SECURE TELECOMMUNICATIONS IN THE AGE OF 5G AND THE IOT

WHY PRIVILEGED ACCESS SECURITY IS KEY TO PROTECTING CRITICAL INFRASTRUCTURE

INTRODUCTION:
CYBERSECURITY IN THE TELECOMMUNICATIONS SECTOR: WITH 5G AND THE IOT, IT'S A NEW DAY WITH NEW RISKS.

Whether you're a communications services provider (CSP) specializing in mobile services, media, or Internet/Web services, the only constant in the industry today is relentless innovation. It's no longer just about the fight to avoid becoming a dumb bit pipe. Sure, that's still a threat. But staying competitive and relevant today requires CSPs to deliver unique business value beyond basic connectivity. The factors undermining established business models are also opening up lucrative new markets and business opportunities for incumbent players. Consider just a few trends and market forces facing CSPs:

The Internet of Everything

Smart cities, smart cars, smart devices—the Internet of Things is transforming markets from transportation and healthcare to retail, shipping, factory management and media.

5G

Transformational mobile bandwidth is coming online at the same time that the IoT is reaching critical mass—the impending disruption will be massive.

Over the Top

Years after Yahoo! Messenger and AOL's AIM came and went, OTT entities keep finding new ways to undermine CSP business models. Just think: As of this writing, the parent company of WeChat, Tencent, has a market cap of ~$450 billion, nearly twice that of Verizon's ~$240 billion.

Vulnerability

Data privacy is a higher priority than ever before: When prominent communications brands like Sony, Verizon, T-Mobile and Facebook have all been implicated in major data breaches, the industry as a whole needs to understand it has a problem on its hands.

75%

Percentage of telcos that expect data breaches to increase.

Source: Ponemon

5G & THE IOT:
THE OPPORTUNITIES ARE REAL, AND POTENTIALLY SPECTACULAR

Disruption

The business priorities for network operators or media companies in the age of 5G / IoT aren't necessarily in harmony with those of device makers, or Internet brands. For instance, there was early consensus that connecting IoT devices like smart vehicles to smart infrastructure via the cloud would be a strong revenue stream for wireless carriers. And sure, smart home device connectivity, V2V (vehicle to vehicle) and V2C (vehicle to cloud) scenarios could still be strong revenue streams, potentially. Yet with every purchase of an Amazon Echo Dot or Google Home Hub, consumer attitudes toward how the IoT will function in their lives get locked in to those brands. CSPs need to deliver value where they can really make a difference.

Playing to Strengths

Once again, as IoT and 5G business models emerge, the nature of the connectivity is almost beside the point. For consumers, the dramatic expansion in bandwidth that will come with 5G isn't likely to inspire an appetite for increased spending on their monthly mobile bill. It will, however, inspire greater media consumption and desire for new experiences, such as streaming video and immersive multimedia. These are definitely opportunities for media providers. Yet, these trends could also provide a huge opportunity for network operators that have the infrastructure in place to support the caching and ad-supported applications that drive these services. CSPs are uniquely positioned to enable these new business models, yet need to be mindful of risks inherent in the data economy.

Emerging Markets for Telecom


Smart Cities & Infrastructure


Connected and Autonomous Vehicles


Streaming Video & Immersive Media


Digital Health Care


Industrial & Agricultural Applications


Virtual Reality

dis·in·ter·me·di·a·tion
/dis,in(t)ərmēdē'āSH(ə)n/

noun

ECONOMICS
1. reduction in the use of intermediaries between producers and consumers.

CSP HEADWINDS

It's an exciting time in the telecommunications sector. Yet established brands need to be realistic about the challenges they face—and it's not just about losing market share to the next What's App or Netflix.

> **Telecom companies are a big target for cyber-attacks because they build, control and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data."**
>
> Source: Deloitte

Stiffening Regulatory Environment

Telecom has long been heavily regulated, with many orgs having deep roots in the sector as national phone traffic carriers, regional cable operators or incumbent broadcast license holders. As communication and media was transformed by mobile devices, DVRs, and wireless broadband, established brands subject to routine oversight by regulatory agencies like the U.S. FCC found themselves competing with startups that didn't have to answer to government very much, if at all. That dynamic began to change as massive data breaches became a regular feature of life in the Internet Age.

Uniquely Vulnerable

CSPs occupy a singular position in the burgeoning data economy. Network operators not only provide foundational connectivity for innumerable other services, they also transmit and store private data for consumers, businesses and government. Data breaches or denial of service attacks on CSPs can reverberate far beyond the initial incident. Moreover, end user equipment—home routers, cellphones manufactured by Apple, Google, Samsung, etc.—are only nominally under CSP control. Easy to compromise, these devices are prime targets for hackers looking to steal data.

The Turn Toward Privacy

The EU's landmark General Data Privacy Regulation rightly gets the bulk of press attention, but momentum is building globally toward stronger protection of individuals' private data, with stark penalties for violations. Many of the world's most prominent telecom brands have been victimized in cyberattacks: Swisscom, Telefonica, AT&T, Deutsche Telekom, Bell Canada and many others. No doubt, telecom brands today need to embrace trust as a competitive differentiator.

OPERATIONAL & SECURITY CHALLENGES IN TELECOMMUNICATION

The many, varied and expanding vulnerabilities in telecommunication infrastructure present a number of risk factors that are potentially far more harmful than the typical privacy breach at a retailer, bank or other consumer-oriented organization. Bad publicity, brand damage and regulatory fines can be very costly, yet a breach at a major retail brand simply does not pose the follow-on impacts that can result from a telecom cyberattack.

Report: The telecommunications industry is among the worst in regard to responding to DNS attacks. 43% of telco organizations suffered from DNS-based malware over the past 12 months, and 81% took three days or more to fix the problem after being notified.

Source: 2018 Global DNS Threat

Vast Geographic Footprint

Telecommunications systems serve as a critical backbone to nations and economies across the globe. In addition, network operators typically maintain extraordinarily diverse legacy equipment infrastructure, with servers, switches, access points and network interfaces from any number of manufacturers. Every day, these systems enable the transmission of financial transactions, business transactions and emergency response communications, and if compromised, the consequences can be dire. Too often, however, access to these systems is left unsecured and unmanaged, putting critical assets at an increased risk of a damaging cyberattack that could impact telecommunications companies and citizens alike.

Priorities: Monitoring & Control

To reduce the risk of potentially damaging unauthorized access to critical telecommunications infrastructure, organizations should tightly control and monitor all internal and third-party user and application access to privileged accounts on these systems. An effective solution will enable telecommunication companies to secure and rotate privileged credentials, proactively secure privileged user sessions and continuously monitor privileged access to detect anomalous activity.

#1 CAUSE OF SECURITY BREACHES: PRIVILEGED ACCESS ABUSE

The Role of Privileged Accounts

Privileged accounts are found in every piece software on a network as well as in many hardware devices, and can provide anyone in possession of a privileged credential with access to and control over sensitive data or critical systems. When used, these accounts permit access to assets such as operator workstations to facilitate automated processes, maintain systems, modify process parameters, and store historical data and other important operations. But in the wrong hands, these accounts can be used to gain unauthorized access to these systems and cause irreparable damage. Yet, some organizations are unaware of the risks that unmanaged privileged accounts pose to the business.

Implications for Telecom Organizations

Privileged accounts and credentials provide superuser access to critical telecommunications infrastructure on-premises, in the cloud and in hybrid environments. To reduce the risk of costly, disruptive damage to these systems, it's critical that companies proactively secure, control and monitor the use of powerful privileged accounts. Remote desktop protocol (RDP) and Virtual Network Computing (VNC) credentials in particular provide cybercriminals with a way to both gain initial entry into networks and move laterally, an essential process for identifying the systems on which malware should be installed.

Privileged accounts, and the access they provide, represent the largest security vulnerabilities an organization faces today. Why are attackers inside and outside the enterprise zeroing in on privileged accounts? Quite simply because privileged accounts are **everywhere** in the telecom technology stack.

- Required for every networked device, database, application, and server on-premises, in cloud environments, and through the DevOps pipeline.
- Used by both human and non-human/machine users, granting all-powerful access to confidential data and systems.
- Have shared administrative access, making their users anonymous.

Compromised privileged accounts and credentials are implicated in the vast majority of cyberattacks.

- Grant too broad access rights, far beyond what is needed for the user to perform their job function.
- Often go unmonitored and unreported and therefore unsecured.

ARE YOU UNDERESTIMATING YOUR LEVEL OF RISK?

- In our recent CyberArk Threat Landscape 2018 Report, we discovered that 89% of IT security professionals recognized that infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured and protected.
- Yet, a good proportion of them indicate that their organization has still not implemented a privileged access security solution to store and manage privileged and/or administrative passwords.
- The 2018 report indicated that enterprises are not doing enough to protect against malware and advanced attacks, but yet 87% of respondents indicated that they still allow users to run with local administrative privileges, which as we all know: most malware requires admin to gain persistence.
- Combining user accounts that are equipped with local administrative capabilities with actual administrative users creates an ever-growing attack surface around privilege accounts.

> “Telecom [organizations] must defend against external attacks involving supervisory control and data acquisition (SCADA) security pertaining to industrial control systems, and telecom equipment security. Device security vulnerabilities are growing, and denial-of-service attacks are a major threat. ‘Always-on’ services and the IoT complicate cybersecurity for telecom companies, especially those providing cloud-based and online services.”
>
> Source: Telecommunications Industry Association

CREATING AN ACTION PLAN

In a cybersecurity program, one of the most effective preventative steps a telecom organization can take is to secure their privileged accounts, credentials and secrets. Cybersecurity decision makers recognize that the process can become complex, especially in large organizations, and securing privileged access is not, unfortunately, a "once and done" activity. Attackers relentlessly look for an organization's vulnerabilities. Consider for example, if an organization secured privileged access a year ago; today they may have new infrastructure, new SaaS applications or applications built using DevOps methodologies, an expanded cloud portfolio, and a data center consolidation in the planning stages. To have the strongest defense against attackers, organizations need to ensure their privileged access security program is up-to-date and continues to protect their most critical infrastructure, applications, customer data, intellectual property and other vital assets.

To proactively reduce the risk posed to privileged access by attackers, telecom companies typically need to:

- Leverage their understanding of the most common types of attacks that exploit privileged access: how does an attacker think and behave in each case to exploit the organization's vulnerabilities?
- Prioritize the most important privileged accounts, credentials and secrets, and identify the potential weaknesses and vulnerabilities in their existing privileged access security program, especially those that could jeopardize critical infrastructure, the organization's crown jewels, etc.
- Determine the most effective actions to close the gap on these weaknesses and potential vulnerabilities. Which actions are the highest priority? What can be achieved quickly vs. requiring a longer-term plan?
- Ensure continuous, reassessment and improvement in privileged access hygiene to address a changing threat environment.

PRIVILEGED CREDENTIALS
THE KEYS TO THE IT KINGDOM

- Privileged credentials are such a critical element in IT operations because they are required to access and unlock privileged accounts, and they're sought out by external attackers and malicious insiders as a way to gain direct access to the heart of the enterprise. As a result, an organization's critical systems and sensitive data are only as secure as the privileged credentials required to access these assets.
- Most organizations today rely on a combination of privileged credentials such as passwords, API keys, certificates, tokens, and SSH keys to authenticate users and systems to privileged accounts. When left unsecured, attackers can compromise these valuable secrets and credentials to gain possession of privileged accounts and use them to advance attacks against organizations. In fact, cybersecurity research shows that the one thing every attacker needs to be successful is access to a privileged account.
- To prevent targeted attacks, protect the keys to the IT kingdom and keep sensitive data away from attackers, organizations must adopt a privileged access security strategy that includes proactive protection and monitoring of all privileged secrets and credentials.

CYBERARK:
THE CYBERSECURITY PARTNER FOR THE TELECOMMUNICATIONS INDUSTRY

CyberArk is the trusted expert in privileged access security. Designed from the ground up for security, the CyberArk Privileged Access Security Solution centralizes and secures privileged account information, enforces least privilege and monitors activity to detect threats. The CyberArk Solution can help telecommunications companies protect internal and cloud-based IT systems, network devices, BSS/OSS systems, and other MIS and NMS systems. Every product in the CyberArk Privileged Access Security Solution is stand-alone and can be managed independently while still sharing resources and data from the common infrastructure. Working together the products provide a complete, secure solution.

Whether you are managing a nationwide mobile network, or running cloud native or traditional applications running on-premises, in the public cloud, or in hybrid environments, CyberArk continues to focus on breaking the privileged access security attack chain. With CyberArk, organizations can stop attackers from stealing data and disrupting operations by blocking the privileged attack pathway. Learn why telecommunications organizations worldwide rely on CyberArk to mitigate the risks of an attack by contacting us or visiting www.cyberark.com.

CyberArk remains the undisputed leader in the privileged access security market. That's why more than half of the Fortune 500 place their trust in CyberArk to protect their most critical and high-value assets. To learn more, visit us at www.cyberark.com.

04.19. Doc. CyberEdge004