

How COVID-19 Is Impacting the Security Industry



You could say that the COVID-19 impact has been the ultimate in workplace disruption for 2020. The ripple effects have been far-reaching, and they may not be wholly realized for some time yet. As the face of the workplace has changed, it is more apparent than ever that security is a critical factor in business continuity. So, what does that mean for the future of the security industry?

Cybersecurity Investment

There is no doubt that the impacts of the pandemic have caused business leaders to recognize that they must reconsider their cybersecurity strategies. Digital, technology and cyberservices must scale to support a remote workforce. That requires investment not only in dollars but in planning, implementation and maintenance.

Traditionally, IT budgets are set as a percentage of revenue. With the COVID-19 impact, forecasts have undergone multiple revisions, and the outlook is still hazy, particularly as the pandemic drags on. What is clear is that no one can risk a breach in the middle of a fight for survival. It is estimated that by 2021, global security spending will exceed \$1 trillion.

Will that still happen? That, too, is unclear. S&P Global Ratings forecasts a decline in IT spending of 3% year over year. As the predictions for 2020 were predicated on the decline of the virus in late Q2, the longer it lasts, the worse the decline could be. Between supply chain disruption, decimated sales and minimized workforce, spending could still fall by the wayside just as the need for robust cybersecurity becomes even more emergent.

Alarm Monitoring

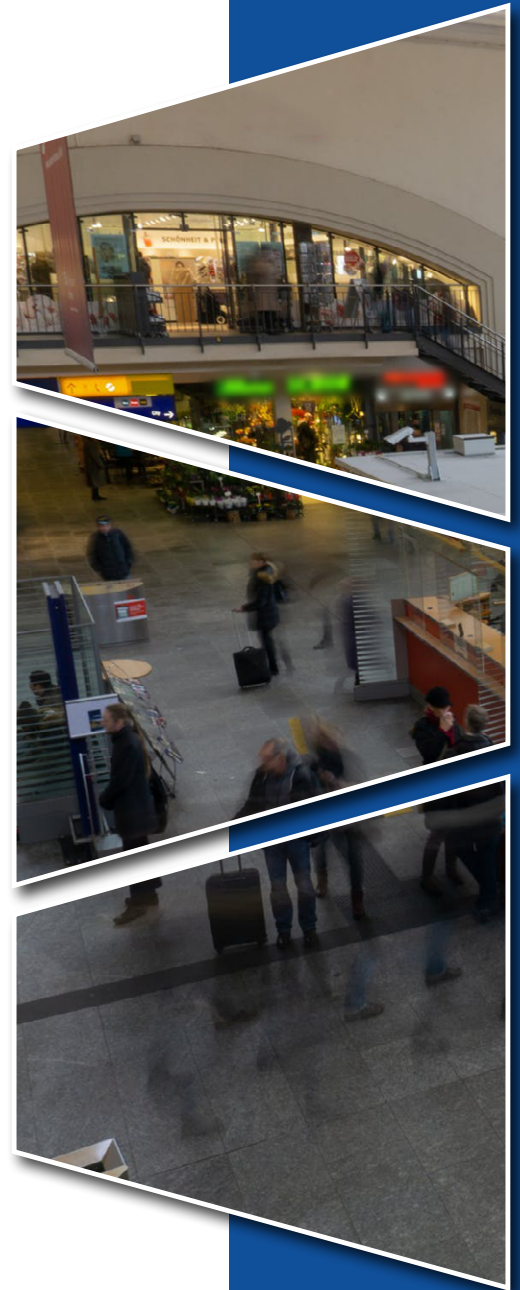
With essential businesses having to work with reduced staff due to the rising infection rates, alarm monitoring is an even more critical safeguard. Recently, the Electronic Security Association (ESA), the Security Industry Association (SIA) and The Monitoring Association (TMA) released the survey results of their collective members of the effects of the pandemic on electronic security and safety businesses. The results were less than encouraging.

Respondents reported an expected 21-30% loss of revenue. More than 60% had already incurred losses equal to or greater than that. 20% reported a loss of over one half of their company's revenue. Of this group, only 4% were denied essential business status. At precisely the time when automation could bolster a flagging workforce, there is no money to invest.

However, despite the dismal statistics, ResearchandMarkets.com predicts that North America is expected to take the market share of the global cybersecurity industry. Understanding that temporary setbacks in spending do not herald a decline in need, some of the industry leaders have adopted innovative growth strategies by forming strategic partnerships. New service launches focus on the unique needs as a result of the COVID-19 impact. Increased use of automation and AI for threat detection combined with a vast amount of data across verticals and, despite evidence to the contrary, increased investment in security solutions are driving the penetration of the technology in North America.

Health and Safety

Healthcare workers, without a doubt, are at the highest risk of any workforce segment during the pandemic. They are on the frontline day after day, immersed in a desperately sick



patient load. It is extremely critical that there is a way to prevent transmission of the virus between workers, particularly in hospital settings. Infrared body temperature monitoring and large scale detection systems are being developed, if not in time for this pandemic, then for prevention of future ones.

It may be a surprise that healthcare has the highest expected growth rate in cybersecurity. You think of only the frontline workers, but there is a huge support staff that keeps hospitals and clinics open. As those segments work from home, the risk to HIPPA compliance from unauthorized use, malware and unsecured home networks increases. Access control becomes even more critical during workplace disruption.

The World Health Organization issued an alert in February 2020 that cybercriminals were creating fraudulent sites and email addresses to pose as WHO. Remote workers are vulnerable to phishing from these fake organizations, many of whom are soliciting donations in bitcoin for the development of vaccines. Cyberattacks happen when there are vulnerabilities. Though the chances of cyberattacks increase when workers use their own devices, according to a survey from Chubb, only 46% of workers were concerned about cybersecurity.

Cybersecurity Is Critical to Global Business

As risks increase, so do opportunities. Cybercriminals understand that. For businesses, investment in cybersecurity is the opportunity when the risk of threats is the greatest. We are all well-versed now in risk mitigation as it pertains to coronavirus prevention. It should become second nature for businesses to mitigate the threat of intrusion and cyberattacks, as well.

SIS knows all about monitoring and threat detection. You could say that it is in our DNA. With numerous partners and certifications from the Department of Defense Information Assurance Certification and Accreditation Process to the Secure Configuration Compliance Validation Initiative and many more, we have the solutions you need to keep your business safe and secure, no matter where your workforce is located. Contact us today for more information.

<https://www2.deloitte.com/global/en/pages/about-deloitte/articles/covid-19/covid-19-s-impact-on-the-defense--security--and-justice-sector-.html>

<https://www.securityindustry.org/coronavirus-resources/>

<https://www.businesswire.com/news/home/20200728005739/en/Government-Cyber-Security-Market-Impact-COVID-19-highlights>

<https://www.globenewswire.com/news-release/2020/05/15/2034055/0/en/Impact-of-COVID-19-on-the-World-s-Cybersecurity-Industry-Major-Verticals-Regions-and-Key-Vendors-2019-2021-Optimistic-as-is-Pessimistic-Scenarios.html>

<https://www.marketsandmarkets.com/Market-Reports/covid-19-impact-on-cybersecurity-market-128702677.html>

<https://securityboulevard.com/2020/05/the-economic-shutdowns-impact-on-security-budgets/>

<https://www.securityindustry.org/2020/05/01/research-results-impact-of-covid-19-on-the-industry/>

<https://www2.frost.com/frost-perspectives/mass-screening-for-covid-19-related-fever-how-the-instrumentation-world-can-help/>

<https://www.benefitspro.com/2020/07/24/chubb-work-from-home-survey-reveals-new-and-emerging-risks-412-101478/?slreturn=20200629130514>

