Talk up AI and ML at the Spring Meeting's Town Hall Innovation Series!

Thank you to all of our security speakers at the Q4 Meeting: David Rogers, Copper Horse; Michael Rosa, NSA; Michael McFarland and Phil Fine, Ciena; Dmitri Vellikok, F-Secure; Christophe Buffard, NAGRA; Owen Law, AWS. You can access the THIS presentations, recordings, and notes here.

Addressing a major concern for the industry, the topic of security was discussed. Our presenters covered the use of AI for both positive and negative purposes, the need for machine-speed reactivity, and service providers being held accountable for every aspect of broadband wellbeing, including security. Interest was also piqued on the role open standards have to play regarding cloud security, the device authentication and anonymity paradox, and how security is multi-faceted.

Key takeaways from the sessions was that security is a by-design requirement in any technology, network, or service we specify and that the telco industry must unite with regulators and institutions to help all companies benefit. This will lead to differentiated services and new monetization opportunities.

The theme presented at each face-to-face meeting align with the Forum's strategic vision and industry trends. These topics are expected to stimulate and influence future work and act as a catalyst for new projects.

The next Town Hall Innovation Series (THIS) sessions on AI and ML will take place on Monday, March 4 during the Spring Meeting in Mainz, Germany. (So plan your trip accordingly!) The call for papers is now open. For more information or to submit ideas, please contact the THIS Co-Chairs Mauro Tilocca and Christele Bouchat at this@broadband-forum.org.

.....

From eSports to criminal usage, industry needs to prepare the ground for greater resilience, transparency and mitigation of AI threats

Network resiliency and assured availability are key for solving AI related security threats and unlocking new opportunities according to **CEO and Founder of Copper Horse, David Rogers MBE.**

"We can't get away from Artificial Intelligence. Despite what we hear in the media, it can be used positively for global applications, such as cancer care diagnostics. Although there remain concerns about ethics," Rogers advised.

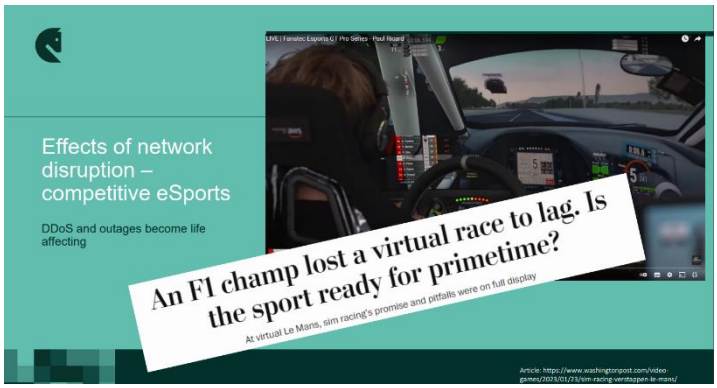
With the pace of AI's development steadily increasing, in many instances, it continues to pass human performance. The number of AI related products and service offerings grows, but so too do the associated fears of criminal usage. Rogers advised that the reality is that new technology will always be quickly embraced by criminals if it enables them to accomplish their goals.

One negative example of AI was the use of deepfake videos and voice cloning to deceive and impersonate people. Rogers advised that fake, 'virtual kidnappings' are already common in the United States and Latin America and that the modus operandi is likely to evolve with AI. There is commonality in the AI threats that the telecoms industry face, and those in the anti-fraud space continue to be concerned.

Malware can be deeply embedded within AI models to hide across platforms and avoid detection by making itself look normal and by changing its characteristics to enhance the capability of the attacker. It is straightforward to create malware, and those performing malicious malware attacks are trying to work out how to exploit guardrails (AI policies) built into AI services. Guardrails can also hamper AI defenses against a malicious AI that has none. Rogers highlighted the real need for greater transparency around AI models and a more mature debate about AI safety when used in a defensive situation due to these issues. While most pieces of AI equipment blindly accept the inputs they are given, Rogers advised, that the telco industry need to carefully design systems against malicious attacks. Smaller organizations might lack the agility or be slow in developing and deploy new protection techniques.

Self-Organizing Networks (SONs) are designed for things going wrong, rather than being made to go wrong through malfeasance. The 'intelligence' that is built-in is rudimentary. Network technology such as SONs can technically automatically self-configure, self-heal, and self-protect. AI, predictive analytics, and pre-optimized software algorithms make this possible. But they must have adequate foundations of security and be ready to deal with attacks. Otherwise, Rogers stated, the technology is not fit for purpose against the likes of distributed denial-of-service (DDoS) attacks against the network.

One example highlighted by Rogers that could act as a good indicator of what the future holds in other spaces was cheating in eSports. This user manipulation occurred in the online digital world for cycling, 'Zwift' where users cycle on a stationary bike that transfers data from the wheel into the game. But these physical sensors can be manipulated to create a misrepresentation of the real world to the digital world. Male cyclists were cheating by registering as women and entering women's races. As such a digital 'anti-doping agency' was established to verify the real-world identity of athletes and to end "digital doping". The use of hacks to gain an unfair advantage and equipment tampering continues in these arenas.



Rogers explained that the effects of network disruption in competitive eSports were very well demonstrated by disruption to simulated GT3 racing online, which has become a huge eSport. This was where lag – resulting in accidents and incidents or race abandonment - and targeted DDoS attacks were experienced during many events. This highlights the crossover of the digital and real world. With real-world drivers who have readied themselves for the consequences of major crashes now taking part in sim-racing, it is entirely possible that a driver could experience harm in the real-world, like a heart attack, due to the stress induced by an 'accident' situation. All these incidents point towards future requirements as we move to a more cyber-physical future. Therefore, to address these issues, the network needs to be resilient and assure the delivery of availability through features such as network slicing.

There remains an issue with input control, quality and validity for sensors and actuators such as low-quality potentiometers used in pedals to remotely drive autonomous vehicles. This includes self-driving cars controlled by gaming equipment. Rogers advised that the industry needed to provide high quality, transducer actuation safety, low latency and assurance, validation and accountability in future networked services of sensors and endpoints.

Global government action is required to outline 'responsible AI' and introduce the necessary regulations. Rogers commented on the importance of strength in depth when deploying security against AI threats in multiple places across the access network and at the edge.

"There is a collective responsibility to improve network architecture to mitigate some of these AI-related risks and build the resilient networks of the future," Rogers concluded.

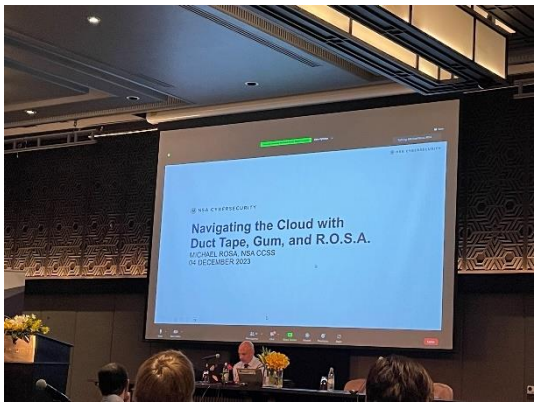
……

Open-source and open standards can reduce fragmentation of cloud security

Michael Rosa, CCSS Cloud Security Lead at the National Security Agency (NSA) discussed the deficiencies in cloud security standards. Rosa urged the industry to take a step back and have an honest conversation about the role of regulations, open-source, security, and automation, and how to expand industry engagement. Acknowledging that cybersecurity within cloud technologies is intricate and a hard problem to navigate, Rosa advised that standards development organizations (SDOs) must come together to find common ground to reduce fragmentation.

During the presentation, it was highlighted that the growing number of global regulations being enforced have led to increased fragmentation and conflicts of cybersecurity standards. Rosa stated that the security threats have not disappeared by moving to the cloud, emphasizing the need for it to be managed at scale with security embedded right at the start.

The increase in open-source projects and solutions, led by the industry, were identified as the key to tackling interoperability issues. NSA aims to contribute to open-source projects to develop consensus-based solutions for cloud security, interoperability, and automation. While open-source technology is nothing new, it is prevalent in pre-standardization research and presents new opportunities for everyone, Rosa stated. But harnessing open-source code in a more secure way is vital.



The likes of automation are helping the NSA mitigate threats, drive continuous Authority to Operate (cATO) through a 'whole-of-Government' approach, and assess methodologies to approach multi-cloud concepts. Rosa sees NSA's work protecting and supporting the adoption of cloud standards for National Security Systems and the United States Defense Industrial Base. Providing its expertise, NSA is also aiming to build Zero Trust principles into international standards.

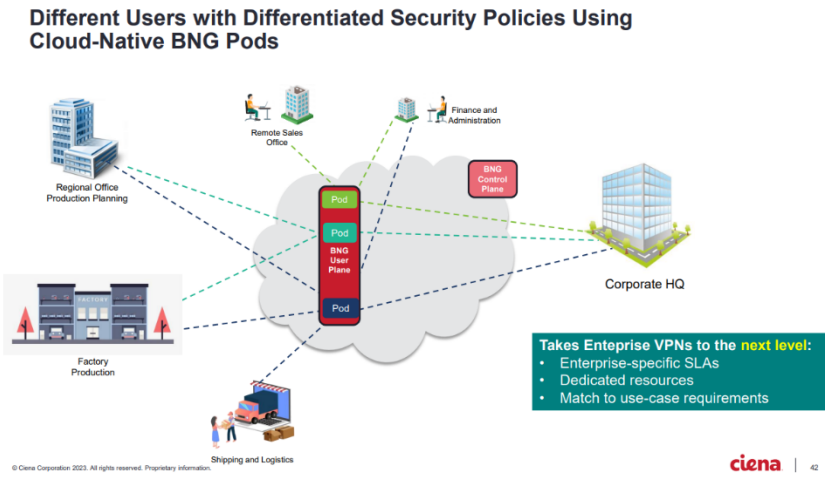
While there are differing levels of cybersecurity to protect networks for varying end-user and enterprise needs, SDOs have an overarching responsibility to move in the same direction and find common ground. Rosa advised that now is a great opportunity for industry collaboration to make recommendations for best practices and continue the rallying call for standardized cloud security and open-source solutions.

.....

Cloud-native Broadband Network Gateways (BNGs) with Secure Access Service Edge (SASE) is the blueprint to follow for secure networking

Combining broadband subscriber management with security is paramount to extracting greater value from network investments according to **Michael McFarland, Senior Director Product Line Management, and Phil Fine, Director, Broadband Access Solutions at Ciena.** The two Ciena experts discussed the rise of security threats and advised that broadband service providers must consider architectures that incorporate network-enabled security to protect their customers.

A key message delivered during the presentation is that subscriber awareness and network-based security can deliver secure connectivity for broadband services. The duo discussed how a cloud-native broadband network gateway (BNG) with secure access service edge (SASE) can provide subscribers with more secure Internet services. Networking can be simplified and security consolidated. BNGs are an essential piece of the network for providing insights into subscriber usage and traffic. And a network without security is "like buying a car without any door locks," said McFarland.

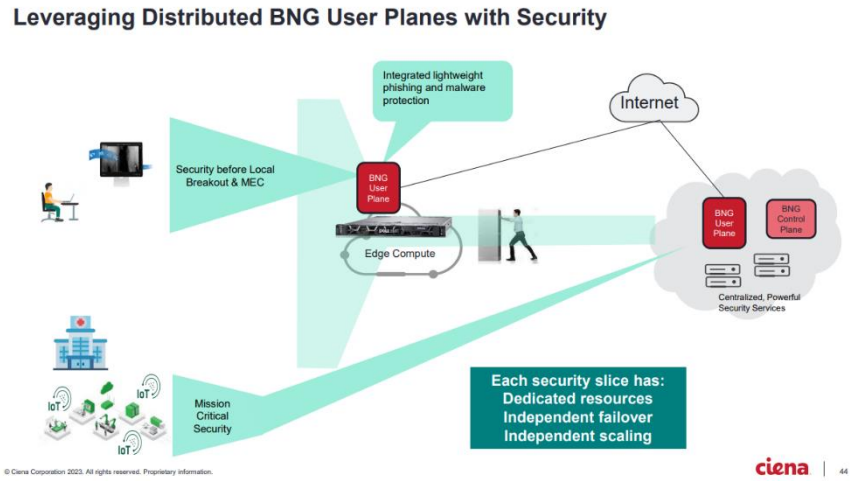


Security is an integral component within the network but there must be different approaches to how security is handled for customers and enterprises forewarned McFarland.

According to McFarland, while traditional solutions have required an on-premises device to provide security, this involves significant Capex, operational complexity, and a single point of failure. By moving security into the network with components of a SASE solution, there are reduced costs and complexity, and a collective set of resources can be allocated more granularly for different end points as not one end point is overloaded.

Importantly, this provides the ability to adjust capabilities over time in a limitless way, delivering more compute and more memory as threats demand. Cloud-native services enable carriers to adjust to dynamic threat environments without distributing new policies to thousands or millions of end points. There are clearly tremendous benefits available to the service providers in terms of cost, network evolution, and delivering a true value-added service to consumers by leveraging the power of the cloud.

The Ciena experts also explained that monolithic hardware-based platforms are as difficult to allocate resources for different use cases, such as enterprise or IoT. During the presentation, the cloud-native BNG user plane was shown as a key way to address enterprise-specific SLAs and allocate dedicated resources to match policies for a particular use case. McFarland advised that this takes virtual private networks (VPNs) to the next level.



SASE can be added to examine and detect attacks in the VPN and MPLS (Multiprotocol Label Switching) Layers and secure the network in a cost-effective way. These same services can be repurposed for consumer grade services too. McFarland talked about the benefits of Broadband Forum's CUPS (Control and User Plane separation) work as the BNG was traditionally centralized, but with CUPS, user planes can be distributed to scale more easily. CUPS enables enhanced network security, such as integrated phishing, malware, and denial of service protection to be rapidly deployed in line with the user plane and enable security on demand. Each security slice can have dedicated resources, independent failover, and scaling.

Next-generation firewall features can include vulnerability assessment and suspect site monitoring.

Ciena was involved in this year's CloudCO Demo to highlight the importance of security in the service delivery network. The Ciena demo highlighted two work from home use cases. They demonstrated the dynamic allocation of compute resources by deploying a cloud-native next-generation firewall (NGFW) in line with virtual BNG user plane function in a hybrid multi-cloud deployment. The NGFW was used to enforce security polices prior to hitting the Internet or enterprise network. The two use cases demonstrated the power of a cloud-native firewall: secure high speed Internet access, and clientless work from home. The NGFW was used to deny traffic as would be the case for securing the subscriber's Internet service, and to allow specific traffic to the enterprise network for the subscriber accessing corporate assets needed when working from home.

Ciena's demonstration of its subscriber and security functions in a secure hybrid cloud environment was emblematic of its innovative thinking about how the cloud can be used to deliver advanced services over multi-vendor multi-technology fixed and mobile access networks.

.....

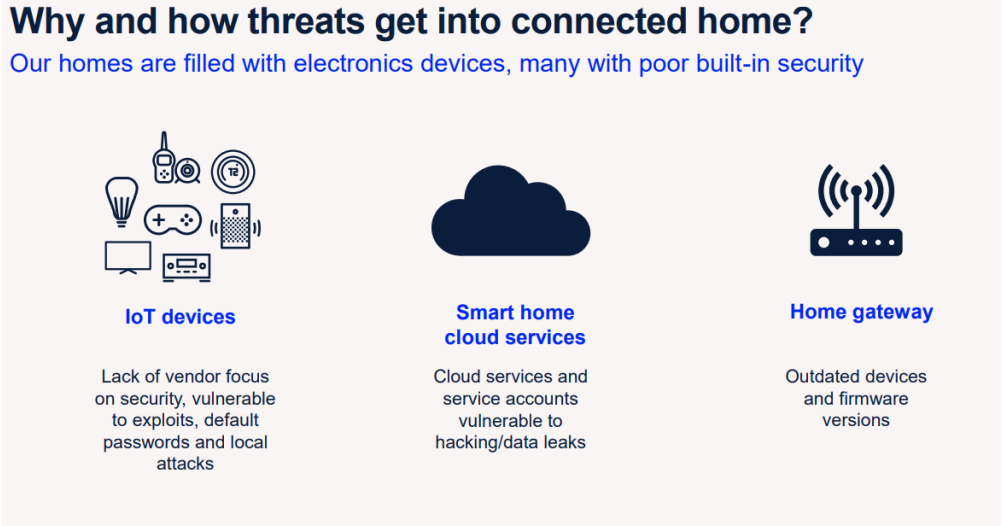
Simplified security measures in the home can lead to greater trust and brand reputation for BSPs, according to F-Secure

Customers are increasingly more conscious of cybercrime and online security. With only 38% of broadband service providers (BSPs) currently offering security solutions, customers are more willing to switch BSPs in search of better security. In addition to feeling more secure, the customer also demands greater simplicity. According to F-Secure research, 82% of consumers in the APAC region stated that they were willing to move BSP, bank, or insurance provider for a clearer, less complex cyber security service, **Dmitri Vellikok, VP Network Security Business at F-Secure** advised.

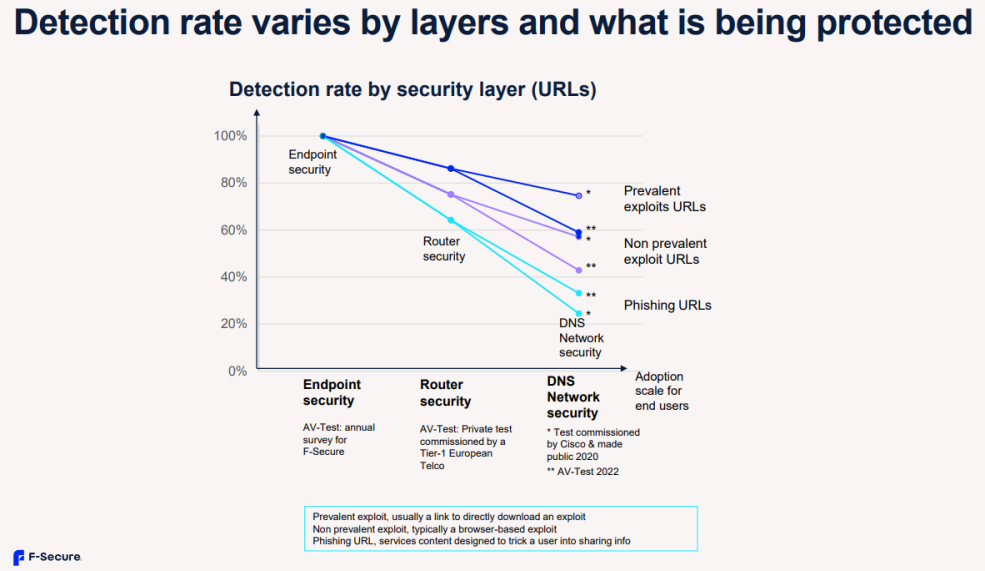
Vellikok highlighted that cybercrime is increasingly more prevalent. In a survey this year, 33% of respondents said that they were victims of cybercrime in the last 12 months, a 4% increase from 2020. Such significant cause of stress and anxiety combined with the possibility of significant monetary loss, drives consumers to look for alternative BSPs if they are not satisfied. Interestingly, F-Secure research highlighted that customers are less wary off banking applications, deeming them more trustworthy than other applications, such as social media.

Home connected devices can often have poor built-in security, making home gateways, IoT devices, and smart home cloud services all vulnerable to hacks. 66% of consumers interviewed expressed worry about the online security of their Internet connected devices, with 48% postponing smart home device purchases. Vellikok advised that there is a key opportunity for BSPs to grasp.

"57% of respondents would rather have car stolen than their identity," Vellikok announced. Customers know that they can replace their car, but not their identity,



and are left feeling helpless at the possibility of identity theft and considerable monetary loss. With no idea if their solutions are secure or not, customers need a trusted partner: 81% of interviewees expect service providers to give them some level of security protection, and 64% would prefer to purchase security solutions from their BSPs. Vellikok advised that these expectations can improve BSPs brand reputation, but offering basic protection is not sufficient. Providing customers with proof points and analytics that can show them that risks or attacks are being thwarted, are essential to help building trust.



Close proximity to the end-users' devices and data matters. There are different solutions for the cloud, device, edge of the network, and home network. But Vellikok noted that detection rates were far higher when it came to the device (endpoint security) and home network (router security).

Getting as close as possible to the customer by delivering security at the router will allow broadband service providers to provide browser extension and protect against malicious activity. The further from the consumer, the lower the protection level is from the service provider.

The customer does not need to know how the security works, Vellikok stated, they just need to be able to rely on and trust their broadband service provider. A suitable security solution drives trust and should be a key staple of BSP's brand proposition. The right security solution should be tailored to each user's specific needs.

Tying into Broadband Forum's app-enabled services gateway project (WT-492), while BSPs previously stopped at the edge, with the subscriber required to be responsible, this is a key opportunity. For the flurry of applications and services in the connected home, it is up to BSPs and third-party providers to provide the missing piece.

Vellikok stated: "Currently many are patching the problem, not providing the solution. But subscribers need to be aware of the issue. If you own a car, it is not the car manufacturer's fault if it is stolen. But security companies can provide the last piece of the jigsaw for securing a network."

It will require the collective effort of all parties to make subscribers aware and allow them to enjoy their lifestyles using their connectivity care-free, Vellikok recommended. BSPs need to focus on bringing security closer to customer accounts, delivering greater simplicity for customers to overcome complexity, and protecting customer digital moments.

.....

The paradox of device authentication and anonymity

Christophe Buffard, Principal Architect at NAGRA, delivered a presentation titled "Wanting it All, The Paradox of Providing Both Anonymity and Authentication." Buffard spoke positively about the advances in wireless technology but warned of the costs that come with new security and privacy measures.

Connected device types are becoming more diverse and, as we use more digital services inside and outside of the home, user anonymity is of paramount importance. So does understanding how the collected data will be used. Buffard explained how user data can be anonymized when using services whilst also ensuring user privacy – even when using an encrypted connection that requires authentication. Acknowledging the paradoxical sounding nature of this fact, Buffard stressed the importance of striking the right balance between privacy and security.

Home devices

Buffard pointed to the growth of connected devices in the home, such as smartphones, tablets, and laptops and the many IoT devices being adopted. This growth is driving the requirement for home automation and the challenge to ensure that consumers' digital lives are secure.

Using WhatsApp as an example, Buffard demonstrated the possibility of secure applications that are very popular can keep data secured using end-to-end data encryption that goes beyond data security. The likes of data masking software, encryption systems, hash functions, database pseudonymization, and cloud-based systems pseudonymization are all key to shaping data anonymity.

For the likes of a smartphone or tablet, when the manufacturer gives it a unique device identifier, typically a MAC. When the device connects to a new Wi-Fi network, a data masking approach gives the device a new MAC address.

Authentication is key

Authentication – whether that be password-based, biometric, two-factor, smart card, or token-based – is a crucial step for secure access control and used in a wide range of applications, including online banking.

Authentication ensures that only authorized personnel or systems can access the network infrastructure and resources. One example Buffard highlighted was a friend of a user who would like to share their home Wi-Fi connectivity. While a digital identity is always unique of a digital service, it does not necessarily need to be traceable back to a specific real-life subject.

Significantly, anonymity and privacy can still be guaranteed if the users or devices are authenticated, but all data exchanged between the device and its backend service or the user browsing data are anonymous to the network. This anonymity is guaranteed if the device or the user's browser uses a Secure Channel Protocol (SCP).

Buffard stressed that authentication needs to be protected, however. There have been cases in which authentication can provide anonymity or even be built on tools to protect against impersonation.

Protecting against attacks

Unrestricted network access to IoT devices may enable attackers to interact directly with the device, Buffard warned, which increases the chance of the device being compromised. This underscores the need for a service that puts the consumer in control. There are new opportunities for BSPs to diagnose issues with devices while ensuring privacy, mitigating the need for customer calls to get the issue rectified.

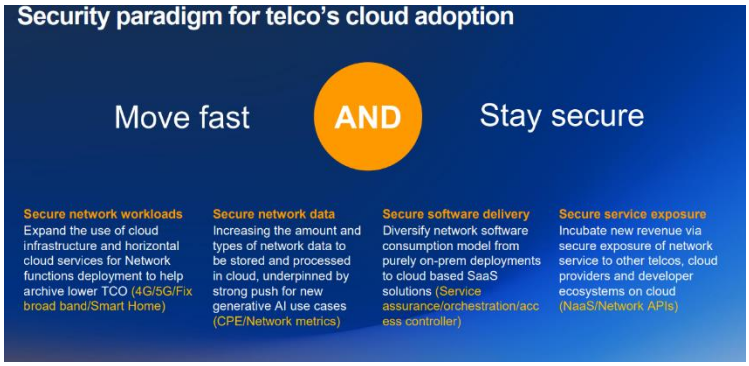
Buffard stressed during the presentation that greater regulations to identify the device and inform the user are needed. And only by correctly securing the device can both authentication and the anonymity of a user be assured, and the right balance struck.

.....

Customer and cloud provider take shared responsibility for security says AWS

A presentation on network and cloud infrastructure security kept eyes and ears attentive as **Owen Law, Principal Solutions Architect Telco at AWS** spoke about the changing security paradigm faced by global telcos and the increasing convergence between cloud and network security.

Law highlighted that while telcos adhere to strict security standards, they are heavily targeted because of the critical connectivity infrastructure they provide towards the likes of key sectors including finance, government, and healthcare. This has resulted in significant investments by telcos in cyber security solutions. He discussed the increasing adoption of cloud by telcos for business agility gains of having more network workloads, network data, service delivery and service exposure platforms. These are driven by leveraging cloud technologies, hence the growing importance of helping telco customers stay secure in the cloud.



Looking ahead, Law recommended the extension of cloud security concepts into the broadband network through open standards and ecosystem collaboration. Engaging different telco authorities on zero trust architecture that do not rely on traditional network controls or perimeters was key and a multi-layer defense-in-depth approach towards broadband network architecture designs should also be considered. Law also stressed the importance of considering security implementations for network analytics and insights, including generative AI. Law echoed sentiments from other speakers on the need for increased industry collaboration to address a clear lack of universal standards for cloud development that are utilized by all telcos.

There is a joint responsibility, Law said, between the customer and the cloud provider. The customer responsibility revolves around the type of cloud services they select, the data they own and controlled, all as part of "security in the cloud", while the cloud provider is responsible for protecting the cloud infrastructure that runs those services as part of "security of the cloud". The customer (telcos in this case) retains full control of their data in the cloud. They can leverage the comprehensive cloud native tools made available to them to encrypt and govern data stored in the cloud, while there remains a strong isolation of customer's data or workload from the underlying infrastructure enabled by cloud systems, such as AWS nitro.

Law also shared use case examples for broadband service providers to apply cloud security design principles to network workloads, especially as they evolve cloud adoption from network data to the management plane, the control plane, and eventually the data plane. He shared how telcos can build a foundation on cloud leveraging the security reference architecture (SRA), such as AWS SRA. An SRA enables strong identity foundation, enabling traceability, applying security at all layers, automating security best practices, and protecting data in transit and at rest. He also shared security implementations for relevant use cases including broadband freedom (cloud-based network analytics for broadband CPE data) and vBNG in hybrid cloud deployment (control and data plane).

.....