TELECOMMUNICATIONS IN A NEW POST-PANDEMIC WORLD:

A FOCUS ON SECURITY SERVICES

Introduction

With the pandemic, where face-to-face communications have been minimized, telecommunications services have become more essential for business continuity, fostering remote work. They have also been instrumental in maintaining personal relationships and providing entertainment during the lockdown.

The impact of telecommunications services can be seen everywhere. As of March 2020, more than 25 percent of US-based adults relied on video calling or online conference systems to participate in work initiatives. Forty two percent of the same cohort relied on the internet for social opportunities during the same time period.[1] The reliance on the internet to support remote work, telemedicine, online learning, and streaming media has skyrocketed.

[1] Coronavirus: impact on online usage in the U.S. – Statistics & Facts, J. Clement, statista, January 8, 2021

Telecom growth: Providing entertainment

The demand for high-speed internet access among consumers has soared.[2] Increased TV and video streaming sees the majority of Americans subscribing to five or more streaming services. Globally, viewing time went up 44 percent in the last three months of 2020, compared to the same period in 2019.[3] In addition to new demands for fast, reliable home-based networks, the pandemic is also accelerating the expansion of mobile networks and satellite internet.

> Almost three-quarters of enterprises (71%) believe the Covid-19 pandemic has accelerated existing digital transformation plans, with 52% signaling greater interest in 5G and the internet of things (IoT), according to research from EY.[4]

Telecom growth: 5G and satellite

In the fastest mobile network deployment ever, analysts project 5G networks to cover about 60 percent of the global population by 2026. By the end of 2020, there were roughly 218 million 5G subscriptions worldwide.[5] Verizon and AT&T have recently spent a combined $68.9 billion to secure licenses for the upper 3GHz band to boost network capacity with mid-band frequencies.[6] Anticipating continuing growth, Apple is already hiring engineers to develop 6G technology.[7]

Likewise, satellite communications are rapidly expanding, as shown by the World Teleport Association, adding ten new members to their current list of 47 members.[8] However, the race to compete in rapidly expanding telecommunications sectors creates a fertile ground for cyber attacks.

---

[2] COVID-19 outlook on the US telecom industry, Deloitte, viewed on February 22, 2021.

[3] Jon Brodkin, AT&T eats a $15.5 billion impairment charge as DirecTV debacle continues, Ars Technica, January 17, 2021.

[4] COVID-19 accelerates interest in 5G, by Joe O'Halloran, Computer Weekly, June 7, 2021

[5] Shara Tibken, 5G will start to live up to its hype in 2021—for real this time, cInet, Dec. 15, 2020.

[6] Jon Brodkin, Verizon and AT&T dominate spectrum auction, spending combined $69 billion, Ars Technica, February 25, 2021.

[7] Mark Gurman, Apple Hiring Engineers to Develop 6G Wireless, Bloomberg Technology, February 18, 2021.

[8] World Teleport Association, WTA Certified Teleports, as viewed on February 19, 2021.

Why rapid growth invites cyber attacks

Before the pandemic struck, telecommunications companies were targets for cyber attacks because they controlled third-party communications and stored large quantities of sensitive customer data.[9] This makes carriers and ISPs prime targets for state-sponsored ATP groups interested in digital espionage, sabotage, and profiting from stolen information.

Espionage

In one threat campaign, hackers compromised the IT environments of over a dozen global telecommunications companies. Attackers stole large quantities of personal and corporate data to gather information about customers in government, law enforcement, and politics for espionage purposes. The threat actors also managed to compromise telecommunications companies' active directory, stealing employee credentials that can be quite useful in further attacks.[10] Espionage attempts can be executed and can manifest in a variety of different ways, including via innocuous-looking avenues.

Between January of 2019 and April of 2020, 5,577 Hulu and Netflix members, among others, were inadvertently exposed to threats when logging onto platforms. These threats included Spy Trojan malware, which could collect personal files and banking login credentials. As a result, billions of pieces of consumer data are now for sale on the dark web.[11] Netflix, Hulu, and other streaming platforms have become prime targets for distributing malware and spam, stealing credentials, and phishing.[12]

In 2018, researchers found that customer credentials were stolen from 42 popular streaming services on the dark web, demonstrating how widespread data breaches are in these platforms. For instance, an attack on AWS enabled hackers to gain unauthorized access to the music-streaming service Mixcloud, which compromised the data of over 20 million users.[13]

Why are attacks succeeding in the telecommunications sector?

---

[9] Global Cyber Executive Briefing Telecommunications, Deloitte, as viewed on February 15, 2021.

[10] Hackers hit telecommunications firms in possible Chinese espionage campaign, researchers say, CNBC, June 25 2019.

[11] Cybercriminals disguising as top streaming services to spread malware, Macy Beyern, TechRepublic, July 16, 2020.

[12] Kaspersky, The Streaming Wars: A Cybercriminal's Perspective, 16 Jul 2020.

[13] Irshivangini on May 21, 2020, Streaming Applications: How to Secure Your Customer Data, Security Boulevard, May 21, 2020.

Sabotage

Beyond espionage, cyber criminals are also intent on sabotaging telecommunications organizations. In 2019, Operation Soft Cell attacked ten cellular networks. Experts assert that the hackers maintained complete control over all ten compromised networks, and could have easily shut them down.[14]

The hackers were "attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more."[15] Theft of this type of information could result in businesses' complete collapse.

Profiting from stolen information

For nation-state backed threat actors, Telecom data represents an intelligence asset. For example, threat actors and their sponsors can glean information concerning where a target lives, and can discern the most effective means of interfering with their day-to-day activities.[16]

Alternatively, cybercriminal groups may elect to sell the data to other criminals via the dark web. Accounts from mobile phone operators may be available for less than $15.00 USD. Criminals may choose to weaponize this data for the purpose of identity theft. For example, forged passports or ID cards represent a common use case.

Stolen information doesn't simply harm isolated individuals; it can also be used to inflict additional damage on companies. Cyber criminals can use stolen login credentials housed in a Telco's database to break into third-party systems. Real-world incidences have occurred. This 'downstream' effect can rupture business relationships and lead to long-term business decline.

So, telecoms know that cyber security and data privacy are paramount. Everyone's committed to mitigating risks. Yet, why aren't we seeing better security outcomes?

[14] Telcos around the world hit by long-term intelligence gathering cyberattack, Dan Swinhoe, CSO, June 25, 2019

[15] Cybereason details operation soft cell: A telco security disaster, Phil Harvey, Light Reason, June 25, 2019

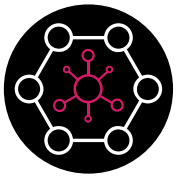
[16] Ibid.

Trends impacting the telecommunications industry

Like many organizations during the pandemic, telecommunications firms have been affected by specific trends. These include:

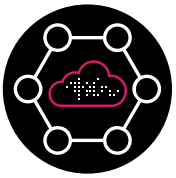
- Cloud migration: Obtain reduced operational and administrative costs, while maintaining unified communication and collaboration
- Remote work: The sudden move from offices to homes created the need for employee's secure remote access from anywhere, everywhere
- Heightened protection: Increased need to protect workloads, apps, APIs, and all interfaces
- Monetization: Firms continuing goal to monetize 5G and CORE network to drive new revenue streams, including security services
- Advanced architecture and technology: A growing need to implement Secure Access Service Edge (SASE), SD-WAN, and Zero Trust
- Cyber pandemic: Responses to elevated cyberattack methods as seen with the SolarWinds supply chain breach and Colonial Pipeline ransomware

Managed security services can include:

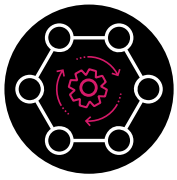


SD-WAN
Secure enterprise branch office SD-WAN connection

Managed Appliances
Hardware-based security outsourcing for all companies



Digital Transformation
Protect enterprises moving to the cloud



IoT
Security solutions for enterprise IoT by vertical

SMB
Managed security for small and medium organizations

The value of managed security service providers

To address the trends cited above, working with or through Managed Security Service Providers (MSSPs) can provide a variety of benefits. It can reduce costs, complexity, and improve outcomes.

What should organizations think about as they consider an MSSP-based approach?

In relation to cost, lower premiums are achieved through consolidation and automation. The simplification of IT infrastructure reduces the number of vendors required for complete protection. AI and machine learning algorithms introduce a high degree of automation, allowing MSSPs to run fast-moving teams that require minimal training.

Organizations that choose to work with MSSPs can select single pane of glass solutions. This architecture requires limited maintenance. Easy, and intuitive management applications also help MSSP solutions and providers punch in above their weight.

Each organization maintains a unique risk appetite. Security may need to be tailored accordingly. Subscribers are demanding advanced architecture that can rapidly prevent, detect and remediate attacks. Customized client-owned, enterprise-managed security controls can help. MSSPs empower organizations to stay on-track and to pursue strategic security solutions.

Competition for market share fuels risk

For telecom organizations, intense market growth comes with intense competition. To deal with fierce competition, money allocated to upgrading cyber security is sometimes diverted to acquiring infrastructure, creating content, and other activities. This renders a business-as-usual approach to cyber security budgeting ineffective. Getting the C-suite on board when it comes to cyber security is key. A strong cyber security posture is no longer a 'nice to have'. At this point, it's a 'must have'.

As telecom organizations race to expand, they often employ vulnerable protocols, complex cloud deployments, and applications that are not rigorously tested for vulnerabilities. Compounding this issue is the fact that DevOps personnel are not primarily accountable for nor fully invested in security. In a survey, nearly 70% of security teams stated that developers balked when it came to remediating bugs. DevOps generally doesn't see itself as playing a role in the maintenance of a larger security framework.[17]

Further, chronic shortages of cyber security staff can leave existing staff members over-worked and under-invested in driving results. This is particularly true when a core member of the staff departs the organization. The average CISO only retains his/her position for three or so years.[18] More junior staff tend to bounce between companies even more frequently. Ensuring solid system management and governance in uncertain staffing situations is challenging in the best of times and can lead to lapses in security.

What are telecommunications organizations supposed to do?

Consolidate security to streamline operations and lower costs

Given corporate, cloud, mobile, SaaS, edge and other IT elements, it takes roughly 60 different security technologies to fully protect today's complex telecommunications environments against sophisticated multi-vector cyber attacks. Implementing this many security controls as standalone solutions creates unacceptable complexity and costs; from procurement to deployment to monitoring, administration, management, and tech support. Using standalone security controls to microsegment your environment in order to create a zero-trust ecosystem is practically impossible.

[17] Who's Responsible for Security? Apparently, I Depends, by Johnathan Hunt, DevOps.com, June 2, 2020

[18] Stop Wasting Money on Cybersecurity, by Jack Danahy, Forbes, December 11, 2020

The answer to reducing costly levels of complexity is to transition from standalone solutions into a consolidated cyber security architecture. Using a consolidated architecture gives your organization a single technology resource that simplifies procurement and tech support. With a consolidated solution, provisioning security engines can be as simple as clicking a button on an interface.

Similarly, having all security controls purpose-built for compatibility prevents any issues during deployments. In addition, security solutions that automatically share threat intelligence throughout the architecture provide much stronger security.

Lastly, being able to monitor, administer and manage all security controls through a single interface reduces the burden on the security staff. Using a single interface for all controls makes security professionals more efficient at delivering adequate security and managing policies—with much fewer staff-hours needed. Consolidated security architecture is the right way to streamline security operations end-to-end especially when you want to microsegment every element in your environment to enforce zero trust.

Conclusion

The proliferation of cyber threats demonstrates the need for telecom organizations to implement top security approaches and tools. Like most large organizations, telecoms are not only responsible for their own security, but are also responsible for the security of their vendors and clients. Keep everyone out of harm's way.

Prevent espionage, sabotage and profit pinching. Leading approaches to data security in the telecom space include MSSP services and security consolidation. You now know the deep benefits associated with these methodologies. Obtain the best security possible to fit your business. Take control over your new normal.

For further information on the benefits of the Check Point Managed Security Services for Service Providers, click here.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com