# Telecommunications Companies: An Interconnected World and Disconnects in Cyber Security

Research shows that telecommunications organizations (telcoms) are facing insidious and extreme cyber security threats. Telcoms are more susceptible to attacks than other industries and need to take action in order to thwart this growing risk.

## Is Your Telecommunications Company Secure Enough?

Cyber criminals perceive telcoms as lucrative businesses to exploit for many reasons. Telcoms are typically at the forefront of technological innovation, implementing the latest networking advancements and infrastructure for their clients. The set-up of new infrastructures at scale can lead to security loopholes that hackers can easily exploit.

In addition, the biggest telcoms have valuable B2B and B2C clients whose data can sell for a high price on the dark web. After the data sells, the buyer will likely capitalize on the information to break into telcom clients' networks. This is an example of the domino effect.[1]

## Fierce Cyber Attacks can Have Fatal Consequences

In a cyber attack that targets telcoms, a network or system can fail. If that occurs, entire government agencies may be affected. The most sophisticated of telcom-focused cyber attacks could lead to the exposure of sensitive military details. In the wrong hands, information extracted from telcoms' systems could precipitate international political incidents. No organization wants to own responsibility for scandals that play out on the world' stage.

In addition, an average cyber attack can cost telcoms over a million dollars in associated remediation fees; a hefty price tag. If one large attack causes extreme damage, or if multiple attacks occur successively, the business could plunge into the red. In extreme circumstances, the business could be forced to fold altogether.

### The Top Attack Types that Telecommunications Companies Typically See?

- 43% of telcoms report experiencing Domain Name System (DNS) malware-based attacks.[2]
- 74% of telcoms witnessed attacks against employees, including C-level executives.[3]
- DDoS attacks have increased by 16% worldwide this year, and telcoms are the most among the most common targets.[4]

---

[1] How to Avoid the Domino Effect, Cyber Talk, 8 May 2019

[2] Over 40% of Telecoms Suffered DNS Attack in Past 12 Months, Business Insurance, 23 November, 2018

[3] Telecom Corporate Accounts at Highest Risk for Cyber Attacks, CPO Magazine, Bob Lyle, 8 October 2020

[4] 16 DDoS Attacks Take Place Every 60 Seconds, Rates Reach 622 Gbps, ZDnet, Charlie Osborne, 18 February 2020

- Millions of bots launch attacks across the internet everyday, and a large volume of them take aim at telcoms.
- Espionage attempts from foreign groups.
- Ransomware schemes are rising. Telcom-focused ransomware attackers recently demanded $7.5 million in Monero cryptocurrency in exchange for releasing a telcom's data.[5]

## Navigating Cyber Security in the Telecommunications Space

Cyber criminals' techniques are evolving at breakneck speed, but cyber security is evolving even faster. Cyber security professionals agree that industry advances are noticeably enhancing cyber resilience. Nonetheless, strategies grow outdated quickly, and now is the perfect time to review your efforts and their effects on your organization's cyber security posture. *Your organization will want to pursue a multi-pronged approach to achieve exceptional protection.*

Start with besting the basics. Be sure that you're really blocking as many Gen V and Gen VI threats as possible. One of the top telcoms in the US recently asserted that the company needed to improve visibility into their network systems, to increase the ease of use when it came to their tools, and to upgrade their attack prevention methodology. Making these simple measures into priorities can dramatically improve your organization's cyber resilience.

Then, take an innovative approach. In the last three years, the number of technology leaders who spend 20 percent or more of their budgets on advanced technology investments has doubled. Eighty-four percent of organizations are investing in machine learning, artificial intelligence or robotic process automation-related cyber security tools.[6] These types of investments make sense financially, as they can instantly alert teams to any issues.

Reconsider your cloud based application management. Telcoms commonly use multiple cloud products, some of which are made available to customers, while others of which may only remain available internally. This makes cloud management complex. Cyber security solutions with multi-tenant features enable you to manage cloud security in whatever way makes sense for your business.

Support systems with automatic updates. Ensure that your organization works with a cyber security vendor that can configure automatic updates for your systems. Also ensure that you're able to see newly downloaded protections. This will assist you in staying secure.

All of these approaches will help you orchestrate exceptional cyber security results and can keep your organization safe.

If you're interested in learning more about security for telcoms, please reach out to your local Check Point sales representative or connect with us here.

[5] Argentine Telecom Falls Victim to $7.5M Monero Ransomware Attack, CoinTelegraph, Felipe Erazo, 20 July 2020

[6] Third Annual State of Cyber Resilience, Innovate for Cyber Resilience, Accenture