

CORPORATE SECURITY PREDICTIONS AND TRENDS 2021

By Pete O'Dell
CEO, Swan Island Networks



2021 is approaching rapidly, though 2020 seems to be lasting an eternity. Most organizations are planning for whatever new normal will emerge in the coming months and thinking about longer-term trends that will impact our people, markets, operations and economy for decades. Many are struggling, making hard choices to ensure day-to-day and month-to-month survival.

Multinational companies must juggle thousands of different situations and regulations across their various sub-jurisdictions around the planet, multiplying the complexity of their operations. Many more companies may operate in a limited area, but are dependent on supply chains that span the globe. The COVID-19 pandemic is a stubborn foe and has defied (so far) any kind of “silver bullet” such as the vaccine which finally brought polio under control in the 50s. It’s a challenging time for all of us.

The team at Swan Island Networks (swan-islandnetworks.com) has built a collection of trends and predictions that we think will impact your security world and overall organization in the next 18 months, directly and indirectly. Our company lives in this rapidly changing security ecosystem and we interact with a broad range of customers, partners, coopetitors and competitors, so our forecast includes many of these collaborations and discussions.

Our predictions are also informed by the conversations that occurred in a virtual executive roundtable I hosted for ten consecutive weeks as the COVID-19 virus spiked. Attendees highlighted significant problems that weren’t always obvious, such as elevator choke points for high rise, multi-tenant buildings. Everyone shared real-time insights, including input from one participant living through the stages of the virus – symptoms, testing, contact tracing challenges and recovery.

Change continues to be a constant, and new developments are happening at a stunning pace, so I’m sure we’ll find we missed the mark on some predictions and were eerily right on others.

We welcome your feedback. Send us comments, augmentations, praise, quibbles and pans and we’ll republish this paper with the best input we receive from others in 45 days, and again at the start of 2021. We’ve found non-proprietary information sharing to be a force multiplier, harnessing the wisdom of the crowds and saving immense amounts of time for all involved. Email Info@swanisland.net or tweet us at [@SwanIslandNet](https://twitter.com/SwanIslandNet) or comment on this article on LinkedIn. Tell us if you prefer to be anonymous or you’re willing to be quoted, we’re good either way. So here goes...

“It is the long history of human-kind (and animal kind, too) that those who learned to collaborate and improvise most effectively have prevailed.”

- Charles Darwin*

*(The University of Cambridge’s Darwin Correspondence Project tells us Darwin didn’t say this, but he should have!)

1. Uncertainty & speed of change

The world has been accelerating in many areas for decades, and we know this rapid pace is going to continue. Our prediction centers around how organizations will reframe how they manage change. We anticipate most companies will spend more resources monitoring emerging events in order to prevent or mitigate damages – and examining secondary and tertiary areas of impact due to the rising complexity they are encountering. The pandemic has sharpened everyone’s sense of awareness, and most companies have experienced events that might have been foreseen, prevented or at least mitigated if someone had been paying closer and more proactive attention. Never have the phrases “pay me now or pay me later” and “if you snooze, you lose” had as much impact. The roller coaster is going faster, buckle up.

2. Uneven pandemic and economic recovery

The economic recovery is seesawing almost everywhere, forcing many organizations and communities to open, close, move a phase back, open schools, and in some cases immediately reclose them. Spain has reverted to a severe infection state, so worldwide diligence clearly must be a sustained 24x7 effort until vaccines show up and impact the majority of global populations. This uncertainty will ripple through companies and impact their staffing and security postures. It’s hard to define a trend here, but we have seen flexibility, innovation and rapid adoption of new methods by the firms handling this the most effectively. We predict the sense of urgency gained will continue and be a benefit to future days.

3. Civil unrest & crime

Worldwide, the number of unemployed people has skyrocketed. The pandemic is accelerating income inequality issues as people with few resources to begin with have to spend what little they have on keeping the lights on, food on the table or look to stressed community programs for help. Rising levels of desperation, frustration and anger drive antisocial behaviors and domestic violence. Legitimate protests against racial injustice are increasingly being marred by opportunistic violence and looting. We’ve already seen spikes of shootings and murders in several major US cities. We’re predicting an unpredictable global situation where careful monitoring and early reactions will help mitigate damages for organizations and communities.

4. Threat awareness

Companies that were prepared and ready for the pandemic should take a bow (with their mask on), because most organizations got a big collection of surprises and negative impacts. We work with several companies who were aware of the virus early on, modified an already existing pandemic plan, augmented PPE on hand, and reaped the benefits. Our prediction is that many more companies will adopt 24x7 all-hazards threat monitoring as a “must have” corporate function, and devote more dollars to contingency planning and capability. We also predict, as with cyber-security, the board and C-Suite will take a more engaged role in managing and directing this effort.

5. Outbreaks – virus recurrence

Security personnel are essential personnel, and vulnerable to exposure despite good training and guidance by the security firms. We predict a major trend will be workforce uncertainty and contingency planning for personnel and systems impacted by a sudden recurrence of the virus. We also predict that testing and screening will become more precise and have nearly instant results, allowing companies to pinpoint problems earlier and adjust responses closer to real time.

6. Commercial real estate in flux

Few prognosticators are willing to predict the state of commercial real estate for the next five years. One can make the case that people will continue to work from home, or that emerging satellite-based high-speed Internet connections will allow a permanent exodus from major metropolitan areas – if you can connect, can you really work anywhere? None of this is proven or certain; the outcomes will have impacts that could affect every aspect of future security efforts.

We predict a mixed environment going forward because critical talent will be able to dictate their preferences in many cases, making a uniform or dictatorial approach by management difficult. The digital collaboration environment is here to stay. Companies should prepare to incorporate home addresses into threat monitoring to manage the distributed cybersecurity danger.

7. Silo merging - budgets

For some companies, 2021 will demand some very harsh changes in personnel and spending to support the survival of the organization. For essential services like security, the answer will be doing more with less, driving our prediction that companies will assess the cost/value relationship of the tools they are using, evaluating competitive solutions that either cost less, offer more value, or provide more flexibility.

8. Silo merging – effectiveness

We've seen a trend toward merging ERM, business continuity, and physical and cyber security into a unified risk/security structure that gains some economies of scale and centralizes responsibility for the C-suite and board of directors. Too many companies have been disappointed or blindsided by the lack of cohesiveness between the strategic, operational and tactical functions responsible for protecting the corporation.

9. Cybersecurity

Cyber is going to continue as a top threat for corporations, complicated by work-at-home flexibility. We're predicting a couple of major breaches where CISOs didn't segregate work computing from family computing, and home users' access from the corporate crown jewels. Hackers will either lock down sites (ransomware) or steal very valuable intellectual property.

10. LEO satellite-enabled security

Getting the bandwidth for monitoring far-flung pipelines, property, and assets has been a challenge – even many in the US and other developed countries are bandwidth-challenged in rural areas. The LEO satellite constellations by SpaceX and Amazon’s Kupier project promise to deliver 4G+ speed bandwidth to every inch of the planet. Besides enabling very remote work from home locations, we predict a surge in security sensors of great variety that can relay geospatial-enabled alerts to government and industry very quickly, broadening the proactive lens aperture. We also predict continued poorly coordinated sharing of this information, blunting its effectiveness (as with the 6,000+ different jurisdictions for 911 alerts).

11. Automation & systems investment

New technologies are continuing to emerge, and we predict a major funding uptick by the investment community (venture capital, private equity) in preventive and response capability solutions. You saw the almost-immediate repurposing of infrared sensing technologies to monitor for temperature screening and similar reapplications with video recognition systems. One robot technology could flash a warning to non-masked entrants using object recognition capabilities. Technology continues its relentless decrease in price and increase in capabilities!

12. Artificial intelligence

If you look at the literature and ads, you’d think everything in the security world is AI-powered; that machine learning is the norm for all corporations; and predictive intelligence is already globally deployed. While the trends are definitely heading these directions, we predict that it will take time before these are all standard issue. We also predict that long-term solutions will be built on AI Service Stacks from the major cloud providers, like Microsoft (Azure), Amazon (AWS) and Google (Cloud), much as high-level language compilers enabled a huge increase in software application development.

13. Intelligent video

Cameras and video management are great, but require a human actively watching (one of the most boring jobs on Planet Earth), or they’re relegated to a forensic tool after incidents happen through a query of the Video Management System. A rapidly emerging set of intelligent video solutions will change the face of video surveillance (pun intended) by recognizing license plates, people, weapons, threatening interactions and much more. These systems can trigger structured alerts to a central situational awareness capability, allowing immediate and more proactive response by the security function.

14. Drones & robots

We predict another watershed moment in security alerting as drones and robots decrease in price, increase in capability, and combine with other emerging technologies such as connectivity, sensors and intelligent video. There may well be new collaborations between government, organizations, and watchdog organizations to enable privacy protection where possible. Note: Those drones and robots could become very invasive, especially as they shrink in size.

15. Supply Chain

Many organizations were caught short when the worldwide lockdowns went into effect, losing vital suppliers and experiencing major delays on essential products like masks and disinfectant wipes. We're predicting enhanced monitoring and situational awareness of vital supply chain elements, including financial health of suppliers, and parallel disruptions such as extreme weather incidents. We also see multi-continent sourcing redundancy, as the worldwide recession drags on toward a recovery.

16. 24x7 Operations Center creation and expansion

We're seeing many more companies create a 24x7 monitoring and command center environment, and predict this will continue, particularly where a company's assets and key relationships span the globe. The role of several of the security departments we work with has been broadening to incorporate additional 24x7 services; brand monitoring on social media is one example. The Security Operations Center could become the Services Operations Center as the need for rapid reaction and continual response increases.

17. Security vendors consolidation

We've seen multiple acquisitions (WorldAware, Stabilitas, Phoenix Systems) in just the last six months. It's easy to predict that this will accelerate as more companies move toward broader, more integrated security solutions. Everbridge, the market leader, has an impressive market capitalization that has increased sharply, but that's also made them a target to established competitors and disruptive startups.

18. Integrated security providers

Companies like Allied Universal have greatly augmented their manned security business with technology and high value risk/consulting services. This trend is likely to increase in the coming years as the complexity of blending many different vendors and contracts intensifies; we've had multiple companies express a desire for a single point of accountability who can manage and optimize the increasing number of equipment, data feeds and integration efforts.

19. Innovation

We're predicting more, an easy extrapolation based on the last 25 years and Moore's law. It's more exciting (and harder) to predict the combinant solutions that meld multiple emerging technologies and disrupt an industry with a new integrated solution. Uber is a great example. Building an efficient ride-sharing system pre-smartphone, pre-mobile payments and other technologies would have been very difficult 15 years ago. Iridium (satellite communications) and WebVan (online grocery) are examples of good ideas that launched too early, before the needed supportive technological infrastructure had been developed. We predict that intelligent video, AI, sensors, and mobility (drones and robots) will be combined into multiple disruptive capabilities in the next 36 months. Several futurists are on record that we'll have more change in the next 20 years than we've had in the last 100 years. The security function we see today will look quite different in five years. Make it happen, watch it happen, or end up wondering "what just happened?"

20. Interoperable data

Proprietary lock-in by vendors will be eroded by customers insisting on plug-and-play interfaces between systems. Google enabled great GIS interoperability with its global donation of KML. The Common Alerting Protocol (CAP) was developed by a consortium of emergency managers, guided by OASIS (itself a nonprofit consortium), to work across disparate systems and is freely available for use. We predict a greater use of interoperable data for device-enabled alerts and an increasing awareness by security strategists of the power of interoperability.

21. Surge services

Keeping extra headcount around for a high-impact, low-probability incident response team is going to be a tough sell to the C-suite, especially as budgets tighten. We see a continued trend toward contingency services – GSOC as a Service (GaaS), Analysts as a Service (AaaS), Intelligence as a Service (IaaS) as a means to ramp efforts in an emergency but keep fixed spending at a known level.

22. Information sharing

Due to the pandemic limiting water-cooler interaction and ad hoc meetings, companies have had to share more information electronically, and have reaped the benefits of digital, time-shifted communication. Cross-organizational information sharing has increased and we predict that the speed and cost burdens of staying current on a solo basis will encourage more information sharing alliances for non-proprietary data.

We hope you found these predictions provocative and interesting. As previously mentioned, we welcome your feedback. Send us comments, augmentations, praise, quibbles and pans and we'll republish this paper with the best input we receive in 45 days, and again at the start of 2021.

Email Info@swanisland.net or tweet us at [@SwanIslandNet](https://twitter.com/SwanIslandNet) or comment on this article on LinkedIn. Tell us if you prefer to be anonymous or you're willing to be quoted, we're good either way. Thanks for taking the time to review our predictions.

About the Author:

Pete O'Dell is the Chief Executive Officer of Swan Island Networks. Before joining Swan Island, he served as the Chief Operating Officer for a number of high growth start-ups and was president of Autodesk Retail Products. He is the author of Silver Bullets (interoperable data) and Cyber 24/7: Risks, Leadership, Sharing. His new book, Global Shared Resilience, is slated for publication in Q1 of 2021. He is an avid fly fisherman and volunteers with www.fishingcommunity.org, a nonprofit focused on veterans and their families.

About the Company:

Swan Island Networks is an Oregon-based SaaS company. Its TX360 Enterprise Situational Awareness platform and TX Global Alert Subscription service are comprehensive, affordable, easy to deploy and use, and continually adding capabilities and intelligence sources. Visit swanislandnetworks.com or our LinkedIn and Twitter pages to learn more.

References

- Alexander, A., De Smet, A., & Weiss, L. (2020, March 24). Decision making in uncertain times. McKinsey&Company. <https://www.mckinsey.com/business-functions/organization/our-insights/decision-making-in-uncertain-times>.
- Kiger, Patrick J. (n.d.). 10 of the World's Most Groundbreaking Futurists. Howstuffworks. <https://electronics.howstuffworks.com/future-tech/10-groundbreaking-futurists.htm#pt10>.
- Dua, A., Mahajan, D., Oyer, L., & Ramaswamy, S. (2020, July 7). US small-business recovery after the COVID-19 crisis. McKinsey&Company. <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/us-small-business-recovery-after-the-covid-19-crisis>.
- Day One Staff. (2020, July 30). Amazon receives FCC approval for Project Kuiper satellite constellation. Dayone. <https://blog.aboutamazon.com/company-news/amazon-receives-fcc-approval-for-project-kuiper-satellite-constellation>.
- Mysore, M. & Usher, O. (2020, March 16). Responding to coronavirus: The minimum viable nerve center. McKinsey&Company. <https://www.mckinsey.com/business-functions/risk/our-insights/responding-to-coronavirus-the-minimum-viable-nerve-center>.