ONTIC®

Whitepaper

Security Predictions for 2022 and Beyond

THE SECURITY INDUSTRY VALUES FEW THINGS MORE THAN A QUIET, UNEVENTFUL DAY — and 2021 was anything but quiet. Two years into the pandemic we've seen pent-up economic and political frustrations bleed into the workplace exacerbated by limited in-person interactions and social distancing mandates. Violence and physical threats to businesses are occurring at a record-high pace.

Predictions for the security industry are critical — they help us to see ahead, plan, and prevent bad things from happening. With threat actors becoming smarter, data becoming increasingly unmanageable, and the threat landscape rapidly evolving and expanding, it's more important than ever to think critically about the year ahead. In sharing informed, evidence-based learnings and expectations that help us to understand what the future may hold, we give ourselves the best possible chance of making the world a safer and more secure place for all.

Ontic's Center for Protective Intelligence spoke with leaders from some of the industry's most reputable companies, as well as its own internal experts, to source predictions for 2022 and beyond.

Turn the page to dive deeper into the following themes:

- Security challenges due to hybrid work continues
- Business continuity becomes a crucial component of security programs
- Strengthening cyber-physical convergence
- An increased need for protective intelligence technology
- Addressing hiring challenges when building a top tier corporate security team

Security challenges due to hybrid work continue

RETURN-TO-OFFICE policies have ignited more backlash than ever expected. Some companies have adopted a hybrid work schedule while others are requiring employees back in the office full time. This shift in the way the world works has caused a dramatic uptick in workplace violence for corporate security teams to address. Now, the duty of care is no longer solely in the office. Security teams are also responsible for keeping employees safe in their homes.

What will physical security professionals need to keep in mind as the workplace security challenges continue? What teams need to be involved internally to ensure proper procedures? Will insider threats play a greater role in the future of the remote workplace?

Physical security professionals will need to be adept at effectively waging a two-front war marked by return-to-office strains under a "new normal" tied to vaccine mandates, mental health and increasing workplace violence on one front, and protection challenges for a remote workforce on the other front.

Lukas Quanstrom
Chief Executive Officer, Ontic

Visionary CSOs and Legal leaders will play the largest role in the success of corporate physical security initiatives in 2022. Security, Legal and HR teams will experience collision as return-to-office policies complicate security procedures. For example, for large companies with thousands of employees, it is difficult to determine who is coming into work on any given day and where they are located ("hoteling"). This is a challenge for security teams who need streamlined, effective methods for communicating alerts and getting people to safety. Security and HR teams need to be aligned on policies to eliminate potential pitfalls. In these instances, technology can help.

Fred Burton
Executive Director, Ontic Center for Protective Intelligence

As the world recovers from the COVID crisis and returns to work, corporate security departments must brace themselves for the increased threat posed by employees and contractors who hold extremist ideologies: extremist insiders. While extremist insiders have always been a problem, the threat is increasing due to growing social polarization and is being compounded by the isolation of the past 18 months. It is amplified by the corrosive influence of social media. This threat will stem not only from extremist ideologies such as jihadism, anarchism, and white supremacy, but also from single-issue extremists to include Incels, and anti-vaxxers, among others.

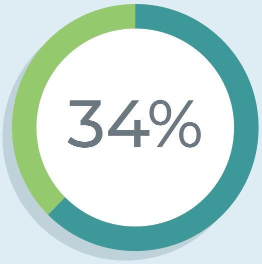
Scott Stewart
Vice President of Intelligence, TorchStone Global, Protective Intelligence Honors Pioneer

Business continuity becomes a crucial component of security programs

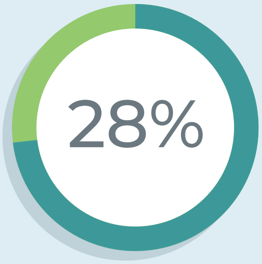
This year has put a spotlight on how security attacks, both from the cyber and physical realms, can affect business continuity. Whether it be an active shooter incident that makes global news headlines, someone making threats against your CEO, or even something as small as a fight amongst employees on the factory floor, these can all change how you are perceived by external stakeholders and how resilient you are able to be in the midst of a crisis.

Companies who adopt a proactive approach to security, one that helps to prevent bad things from ever happening in the first place, are better able to deliver on their vision and brand promise and keep the business functioning at the level it needs to be.

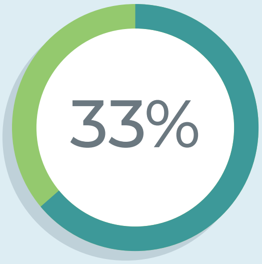
Ontic's recent 2021 MID-YEAR OUTLOOK STATE OF PROTECTIVE INTELLIGENCE REPORT highlights a variety of incidents that have occurred at companies since the beginning of 2021 as a result of intelligence failures, all of which have an effect on business continuity:



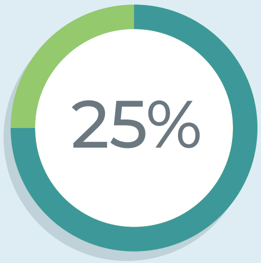
An insider abused authorized cyber access that led to property theft or supply chain damage



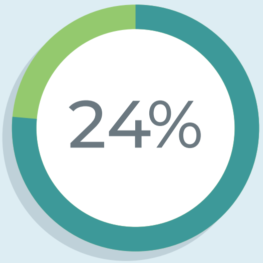
An employee was threatened and/or harmed while working remotely



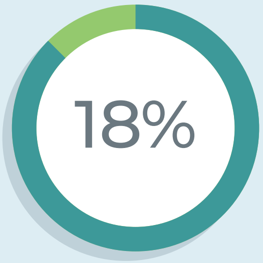
An employee was threatened and/or harmed while working at company facilities



A former employee threatened and/or harmed current employees



Our CEO and/or family members received threats and/or were harmed when working from their private residence or while traveling



An active shooter event occurred at one of our locations

What should employers and corporate security teams be doing to support business resiliency?
How can companies stop threats in advance, rather than waiting for a crisis to occur?
How should teams be aligning internally?

2022 is likely to be the year of the "new normal." As the pandemic begins to wind down, security leaders and their counterparts will need to chart a new, more comprehensive approach to risk monitoring and mitigation that is truly all-hazards in nature. A mindset of continuous learning and collaboration among other crisis, sustainability and business continuity functions will be required to stay ahead of the next uncertainty that may come from issues as wide-ranging as human rights and climate change or as immediate as insider threat from a disgruntled employee. Bosses will also need to stay on top of ensuring a healthy mindset and work environment among security staff who may be worn down after the perpetual crises of the last several years. In short, in the coming years, the job is getting bigger, the risks are becoming more acute and the need to keep a finger on the pulse of the threat environment has never been so important.

Meredith Wilson
Founder and CEO, Emergent Risk International, LLC, Protective Intelligence Honors Pioneer

Managing the complex threat landscape in a global capacity will be the greatest challenge facing corporate physical security teams in 2022. This can only be done with technology and scalable software solutions, due to the rapidly expanding threat landscape. The common threats everybody deals with such as workplace violence, disgruntled employees, etc. are, from a holistic perspective, the things that will hijack our daily narrative and daily life. For the security industry, it is often a tragedy that forces change. Most companies wait until a tripwire event occurs until they make these changes. Mindsets have historically been difficult to change absent some compelling event like this.

Fred Burton
Executive Director, Ontic Center for Protective Intelligence

Strategically, information will be a challenge that organizations must contend with. The vast amount of data and telemetry that is received must be managed and, where applicable, be used to create intelligence that informs decisions about risk. The ability to manipulate this data, thereby interrupting trusted processes, is perhaps the most profound challenge leaders must manage.

As we examine the following year, security will (and must) continue to embrace convergence. Risks can no longer be titled as just binary or physical; it doesn't care about hubris or territory. While the discussion concerning joining together to share and work on problems has been in the ether for some time, we will see organizations (both internally and externally) collaborating and coming together in "hubs" of holistic intelligence sharing. This will undoubtedly be a forcing function to test old ways and focus efforts and resources where leaders can best use them to protect and defend people and organizations.

Charles Randolph
Senior Director of Operations and Intelligence, AT Risk International, Protective Intelligence Honors Thought Leader

Strengthening cyber-physical convergence

When it comes to enterprise security, the physical world and the cyber domain have long been treated as separate. 2022 and beyond will prove to be the time when those days finally fade.

In a SURVEY commissioned by the Ontic Center for Protective Intelligence, both Physical Security (95% agree, including 45% who agree strongly) and IT professionals (95% agree, including 55% who agree strongly) that cybersecurity and physical security must be integrated, otherwise cyber and physical threats will be missed. What's more, 42% of those surveyed say cybersecurity alignment is among their top three immediate priorities for physical security operations integration and cross-functional collaboration.

How will enterprises converge the two? Why is it important to do so now more than ever?
What risk do we run into by not breaking down the existing silos?

Physical and cyber security will continue to converge in 2022, especially in the case of handling troubling employee behavior. Those who work in the field of behavioral threat assessment already know that physical security and cybersecurity are often closely linked, especially when it comes to concerns about current and former employees. Employees who engage in troubling or odd cyber behavior may also be engaging in alarming in-person behavior in the office or on Zoom calls, etc. However, if physical security responsibilities and cyber security domains don't communicate with each other, they may miss opportunities to share information, 'connect the dots', and identify growing concerns.

Dr. Marisa Randazzo
Executive Director, Ontic Center of Excellence

While I don't anticipate that it will be a drastic or immediate shift, I think that in 2022, aside from the ongoing efforts to address the COVID-19 pandemic, the physical security industry will be marked by the continued evolution of the relationship between the physical security and cyber security spaces. The relationship between what we're seeing in the cyber realm and how that plays out in the physical world is likely to become increasingly intertwined. While cyber and physical security will likely remain distinct in how threats manifest and are countered, the flow between the two will grow increasingly complex. This evolution will necessitate a close alignment between physical and cyber security leadership.

Angela Lewis
Manager, Global Intelligence and Threat Analysis, The Walt Disney Company, Protective Intelligence Honors Thought Leader

For physical security in 2022, we will start to see more collaboration between cyber and physical attacks from threat actors. Stopping the attacks will not be enough, we will have to determine which attacks are random, internal and which are directed and where they are originating.

Chris Story
Senior Protective Operations Leader, Consultant and Specialist Trainer, Protective Intelligence Honors Thought Leader

An increased need for protective intelligence technology

Businesses are operating in a growing sphere of activity — expanding into new countries, markets, and onto the kitchen table (or home office). Manual methods of collecting data to determine patterns in activity leave teams struggling to prioritize, know what to act on and who to inform. The days of multiple, antiquated solutions are over. Technology fills this void by serving as an always-on engine, surfacing threat intel and streamlining day-to-day processes.

Now is the time for security teams to leverage one solution that allows users to see critical signals through the noise, bring together data, people and processes to verify and develop advanced understanding and context and ensure a coordinated response with connected workflows to activate operations and facilitate action.

What types of threats are emerging that signal a need for technology? Why is now the time that we need technology versus ten years ago? Why is one single solution the key to success?

Workplace violence and insider threats will be the greatest challenges facing corporate physical security teams in 2022. Investment in technology and scalable software will help security teams adapt to and prepare for these challenges. The 'single pane of glass' ability to have a converged view of threats from public and private risk signals, will have the biggest impact on corporate physical security in 2022.

Manish Mehta
Chief Product Officer, Ontic

The industries that will benefit most from the digital transformation of physical security in 2022 are those with multiple locations - including retail, manufacturing, energy, and distribution centers. Supply chain and critical infrastructure will continue to be disrupted by organic risk, and then further exploited by external threat actors. In times where physical and cyberinfrastructure is strained to the extent it currently is, both become even more vulnerable.

Tom Kopecky
Chief Strategy Officer, Ontic

COVID-19 brought us the single most rapid change to security operations since the 9/11 attacks. The shift from secured facilities to our staff working from remote locations made security teams globally rethink how we protect assets, data, and our staff. We can no longer simply watch cameras or monitor movement and must now focus on monitoring the movement of data and intellectual property digitally. Rethinking our insider threat programs will be key to helping ensure the safety of our property and staff members, and a heavier focus on evaluating our third-party vendor relationships will be critical.

Wayman Cummings
Vice President, Security Operations, Corporate Security & Infrastructure Office, Unisys,
Protective Intelligence Honors Thought Leader

Addressing hiring challenges when building a top tier corporate security team

Having skilled security professionals you trust is arguably the most important element of a successful security program. Technology is crucial, but it only gets you so far if there is not a qualified, driven team on the other end evaluating the data and executing the next step.

A global shortage of qualified and diverse security professionals is causing challenges when it comes to hiring. When you add this to the fact that those focused on security are overworked, and often undervalued in relation to the larger organizational structure, you create a recipe for disaster when it comes to the future of this industry.

How can enterprises begin to address hiring challenges and ensure they're recruiting the proper staff? Why has it been so challenging in recent years and will we start to see a shift?

Companies, NGOs, and other not-for-profits will likely be challenged to sustainably meet their brainpower supply chain requirements for protecting people, assets, and information. Competition for security personnel is heating up. Current assignment fatigue, COVID exhaustion, and the appeal of greener pastures appear to drive competent subject matter experts to consider their options. Analysts, cleared personnel and digital transformation technologists, in particular, are in high demand. Brands that require continuous protection improvement may prudently identify at-risk personnel for more engaged career planning, leadership development, and benchmarked remuneration.

Francis D'Addario
Emeritus Faculty Lead for Strategic Innovation, Security Executive Council (SEC),
Protective Intelligence Honors Thought Leader

There will be a variety of challenges that security teams will encounter in 2022. The one that leads the pack is going to be finding enough qualified people to fill all the positions that are opening up. This has been all over the news, but it's quite another thing to deal with it personally.

Ami Toben
Director of Consulting and Training, Highcom Security Services Inc., Protective Intelligence Honors Thought Leader

I see the challenge of getting folks to come out to work continuing. We need to think about how we're hiring, training and onboarding. Some of the technology like metal detectors, for example, creates incredible efficiencies with the labor force as it reduces the burden on the labor side and helps us be more efficient with what we have.

Mike Fogel
Director of Safety and Security with Austin FC and Q2 Stadium

Conclusion

Organizations have a lot to keep in mind in the coming years. Threats are only going to continue. Threat actors are only going to get smarter. We must continue to advance our approach to protective intelligence and ensure we come together as a community to share emerging trends and anticipate both the challenges and opportunities ahead so that we can all avoid those seemingly unpredictable moments.

Ontic's Protective Intelligence Platform enables enterprise security teams to see around corners and keep their businesses safe.

Learn More

Let's make nothing happen together™

Named the top industry innovator in the Frost Radar™: Digital Intelligence Solutions, 2021, Ontic is the first protective intelligence software company to transform how Fortune 500 and emerging enterprises address physical threat management to protect employees, customers and assets. Ontic's SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge so companies can assess and action more to maintain business continuity and reduce financial impact.

Ontic provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals through its Center for Protective Intelligence and Center of Excellence, the latter of which also offers program development and training services in behavioral threat assessment, threat management, and violence prevention for major corporations, educational institutions and government agencies.

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

ONTIC®