www.pipelinepub.com
Volume 19, Issue 1

Letter from the Editor

By: Scott St. John

It's that time of year again. For those that celebrate Halloween, it's chocked full of costumes, candy, and late-night scary movies. It's an interesting holiday, where millions of people try to turn fear into fun. It's also become big business as candy, costume, and content companies all try to cash in.

After all the tricks and treats the real world awaits, and it can be even scarier. Hard as we may try not to, many have to worry about what will happen when they simply leave their houses, go to the movies or a concert, or even send their children to school. The world can feel like a menacing place and in many ways, it is. Whether it's the prevalent threat of violence, the next pandemic wave, senseless random acts, or the increasingly possible threat of nuclear war the risks are real.

Unfortunately, the threats don't end there. They extend to many other aspects of our increasingly connected world. And that's top of mind for technical executives and security professionals going into the New Year. The focus has shifted from simply delivering services to worrying about nation-state attacks, ransomware, and hackers targeting your connected devices to create a massive digital army to conduct massive DDoS attacks, target implanted medical devices, or bring down critical infrastructure. Business as usual has become rather unusual, with security becoming a paramount consideration of virtually every facet of operations today.

However, defending against the next threat can be a difficult business itself. It's like attempting to find the proverbial needle in a haystack, in multiple haystacks, while the needed continues to change shape, size, and color. To complicate things further, the haystacks keep getting bigger and bigger as do the real-world consequences of a breach. Think about the stolen Pfizer COVID-19 vaccine data leaked by hackers in 2020, or how the Colonial Pipeline ransomware attack brought oil and gas operations to a halt for five days. Or the 2021 ransomware attack that shut down JBS meat processing plants in three countries for more than three days.

The lists go on and on (e.g., Dyn, Equifax, SolarWinds, Target…). These are real threats, and increasing in frequency size, severity, sophistication, and scale. The costs are also escalating, and fast. IBM estimates the average cost of a data breach this year at between $4.35 million (globally) and $9.44 million (in the United States). But that's just an average, not the ceiling. The Colonial Pipeline ransom tallied $5 million, and the JBS reached $11 million. Hacking, like Halloween, has become big business. And those are just the amounts that hackers demanded to relinquish control over victim's systems. It doesn't account for the millions and billions in lost revenue, regulatory fines, or the many lawsuits the stem from breach. This is the world we live in today, and these persistent and prevalent risks now jeopardize everything–from heating our homes to putting food on the table.

The good news is that there are many technical innovators and cybersecurity masterminds developing and deploying the most advanced security solutions around the world. They are on the front lines working tirelessly to outsmart and combat bad actors to thwart the next attacks. They are making next-generation security a reality, with AI-driven cybersecurity solutions, drones, robot patrol dogs, zero-touch network security, and automated threat detection and response solutions. Their innovations are changing the game for technology decision-makers. It's what makes this issue of *Pipeline* critically important.

In this issue of *Pipeline*, we explore a variety of topics related to security and assurance. ZPE Systems reveals how to **close the Top 5 operational security gaps** with holistic cybersecurity. *Pipeline's Dr.* Mark Cummings identifies a promising approach to tackle the **needle-in-a-haystack problem of cyberattacks**, while Orchestra Group explores **emerging AI cybersecurity approaches** to bolster cyber defense. Allot presents **zero-touch cybersecurity** as a 5G differentiator, and Novva Data Centers shows us how **AI, drones and robotic dogs are transforming the future of security.** Dispersive Holdings explains the **value of deploying a stealth networking strategy** to protect critical infrastructure and Corsa Security shares how a **virtual firewalls** can help service providers unlock new opportunities. Red Hat analyzes how open-source tools can be used to **revolutionize supply chain security.** Spirent explores how **adopting active assurance** can help CSPs reimagine how they monitor network services, and Subex illustrates how **real-time margin assurance** can help CSPs protect their bottom line. All this plus the latest **enterprise and communications technology news** and **more**.

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

Scott St. John
Managing Editor
Pipeline

Follow on Twitter | Follow on LinkedIn | Follow *Pipeline*