Beyond a Cataclysmic 2020:
Security's New Opportunities to Address Workforce and Workplace Risk

By Michael Gips

White Paper

THOMSON REUTERS®

This white paper explores the opportunities for the security profession to move forward as the world crawls out of the wreckage of 2020.

COVID-19. Historic unemployment. Industries devastated. Civil unrest. All marked the surreal year 2020, and all presented enormous challenges to the security profession. These things will pass or evolve, as every crisis does, as we move into 2021 and beyond.

But what does the cataclysmic 2020 mean for the security profession?

Security, operating without a script, responded to trying times with agility, courage, and grit. The profession now has a unique opportunity to write its own story, to help define a workplace and workforce undergoing a massive shift. Will security executives leverage the lessons of 2020 to position themselves as key corporate risk executives with business savvy who merit access to key decision-makers? Or will security revert to being considered a drag on business, a subset of crisis management or facilities, a damper on innovation?

This white paper describes how security professionals have responded to 2020's challenges, including both assuming new duties and forsaking others. It then explores the opportunities for the security profession to move forward as the world crawls out of the wreckage of 2020.

The current environment

In an article published by Thomson Reuters Legal Executive Institute in August 2020, we wrote:

> Leaders are forged in times of crisis. So, it's not surprising that a rare confluence of events that includes the current pandemic and recent social unrest has given organizations' Chief Security Officers (CSOs) and security executives an opportunity to exercise even greater leadership and mission-critical influence during these historically trying times.
>
> The economic fallout of the global pandemic, as well as the seismic rifts widening in our civil and political discourse, highlights the increasing importance of the security department. This period of heightened tension calls upon security professionals' skills to deescalate tensions and exhibit empathy but also to protect staff, supply chains, and information.

The opportunity

The article recognized that the current crisis had opened the door for CSOs to become direct advisors to corporate executives or senior government officials. Security leaders have been thrust into the center of all-hazards corporate risk management, business resilience and continuity, and crisis and emergency response plans. Businesses today face new existential threats, giving security a chance to show its importance.

Security has been grappling with many new and exacerbating issues involving human resources alone. First, industries such as logistics, health care, and big-box retail have undergone a burst of hiring and onboarding — while abbreviating background screening. Travel, entertainment, and lodging providers have slashed payroll, triggering possible violence or sabotage. Aggrieved or financially threatened workers pose increased insider threat risks. Forsaking full-time hires, businesses have turned to contractors and gig workers, who owe them no allegiance. And the vast majority of office workers have been working at home for the better part of a year, raising a raft of new issues.

The rapid transition to work-from-home has accelerated digital transformation. Today's CSOs must keep pace with investments in work-from-home infrastructure. Tony Howlett, CISO at SecureLink of Austin, Texas, points out that security is faced with quickly helping companies deal with unexpected developments, including scaling work from home technologies to handle near 100% participation.

Other issues are even more grave. The world is experiencing more frequent disruptions to business continuity due to hurricanes, wildfires, floods, and other natural disasters. Extremists and conspiracy groups such as QAnon and the Boogaloo Boys are burgeoning and becoming emboldened. And the resurgent focus on civil liberties, fair employment practices, and corporate social responsibility is forcing many businesses to proclaim stances on social issues publicly.

No less critical is how security is dealing with changes in business strategy and the increasing importance of demonstrating business value.

COVID has created an all-encompassing need for security services and strategies to protect the workforce and prepare return to work strategies.

Security's response and the effect on the security function

How security is responding to these challenges comes from three sources: A July 28, 2020 webinar entitled "Security and the 'New Abnormal': Managing Risk in Uncertain Times," featuring four security executives; interviews with several other security executives; and a survey of 121 security executives conducted by Thomson Reuters in late August 2020.

New day-to-day duties

Dave Aflalo, SVP, Global Security & Facilities, at GM Financial, says the pandemic has profoundly affected security's duties, and the numbers bear him out. "There's no question in my mind that the vast majority of CSOs have had their portfolio of responsibilities increase as a result of COVID and helping to shape the business response strategy," he says.

Indeed, the survey results show security adding a range of duties, mostly due to the pandemic. The most common new responsibilities include travel safety/risk management, reengineering facilities, and enforcing social distancing and occupancy limits. These are followed closely by health checks and temperature screening. As one respondent puts it, "COVID has created an all-encompassing need for all of these services and strategies to protect the workforce and prepare return to work strategies."

The CSO of a metals company based in the United Arab Emirates elaborates. His department assists with temperature checks and social distancing, with the assistance of video feeds and officer patrols. "We have a patrolling checklist that includes checking on washing, sanitization, and mask compliance," he says. That includes access to where patrols had not gone before: the restrooms.

Increased authority and influence: Never waste a good crisis

Three-quarters of survey respondents say leadership views security more favorably since the pandemic. Specifically, 30% say that security has gained significant authority, responsibility, and/or voice, and 33% say security has gained some authority, responsibility, and/or voice. A mere 3% have seen a decline. One respondent adds that security gained responsibility but not authority.

And that heightened awareness flows through the organization. Thirty-eight percent of respondents say that many more staff understand that security is increasingly nuanced in today's complex world. A further 26% say that slightly more staff better understand security's role. Almost all the rest (30%) cite no change.

Several CSOs say that their responsibilities and authority have increased because of their sangfroid during crises. "One of the reasons security has stepped into the COVID role more effectively than other groups is that corporate security has a crisis management element to it," says Chris Gallo, global corporate security manager at Houston-based Parker Drilling Company. "You're always in the shadows managing crises. You can use that reservoir of knowledge to advise people in other departments." And that knowledge starts with understanding how the business operates both during normal times and in a crisis.

Gallo laid the foundation for security to step into a larger role well before the pandemic. He recalls that a contracts manager who sat in a nearby office told him that he forgot he was in security because Gallo had such an intricate knowledge of all the organization's processes. "You can't do your job effectively if you don't understand all your organization's operations," he says. "That really set the table for security to take this role. No one else really knew the operation and the likely impacts of COVID."

Most forward-leaning CSOs built relationships within their company, both within the C Suite and outside of it, well before the crisis occurred," agrees Aflalo. "I've always believed that the value proposition of the CSO may well be highlighted during a crisis," he continues. "But, ideally, it should not be established during one."

Today's strife "places security leaders in a position to lead through a crisis," adds Aflalo. He cites not only knowledge of organizational operations, but experience with and reputation for collaboration and information sharing across business units and with security departments in other organizations across industries.

The CSO from the metals company says that today's environment has shown business leaders that security is about more than protecting assets. It includes business assurance, protecting brand and reputation, and supporting a health and safety culture. "It has enhanced security's role and respect in the boardroom," he says.

He now gets invited to executive committee meetings. Based on his early briefings on what security learned and how it adapted to managing the crisis, "They started to invite our team and appreciated what we were doing on the ground," the CSO says. "Now, for major issues, they ask, 'What do you think about that?' Security might become a permanent presence."

"Security personnel must recognize potential stressors in their workforce … employees need to hear that they are respected and supported."

Navigating the new blended office

Scott Bethel, CEO of Integrity ISR and a former U.S. Air Force Vice Commander, says the work-life "balance" discussion is giving way to the need for harmony: "Work for a little while, do something with the kids for a little while, do a little project in the house. That's what people are doing," he says. Add dogs barking during Zoom calls and families sharing the same devices, and it opens up new attack vectors. But an upside is that less commuting means additional productive hours.

In addition, security departments are deciding whether to visit staff homes and fit them with security methodologies or else run all activity through a single server. Then they are establishing policies on which devices can interact with company computers.

The new work environment is also reshaping employers' duty of care. "Employees' homes are becoming a legitimate workplace, especially with companies providing furnishings to facilitate remote work," says Aflalo. As domestic violence increases during the pandemic, questions arise about whether companies owe the victims a duty of care.

Forging and strengthening partnerships

One of the upsides is increased cooperation with IT security. Many physical and cybersecurity leaders note closer relationships, somewhat attributable to an all-hands-on-deck mentality.

But the partnerships go well beyond IT security. "We're seeing multi-disciplined, COVID task forces, the formation of core response teams working in concert to develop holistic strategies around COVID-related risks to the business," observes Aflalo. These teams include health and safety, facilities, and HR, among others.

Stress management

This new state of affairs, as well as the prospect of returning to an office that will look radically different, has disrupted normal patterns and intimidated staff, notes Robin DeProspero Philpot, former CSO of the U.S. Secret Service: "Security personnel must recognize potential stressors in their workforce," she says. "They must also recognize that during some sort of a crisis, employees need to hear that they are respected and supported. If not, you are going to have a workforce with extremely low morale, low productivity, higher attrition, and more employee issues."

Addressing that issue requires training for security and HR staff. DeProspero Philpot also recommends encouraging managers to have one on meetings with their personnel. "That way, you can really observe an employee. Ask them to come in one day a month, or every two months, or at least every quarter," she says.

The CSO of the metals company adds that security officers may feel particularly stressed since they interface with staff and visitors and fear catching the Coronavirus. "We need to listen to guards, and help them maintain their well-being," he says. "We need to be more emotionally connected to the team on the ground," he urges. "Technology is emotionless and faceless. We have to stay connected to people in a high-touch way."

Scammers are exploiting any emotionally charged issue.

New threat vectors

Aflalo points to a surge in "cyber scams, business email fraud schemes, and phishing efforts across a broader and expanding attack surface," especially due to COVID. One large company alone lost $37 million in an email fraud scheme. In addition, counterfeiters are thriving on the scarcity of products by producing and selling inadequate and fraudulent masks, ventilators, disinfectants, and COVID testing kits. This is not only an economic problem but a serious health concern.

But scammers are exploiting any emotionally charged issue. Emails purporting to provide information about Black Lives Matter, for example, are distributing malware to anyone who falls for the bait. Political fundraising scams are exploiting citizens who react reflexively and will let their guard down.

Filling the law enforcement void?

U.S. cities have already begun reducing police budgets due to protests over police abuses. Private security will be called upon to pick up the slack. DeProspero Philpot notes that laid-off police officers may gravitate to private security, which is a double-edged sword. On the positive side, they bring training, experience, and professionalism. On the other hand, they won't be able to operate under the authority of law, she says. Forgetting that even for a moment could generate enormous liability. "The bottom line is," according to DeProspero Philpot, "does your organization have the staff and budget to be your own police force?"

Whither non-COVID duties?

With all hands addressing the multipronged crisis, companies have diverted resources that ordinarily go to day-to-day projects such as system maintenance and upgrades. In fact, survey respondents note a wide array of affected initiatives. Taking the hit most directly are site/risk/threat assessments, staff training, equipment maintenance and upgrades, and policy and procedures reviews. Multiple respondents point out that travel risk management duties have ebbed as business travel has shriveled.

Gallo, of Parker Drilling, says that his department has slowed its pace on audits and risk assessments. "But that's appropriate in a crisis," he qualifies. The catchup period will be immense, though, with security likely triaging issues as they arise." That's more difficult due to the current dynamic and unpredictable period of risk, with escalated geopolitical tensions, civil unrest, racial tensions, natural disasters, and climate and sustainability exigencies.

At the Emirati metals company, the CSO says that COVID shut down new projects, such as CCTV upgrades. "We can't afford to use our own manpower, and if we bring in people from outside, there's a risk that they will be infected," he says.

Tony Howlett, CISO at SecureLink, says he is still doing the "basic blocking and tackling of infosec." But larger projects and nonessential spending have been reduced or eliminated, even though the company's bottom line, and the industry as a whole, is healthy.

Security professionals will continue to play a more prominent role in workforce and workplace risk.

Another CSO has even split his staff so that non-COVID essentials get done. A special team is tasked with doing everything except COVID-related duties.

Future prospects

By self-attestation, at least, security has risen to the fore. But what happens when the lights come on, and the crisis is over? Is it back to business as usual — with most security departments excused from the table?

Survey respondents were asked whether they expect to retain or relinquish the duties they gained during the last several months. Almost half (45%) expect to keep them, and 35% are unsure. Only 10% plan to relinquish them, though one respondent urgently wants to "stop writing pandemic response plans."

Asked what percentage budget increase would enable them to take on these additional duties adequately in future years, most predict it wouldn't take much: 38% say a 0-5% increase, and 26% say a 5-10% increase. Four percent say a prodigious 50% increase or more.

CISO Howlett is hopeful that newfound prominence will stick. "Some permanent change and good will come from this," he says. It will lead to the "final dissolution of traditional perimeters based on physical locations and specific infrastructure and lead to wider adoption of technologies like zero trust," he says. Howlett adds that just as Hurricane Katrina spurred companies to invest in long-term power backups and 9/11 did the same for hot sites, COVID will lead to more funding and better technology.

The metals CSO says that CSOs can cement their elevated status by identifying future crises before they severely affect their employers. "It behooves the executive team to keep security in the loop," he says because incidents constantly occur that can affect brand. "A small crisis may harm you more than COVID," he says. He would position security in this role to the executive suite and provide metrics on how security assisted.

And that's a good beginning to a new playbook in which security professionals will continue to play a more prominent role in workforce and workplace risk.

This white paper is the culmination of several weeks of discussion and research that began with Thomson Reuters Legal Executive Institute publishing an article called "The Rising Profile of the Corporate Security Executive." A webinar, "Security and the 'New Abnormal': Managing Risk in Uncertain Times," picked up and elaborated on the themes of that article. Concepts and discussion points fleshed out in the webinar led to interviews with select security executives and a benchmarking survey of 121 corporate security leaders. This white paper pulls all those threads together.

About the author

Michael Gips, named one of security's most influential people in 2019, writes about the latest trends and news in corporate security, cyber-security, technology, and crime.

Thomson Reuters

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting, and compliance professionals combined with the world's most global news service — Reuters.

For more information on Thomson Reuters, visit tr.com and for the latest world news, reuters.com.

Contact us today

+1 888 728 7677

TR.com/CLEAR

THOMSON REUTERS®