Global Health Security Alliance

GloHSA

3|2020

CORPORATE SECURITY POST COVID-19

Lana Djurkin-Koenig

GloHSA Brief June 2020

Global Health Security Alliance (GloHSA) I ISSN 2627-1397

www.glohsa.com

Corporate Security Post COVID-19

The future is not what it used to be. The dire threat posed by COVID-19 is unprecedented. Also, this is not a one-off event. There will be further waves of this pandemic, moreover after this one is before the next one due to climate change and other contributing factors.

While the global economic outlook is difficult to quantify at this stage of the pandemic, current projections remain not good. Improving economic forecasts depends on a comprehensive response to the pandemic - government, society, and business. Corporate security is undoubtedly at the forefront of, at least in the business world.

What those developments mean for the security profession post-COVID-19 depends on what is the next and the new normal in the world, how the workspace of the future is going to look, and whom the future employees are going to look like be(come). This situation has a profound impact on the corporate security profession as it will need to re-imagine itself and how the work is done – the change is and will become omnipresent.

New work has come with an unprecedented speed

While at the moment, the focus remains on safely returning to work, societies are generally showing a sharp divide between those who want safeguards to remain in place and those who want "normal" life to resume. Trying to go back to the "normal" life is something that everyone would like to do, except that the old "normal" is gone. At least for now. For now, we all need to learn to operate in the new "normal", full of fears of re-infection in society and the office. According to the Harvard Business Review, the most effective (albeit most expensive) control against the virus threat is work from home (WFH) policies. Many companies have quickly introduced the WFH approach as an emergency measure and have adapted to new working models showing extreme resilience. Twitter's announcement of a shift towards WFH policies as a lasting norm – albeit with offices open for those who need them – reinforces the trend of companies, particularly in the tech sector, to improve labor conditions and save costs by reducing

Lana Djurkin – Koenig

GloHSA Associate Lana Djurkin-Koenig is a security professional with more than 16 years of experience in national, international and corporate security. In her current role she leads the internal and corporate security and business resilience function of EY GSA, one of the largest regions in EY globally.

Before that, she was the coordinator of the Global Security Situation Center for the Deutsche Post DHL Group´s Corporate Security, where she focused on comprehensive security intelligence analysis to support relevant decision makers at the strategic level in managing their security risks and challenges. Before joining DPDHL, Lana worked internationally in several positions in the field of security and was awarded a NATO Medal while working for ISAF in Afghanistan.

To cite this article: Djurkin-Koenig, Lana. “Corporate Security Post COVID-19”. GloHSA Brief no. 3(2020); https://glohsa.com/.

substantial real estate overhead.[1] Also, Google, Facebook, Amazon, Capital One, and others are extending work-from-home policies to the end of 2020 and sometimes beyond. Those moves reflect the reality that no one is sure how COVID-19 will evolve.

Even after the coronavirus no longer requires it, WFH is likely to remain a significant presence in corporate life. It will have a broader societal impact and reshape cities and the commercial real estate industry and change the culture at companies that have been building elaborate temples for their workers for years.[2]

How does it impact corporate security?

From a security standpoint, remote work presents a more significant concern, especially information security issues. Offices are, and many of them will stay empty for a while. Businesses are under pressure, and employees are adapting to the new mode of working. How does it enable scaling up to ensure the same level of securing remote workers that are here to stay for some time? Corporate security is coming out as a crisis leader and resilience enabler at the heart of this complex and fast-changing world. However, it needs to make sure that they are enablers and not blockers of the change here to stay.

Trends that picture next and beyond COVID-19 phases

No one has a crystal ball, but there are a couple of trends that are possible to foresee. Companies are asking: How to keep employees safe? If employees feel that their company and its leaders care about their security at work and home, they will be more likely to trust the company's decisions.[3] Corporate security becomes a significant trust enabler. It also has a fundamental chance to contribute to the long-term value preservation, through the human-centric approach of doing business.

Security and safety have become sort of a "corporate benefits offering". It will no longer be taken for granted but will become proactively asked from the side of employees, clients, public and other stakeholders, and who fails on security and safety will lose - trust. Trust and its preservation are the key differentiators between corporations in the age of digital transformation and post COVID-19 world. Having re-surfacing infections on premises and among the workforce will become the brand and trust issue.

Following this argument, we can conclude that corporate security has a historical chance to claim the big table's seat as a strategic enabler of the business. This

[1] Obtained from: https://www.forbes.com/sites/andrewsolender/2020/05/07/trump-campaign-to-run-massive-negative-ad-blitz/#66a2617d99d2 and from: https://www.nytimes.com/2020/05/08/technology/coronavirus-work-from-home.html?smid=li-share.

[2] Obtained from: https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2020/Resetting-the-Business-After-the-COVID-19-Pandemic/?MessageRunDetailID=1784418018&PostID=14683152&utm_medium=email&utm_source=rasa_io.

[3] Obtained from: https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2020/ESRM-and-the-COVID-19-Pandemic/.

To cite this article: Djurkin-Koenig, Lana. “Corporate Security Post COVID-19”. GloHSA Brief no. 3(2020); https://glohsa.com/.

assumption is also visible observing a couple of trends that will paint the next and beyond COVID-19 phases.

1. Preparation for the next outbreak

After the pandemic, is before the new pandemic. Corporate security departments will, for an unknown period, have the responsibility to scale up company resilience, preparedness and monitor new outbreaks on the premises, manage and support national and international travel restrictions within the traveling population and become guardians of remote working populations' Duty of Care and security.

2. Higher degrees of remote and flexible work

One positive outcome from forced remote working has been conclusive evidence that flexibility needs not to come at the expense of productivity. Remote working will become a norm, especially among the workforce who has proven that this concept works for their effectiveness and potentially have specific private issues like health or family-related, which might hamper them to go into the office environment actively and public transportation risking un-necessary virus exposure.

3. Workforce expectation and behavior shifts

These behavior shifts do not mean that tomorrow those employees will be sitting in the home office, but rather using flexibility to work from everywhere, whether this is their home, park, coffee bar, or the beach. Nevertheless, security, health, and safety will still stay the company's and people's top priority and will heavily influence expectations of Duty of Care. If companies were until now providing security at the office premises, how do they continue exercising this same Duty of Care towards their employees that are somewhere? Where are they? Do they need to know this, to be able to protect them, and if yes, how to do this in GDPR compliant way? What do they expect from the company, and how can companies instill security DNA in them to make them the strongest and not the weakest link in companies' perimeters, that vanished from the offices and became liquid?

4. Workspace change

COVID-19 will have implications on the real-estate strategy. Many companies will understand that they don't need to occupy so much of the office space and will start to cut down office presence. The office of the future will become the touchpoint, meeting place, and an open office environment. In the context of the post-COVID-19 working environment, flexibility is becoming the norm, with remote work emerging as crucial components.

5. Investment in digital security

New Duty of Care expectations means stepping away from reactive into the proactive mode of exercising it, which calls for the real-time security support that is intelligence-driven. Employees that are in the know of what is happening around them in real-time and corporate security that is easily approachable to support them when they indeed find themselves in an incident will become the new norm.

6. Change in the way of leading and co-operation

Corporate security needs to adapt to the radical shift from the 'command and control' (C2) approach prevalent in the industry to a style of working that empowers people to make decisions, and this may be one of the most significant challenges. It goes against the traditional C2 culture and the sentiment that everyone should operate in need to know the way. Empowering teams to make decisions will lead to greater agility and innovation.

Post COVID-19 security: what to do next?

"Stay alert and re-think what profound impact this pandemic had on your company and you as well." Staying alert means continuing to understand how is COVID-19 developing and the mitigation measures we have put in place working. The focus needs to be on collecting internal and external information and analyzing them to gain insights and understand patterns and trends to forecast impact on our operations.

Next steps that should be done right now:

Step 1. Develop a *security mindful* corporate culture

Developing a security mindful corporate security is based on two hypotheses:

- The workspace of the future is mobile and empowered, and flexible employees drive it.
- Empty offices and remote workers present higher security risks.

Every company that wants to go remote needs to develop and ingrain the company's security DNA with a top-down approach and this needs to be done together with installing great physical security and cyber hygiene as well. Every employee should become mindful of security and their actions. However, this DNA needs to be in line with the corporate culture. It should feel infused in culture and not go against it as it will feel too aggressive and will not be supported.

Step 2. Break the silos

The second thing that is certain is that silos need to be broken as the world out there is filled with hybrid threats meaning that defense needs to be holistic. What is next in security is a one-security-approach. Barriers between InfoSec, data privacy and protection, and physical security need to be broken. Silos need to disappear. Specific education and awareness training, threat and risk monitoring, and policy requirements need to be done holistically in preferably Remote Working Security Hub approach. This approach covers all security aspects for employees and data protection once they step out of office space.

Step 3. Develop an integrated approach to assets' protection through real-time support via SOC

A third aspect is the assets' protection. Here is the baseline thought: in an open office space and remote concept, employees carry company assets with them all the time in their daily life. Assets will get lost or stolen in a higher amount than before, simply because of more opportunities for incidents.

So regulation and communication on how to behave once someone steps out of the office (where ever it is) with these assets will be helpful. Together with real-time security support where incidents can be reported, if for nothing but then because

To cite this article: Djurkin-Koenig, Lana. “Corporate Security Post COVID-19”. GloHSA Brief no. 3(2020); https://glohsa.com/.

the company might lose those 72 hours quickly to report GDPR breach if the information is lost on Friday evening and waits Monday morning to be reported.

Step 4. Develop a holistic data protection plan

When we talk about information stored on assets or hardware, we should not forget that data sitting there – comes in other dimensions as well and not only digital form. It is still stored physically in printed documents or can be transmitted mouth to mouth. These data protection dimensions need to be covered as well with remote workers. How many times employees printed out a document and took it home with themselves and then just threw it in the garbage? Remote workers need education about other aspects of security around the storage of physical data, such as the proper way to destroy any printed material or use portable storage to ensure the threat of any data breach is minimized. In the age where data is the new oil, the value of "garbage intelligence" or dumpster diving should not be under-estimated. If there is not enough security hygiene implemented through awareness and education, it would be straightforward for organized criminals and social engineers to understand where executives are living, judging by their selfies from their home offices and conduct espionage attacks.

Step 5. Redesign physical security and safety of the offices

A new real-estate strategy will come. Corporate security needs to claim the seat at that table to help redesign office space into a safe working environment that includes lessons learned from COVID-19 recovery phase. A good idea would be to introduce security risk assessments of individual locations as an intelligence-led approach, through definitions of phrasal restrictions implementation in the working space in case of a new pandemics or rebound of this one. This methodology can be based on red-flag warning indicators that are characteristic for each phase of pandemic and are combined with introducing timely and scalable restrictions into the workforce and office space usage, to prevent infections and re-infections.

Step 6. Insider threat programs are a must

The potential for insider threat attacks has grown significantly during the pandemic. Therefore, an insider threat program becomes a must. The impact of culture change will be profound in the human enterprise. There are aspects of culture change from on-site to remote that lead to:

- Loss of social cohesion
- Loyalty decrease
- Out of sight, out of mind
- Disgruntlement (layoffs)
- Leadership approach change

In HR departments, on-boarding and off-boarding happen online currently, and in the age of GDPR, it is difficult to do proper background checks and employee vetting. Some of the hypothesis' is that:

- Remote work could impact employees' loyalty negatively as well
- Remote work reduces the chances of recognizing disgruntled or radicalized employee

- Some of the jobs will get lost as it has been shown during Covid-19 that they are obsolete
- A new era in work leads to higher employee turnover and more gig economy

All corporate security departments need to brace for rising insider threats and holistically approach the problem with InfoSec and IT Security through the DLP program, together with Data Privacy need to deliver input here from the technical and legal side. Nevertheless, physical security experts, especially the ones that are coming from the counter-intelligence field, have here a great chance to either contribute to or implement and lead this program comprehensively and sustainably. HR and legal departments are here crucial, creating the right approach.

Lana Djurkin-Koenig

To cite this article: Djurkin-Koenig, Lana. “Corporate Security Post COVID-19”. GloHSA Brief no. 3(2020); https://glohsa.com/.