and its employees.

MANISH MEHTA
Chief Product Officer, Ontic

Organizations are struggling to manage a risk environment that is becoming more dynamic and complex. Risk management activities in most organizations are segmented and siloed starting at the Enterprise Risk Management (ERM) level and further siloed within the operational risk domain. The Protective Services disciplines – cyber security, physical security, personnel security, business continuity, emergency management, crisis management, supply chain security, and even environmental health and safety – are tribal, largely isolated and operate with siloed systems and data. This situation does not build confidence with senior management, the board or clients.

It is time to move to a more holistic risk management convergence top to bottom and across the protective disciplines. At the enterprise level, organizations need to jettison the list-based Enterprise Risk Register approach and move to an Objective-Centric ERM approach. That is, start with the board/senior management business objectives, assign a business owner to each objective, conduct a multidisciplinary risk assessment across all related risk domains, and assess the certainty that the objective will be met through an ERM risk register organized by the objective. This way everyone has a clear understanding of the risks, mitigation approach, residual risk, investments and certainty in the context of the organizational objectives to be achieved.

Likewise, for the operational risk domain, the aforementioned tribes would come together around each objective, evaluating the same data, and coming to a consensus risk assessment for the organization. This is what convergence should mean.

BRUCE MCINDOE
President, McIndoe Risk Advisory, Founder, iJET/WorldAware

Businesses face a growing number of threats, resulting in greater uncertainty and costs. According to the NOAA's National Centers for Environmental Information, there were 20 separate billion-dollar weather and climate disasters in 2021 alone. The final price tag? $145 billion. This year, more than six million acres of land have been burned due to wildfires, and damage continues to mount as a result of droughts, floods, and impacts on core infrastructure. While businesses cannot control when or where these natural disasters occur, they do have the ability to influence the impact on their people. In 2023, we'll see organizations deepen their focus on emergency preparedness and expand the use of modern technologies, such as threat monitoring tools, to further improve the connection to their people as well as reduce asset loss and improve business continuity before, during, and after severe weather events.

PETER STEINFELD
SVP of Safety Solutions, AlertMedia

FOR MORE INFORMATION PLEASE VISIT ONTIC.CO

ONTIC