www.pipelinepub.com
Volume 17, Issue 7

Mitigating Risk & Compliance

By: Dr. Cemal Dikmen, CTO, SS8 Networks

It has been said that nothing is constant except for change. But not all change is the same and the pace of change we are now seeing is very different than what we've seen before, presenting both new opportunities and challenges.

The evolution of technologies we've seen over the last decade or two has been exponential and is having a compounding effect. We've seen dramatic increases in storage capacity, bandwidth, and computing power. Add to this the evolution of mobile technologies as we quickly progressed from 2G, to now 5G, at an incredible pace. Then, layer on top of this technology drivers such as e-commerce; mobile device proliferation; the Internet of Things (IoT); cloud, containerization, and virtualization; software-defined networking (SDN), automation, machine learning (ML), and artificial intelligence (AI) – and it starts looking a lot less like change, or evolution, and a lot more like combustion. It would be like if the advent of human flight, nuclear fusion, genetic engineering, rocket fuel, and space travel occurred at the same time as that of the advent of the wheel. Certainly, this would have created an explosion of new opportunities and, with it, an abundance of risk.

Multi-dimensional risk factors

Each facet of these advancing technologies comes with their own unique and inherent risk profiles. Our dependency upon them as well as the mission-critical nature of their use cases only exacerbates these risks. 5G, for example, has its own, unique risk factors – but add to that the use case of self-driving cars or smart utility grids, and the risk is significantly amplified. Similarly, the

explosion of the IoT creates unique vulnerabilities, but then consider the use case for remote surgery or insulin pumps and risks increase exponentially. In addition, the rate or speed of adoption across all these technologies is being driven by a seemingly insatiable demand with enterprises and service providers struggling just to keep up, focusing primarily on implementing the required infrastructure needed to capitalize on these emerging opportunities.

Government regulators are tasked with developing broad-reaching requirements to mitigate risk to citizens, businesses, economies, and even entire countries. There is just one problem. The regulators are less concerned about the underlying technologies, and much more concerned about the consequences. In the case of terrorism, they don't care about how you are delivering your services, they care about stopping the threat through effective lawful intercept. They don't care if a self-driving truck is using 5G connectivity, they care about stopping someone who may have loaded it with explosives and now has control over where it goes. And, while that may seem farfetched now, it's not as unrealistic as you might think.

Not that long ago, we saw the disruption of connectivity across the entire US East Coast with the Dyn attack – costing companies an estimated billions of dollars in damage. Hackers used malware to take over millions of unsecured IoT devices and launch sophisticated and coordinated waves of attacks to overwhelm Dyn's servers and bring down large ecommerce, social media, and entertainment companies such as Paypal, Twitter and Spotify. While several years ago, the Dyn attack serves as a dark milestone as the world's largest, most coordinated, and effective IoT cyber attack in history.

More recently, the US saw foreign states penetrate the highest level of government for months, with what has become known as the SolarWinds attack. Couple that with the cyberattacks on pharmaceutical companies developing the COVID-19 vaccine, and the risk is very real. In addition, the persistent threats to infrastructure can cost more than money; they can cause the loss of life.The 2020 winter storms in Texas illustrate how critical our dependence on infrastructure has become, and the havoc that could be caused by a successful attack on power grids. And what we have witnessed to date may just be the beginning or, if nothing else, the tip of the iceberg. These events aren't just indicative of the actual risk today, but rather a small glimpse into what the telescoping magnitude of risk could look like in the future.

In fact, four days after this article was originally published in *Pipeline* magazine, a coordinated ransomware attack was conducted against Colonial Pipeline, which is being viewed as "one of the most significant attacks on critical national infrastructure in history." The attack, coordinated by the Russian-based cybercrime organization DarkSide, shut down the flow of oil, gas, diesel, and jet fuel to nearly half of the US East Coast, affecting millions of people and disrupting hospital, medical, emergency, first responders, transport, and air services.

Failing to comply with regulations creates a wide variety of risks. To the companies at the epicenter of a breach, like Dyn or SolarWinds, the damage to brand recognition can be almost incalculable. Their brand has now become synonymous and forever aligned with the term, "breach." In the case of Colonial, the company shelled out nearly five million dollars to recover their data and control of their systems. However, the public risk, may actually be higher. In the case of SolarWinds, the breach has led to the increase of tensions between the US and Russia.

In April, we learned that Russian-backed cyberterrorist organization REvil was responsible for a ransomware attack on the Taiwanese Apple-supplier Quanta, and began releasing Apple's intellectual property on the internet – and stated that it will continue to do so – unless it meets its demand for a 50 million dollar payment. Leading some to speculate the attack was a response to the sanctions recently levied on Russia by the US for its part in the SolarWinds breach. And SolarWinds isn't going away, as Microsoft reported in a blog post that a second attack seems to have conducted by the same group as the first, which began in February and culminated through May 2021.

In response, the US Department of Justice has announced the launch of a multilateral task force comprised of Executive, Judicial, Treasury, and Intelligence agencies to investigate and respond to nation-state-sponsored ransomware attacks. This comes just weeks after the White House had already announced the launch of the Unified Coordination Group (UCG) following a Microsoft breach which has been attributed to China. These things tend to escalate quickly.

These are just a few examples that underscore the important of a good security posture, encompassing both regulatory compliance and lawful intelligence. It is also why failing to comply with these regulations comes with steep penalties. These penalties can range from $10,000 to $50,000 dollars per incident, per day, or more – including the revocation of your FCC license.

Innovating Lawful Intercept

Mitigating these risks, in addition to being a legal requirement, can also be viewed as a moral, civic and fiduciary responsibility. Doing it wrong, however, can be costly. Doing it properly can not only protect your organization and the public, but it can also empower law enforcement to better respond to real and active threats with real-time lawful intercept.

We are working with organizations around the world to ensure they are compliant and their infrastructure is secure. We are also acting as a bridge between the organization, application providers and law enforcement to rapidly respond to legal requests needed to provide law enforcement with the lawful intelligence they need. This provides us with a unique perspective on the challenges they are facing today.

Over the last decade much communications intelligence has been going dark due to the mass adoption of encryption technologies across networks and applications. Even with a court order, this can be challenging. At the same time, the amount of data law enforcement has access to has been growing rapidly. This includes social media, traffic cameras, over-the-road tolling, license plate readers, location data, and credit card transactions.

Technologies such as 5G can be used to provide better throughput for law enforcement, and more precise location data based on density of 5G access points required to provide adequate 5G coverage. In the past, location data using cell-tower triangulation would be accurate to within a few miles. With 5G, it can be as accurate as to within a few centimeters. Correlating precise location data with data from multiple sources in real time can literally save lives.

In just March of this year, a gunman went on a shooting rampage in Georgia at spas throughout the Atlanta area. The Georgia State Police (GSP) was able to obtain video footage from the businesses to post an image of the suspect on social media, where his family identified the suspect. The GSP then used location data from his cell phone to locate his position, where law enforcement was able to intercept and put an end to his killing spree. After he had been taken into custody, the alleged shooter indicated that he had no intention of stopping and was on his way to continue his heinous acts into the State of Florida. Had he not been stopped, the death toll could have been much higher, and it was only through a rapid and coordinated response by law enforcement, and a correlation across a variety of data and tools, that law enforcement was able to stop the shooter and save lives.

Providing this critical link for law enforcement for lawful intercept is monumental. It goes well beyond the need for compliance and underscores the importance of the role that organizations, application providers and service providers can play to protect the public.

Lawful Intelligence

As organizations accelerate the adoption of new technologies, they need to contend with serious compliance regulations. They also have a responsibility and an opportunity to play a vital role in lawful intercept by efficiently and effectively doing so. The threats are real, and now is the time to work together to mitigate risk and protect each other and our future.