www.pipelinepub.com
Volume 21, Issue 1

Letter from the Editor

By: Scott St. John

What was once the subject of science fiction is now becoming top of mind for business leaders. Some threats are here today, and others are just over the horizon. Artificial Intelligence (AI) is being used, right now, to target your business. Medical devices are being programmed remotely, “over the air” and are vulnerable to attack. Quantum computers are being designed to crack encryption to gain access to trade, and national security, secrets. Concern is certainly warranted. *The Future of Life Institute* went so far as to posit modern advancements "create risks of catastrophe on a global scale."

Our lives will continue to depend upon complex, ever-evolving systems. But, pulling the technology rug out from under us at this stage has the potential to shatter entire economies. We rely on these systems to sustain our work, health, social life, and financial security. But even a cursory glance at the nightly news shows the fallibility of day-to-day reliance on technology. Whether it’s the Crowdstrike outage, SolarWinds supply-chain attack, Dyn DDoS attack, Colonial Pipeline IoT critical-infrastructure ransomware attack, or any of a myriad of other examples of data breaches in recent memory, we have ample evidence that the risks are very real. What’s important is we learn to balance the risk with the reward.

Conservative estimates put the cost of the Crowdstrike outage at $5 billion and Delta Air Lines has filed a $500 million lawsuit as a result. And that was just one, small “glitch.” But financial costs are only one factor. There are many other cases where the consequences can be much more severe.

For instance, GenAI is autonomously running extremely sophisticated social engineering and phishing scams that appear legitimate – including realistic but artificially created communications between executive stakeholders. It's also possible that medical Internet-of-Things (IoT) devices such as pacemakers or insulin pumps could be targeted, and hacked on a large-scale basis. We’ve already seen a massive-scale, coordinated IoT attack with Dyn. Q-day is a lot closer than we think, and we already saw the exploitation of government vulnerabilities during the SolarWinds breach.

Futurist and principal researcher at Google Ray Kurzweil popularized the concept of the singularity, which happens when progress achieves a near-infinite growth rate. The same idea applies to the dangers posed by technologies like AI and quantum computing. The risks may accelerate at the same speed as the opportunities. Enterprises, the primary drivers of growth and adopters of technology, must pay equal attention to both sides of the equation.

Stringent ethical and cybersecurity measures, along with appropriate certifications and assurance processes, are no longer optional. They're a business imperative, and necessary to avoid catastrophic consequences. They are also needed to ensure the safe realization of the colossal benefits these new technologies can provide, such as allocating resources in disaster zones or enabling AI-driven cybersecurity.

It's in this context that *Pipeline* looks at innovative approaches to contend with emerging threats. Increasing technical complexity breeds specialization. For example, a quantum computer is vastly more sophisticated than a classical one. Responding to a cyberattack run by AI demands a more sophisticated response than one orchestrated by a human hacker. This must be taken into consideration, and imbued across all technologies business leaders adopt.

Fortunately, there are those that are both sounding the alarm and answering the call. We're seeing an array of dedicated solutions, standards, services, certifications, and best practices to deal with emerging threats. As the risks evolve, so do the counter-measures. In fact, they are an essential part of the innovation stack that enables businesses and technology leaders to create differentiated, groundbreaking offerings. And, it's what makes this issue of *Pipeline* so important.

In this issue of *Pipeline*, we focus on security and assurance in an increasingly dangerous digital world. Dispersive looks at cybersecurity challenges in the age of AI and quantum computing. CHR Solutions provides best practices to contend with rampant cyber attacks. *Pipeline*'s Dr. Mark Cummings explores the rising threat of GenAI social engineering attacks in a special feature. Red Hat outlines several important open-source AI use cases and ethical AI standards. Oracle discusses how SATCOM and 5G are saving lives in disaster zones. Atheras Analytics demonstrates how AI is being used to prevent outages in high-throughput satellite (HTS) networks. Mobileum analyzes satellite security and assurance for fraud-free IoT and Subex shows how CSPs can navigate digital transformation with effective migration assurance strategies. Botdoc discusses why the future of automotive data privacy lies in adopting stringent measures and CyberNINES offers an in-depth practical guide to cybersecurity certification. Plus, we bring you all the latest IT and telecom news headlines and more.

We hope you enjoy this and every issue of *Pipeline*,

Scott St. John
Managing Editor
Pipeline

Follow on X | Follow on LinkedIn | Follow Pipeline