99.99

The Four Nines Project

Cybersecurity for Teleport & Satellite Operators

World Teleport Association
www.worldteleport.org

Teleport operators and software providers share insights into the need for cybersecurity and the methods and technology in use to provide it.

July 22, 2015

US$1,650, free for WTA members

Contents

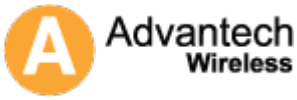
***Cybersecurity for Teleport & Satellite Operators* is made possible by the generous support of**

DataPath specializes in advanced remote communications, networking and IT solutions tailored to the unique requirements of aerospace, broadcast, government, and infrastructure clients. The company's products include a range of both custom and commercial off-the-shelf field communications and information technology products, including satellite communication systems, network management software, and cybersecurity services. All of DataPath's offerings are backed by 24x7 customer care and global field support. For more information, visit www.datapath.com.

***Cybersecurity for Teleport & Satellite Operators* is also made possible by the financial support of WTA's Industry Leaders…**

arqiva

…And Industry Patrons:



Foreword

By David Myers, President & CEO, DataPath

Without a doubt, cybersecurity is the biggest issue facing today's CIOs and IT departments in organizations large and small across virtually every industry. For even for the most IT savvy organizations, figuring out what is needed to prevent a cyberattack, or how to respond when an attack does occur, can be truly daunting. And for the satellite communications industry and its teleport operators, the challenge is compounded by the unique "over the air" technologies employed in these mission critical networks.

The threat of cyber incidents is growing every day, and the forms in which they manifest are constantly evolving. Protecting your communications network requires vigilance. Satellite network and teleport operators should be asking themselves some key questions like:

- *What does a good cybersecurity plan look like?*
- *How do I implement a cybersecurity solution tailored to my unique environment?*
- *How do I ensure my network and my clients are protected for the long-term?*
- *How do I minimize the time, cost and complexity of cybersecurity?*
- *How do I respond when (not if) an incident does occur?*

If you don't have clearly defined answers to questions like these, then your network may not prepared for the unexpected.

One thing is certain: technology alone cannot solve the problem. A comprehensive cybersecurity strategy must include vulnerability assessments, risk mitigation techniques, incident response procedures, and internal and external communications plans. Most importantly, it requires an ongoing commitment and investment in the overall security and health of your network.

Not every network environment has the same vulnerabilities or security requirements. As a result not all cybersecurity solutions are created equal. It is one thing to develop a security plan to protect a corporate network or healthcare data or credit card payment process. However, mission critical telecommunications networks, especially those that employ satellite and fixed wireless technologies, have very different needs. Today almost anything can be IP addressable, and is therefore a potential vulnerability access point – from a transmitter on a cell phone tower to the modem used in a satellite network to the sensors or security cameras at an unmanned utility site. Protecting networks with carrier grade telecommunications equipment or industry specific sensor data collection systems requires unique expertise.

Satellite networks play a critical role in how we communicate as a society. For military operations, broadcasters, disaster relief missions, oil and gas mining, and others operating in remote or harsh environments, reliable and secure communications systems are critical – not only to supporting the mission, but to ensuring the safety of personnel in the field.

At DataPath we are proud to be developing, tools, services and even complete solutions in cybersecurity that are specifically tailored to the unique challenges of satellite and wireless communications networks. This World Teleport Association (WTA) report helps bring to light many of the challenges and concerns that impact the safety and security of today's satellite networks. We hope that you will find it both insightful and thought provoking, but perhaps more importantly, we hope it we help all of us in the industry raise the bar on security for satellite based communications.

Introduction

"What's your cybersecurity plan?" It is a question that some teleport and satellite operators would prefer not to hear from their customers, because it is an area where many of them are still playing catch-up. In the last decade, teleports have become data centers with connections to the digital skyway as well as information highway. Satellite is a unique environment and securing it requires knowledge and skills beyond those typically found in terrestrial IT and telecommunications.

In *Cybersecurity for Teleport and Satellite Operations*, WTA shares the insights of technology executives on both the operator and vendor sides of the fence about the current state of cybersecurity for teleports and satellite operators. It identifies the major risks, assesses how well the industry believes it is coping with them, and identifies best practices in securing the digital and physical infrastructure of the "data center with antennas" that teleports have become.

Methodology

Through interviews with the senior executives of technology firms, teleport and satellite operators, *Cybersecurity for Teleport and Satellite Operations* investigates themes including:

- Cybersecurity risks faced by teleport and satellite operators, both those common to digital networks and those unique to satellite communications
- Changes in technology, the market or customer requirements that increase those risks
- How operators are managing risks, and reassuring customers about the security of their data
- Technologies and procedures that operators are finding most valuable in tackling security issues
- Security as a marketing, sales and management issue

Acknowledgments

WTA thanks the following individuals for contributing their time and expertise to the project:

Denis Onuoha
Head of Information Security
Arqiva, UK

Hank Huijzer
CTO
Castor Networks, Netherlands

Peggy Rowe
VP Software and Cyber Solutions
DataPath, USA

Jeremy Bargainnier
Senior Manager, Cybersecurity Solutions,
DataPath, USA

Alan Young
Chief Technology Officer
Encompass, USA

Scott Herschander
VP, Information Technology
Globecomm, USA

Tim Berdon
VP, Corporate Software Application Innovation
Globecomm, USA

Jeff Winkler
Senior Director Information Assurance
Globecomm, USA

Alan Benitez
Senior Scientist
Globecomm, USA

Andy Lucas
CTO
Harris Caprock, UK

Richard Harding
Operations Director
OnLime, Germany

Chris Meulman
Exec. Director for Product & Innovation
Optus, Australia

Ziv Mor
CTO & VP, Business Development
RR Media, Israel

Oded Shor
IT Manager
RR Media, Israel

Shai Barfy
Network Engineering Manager
RR Media, Israel

David Cohen Yehuda
Network & Security Engineer
RR Media, Israel

Matthias Riede
CTO
Signalhorn, Germany

Istvan Rabai
Manager, IP Networks
Signalhorn, Germany

Yves du Sault
Marketing Director
Sonema, Monaco

Executive Summary

What are the Risks?

In recent years, cybersecurity breaches have garnered a great deal of news coverage. No one is immune, it seems: governments, banks, retailers and broadcasters have all been hacked.

The greatest amount of time, energy and investment, according to the teleport operators we interviewed, goes into defending against cybersecurity risks that are common to all networks. Historically denial of service (DoS) has been the most common issue. The other threats are malware that distributes viruses across systems, and targeted hacking to steal information.

Satellites do, however, present their own unique vulnerabilities, since they send their signals through air and space. That creates the potential for anyone in the footprint with the appropriate skill and equipment to interfere with the RF signal in the satellite equivalent of a DoS attack.

A signal moving between satellite and terrestrial traverses a substantial chain of equipment at the teleport, most of which has been IP-enabled so that it can be remotely controlled over a standard data network. If control of these devices takes place over the teleport's internal network, and that network connects to the Internet, it creates the possibility for unauthorized users from outside to take control.

Who is the Adversary?

Cybersecurity risks arise from the actions of adversaries both far and near, some of whom are not even adversaries in the conventional sense:

- Competing Governments and Corporations
- Criminals
- Disgruntled employees
- All other employees, who may inadvertently let intruders into the network

All of the operators we interviewed stressed the importance of training everyone in the organization – from the receptionist onwards – on the importance of safeguarding data, recognizing phishing emails and telephone calls and not disclosing passwords.

How Concerned Should You Be?

All of the operators reported concerns about the security of their networks and protection from cyberattacks. How proactive they are, however, varies widely with the size of the company and budget constraints.

Respondents' reports on the level of cybersecurity concern among customers varied widely. High profile customers have greater concern. The most concerned customers are those in the government sector and organizations that are responsible for monetary transactions. Commercial maritime and oil and gas are other sectors where security concerns are typically high.

How Do You Deal with the Risks?

For most teleport and satellite operators, cybersecurity remains the responsibility of the engineering and operations departments. The amount of time dedicated to network protection and cyber defense varies from full-time to part-time to incident response only.

Some of the larger global operators have internal groups audit their networks annually, or even more frequently, and have internal Information Security staff.

Small to midsize operators with lower budgets may appoint an operations or engineering executive to serve as the point person on cybersecurity. Smaller companies tend not to audit their own systems or have staff dedicated to cybersecurity, despite having the same concerns as the larger organizations. As a substitute, they may work to comply with accepted industry standards. Many companies choose to outsource their network security to experts in the field.

Procedures & Best Practices

Most respondents were quick to point out that technology alone is not the answer. As one put it, "management buy-in, training, practice, ownership of the process and vigilance are the most valuable aspects of a cybersecurity assessment and mitigation strategy."

Best Practices include:

- Vulnerability Testing
- Internal Information Security Specialists
- Outsourced Cybersecurity Services
- Achieving ISO 27000 certification

Technology Recommendations

Firewalls are the first line of defense for most of the operators. In addition to the firewalls themselves, provided by companies from Microsoft to Cisco, several operators mentioned using add-ons solutions to help bolster system security and monitor outages and usage.

Strong authentication controls that force periodic password updates and centralized management systems are also used by many operators. Many organizations are also applying other tools to catch viruses, worms and spyware that firewalls, guarding the network edge, can miss.

What Should We Expect in Future?

Nearly every respondent cited the move to IP and the cloud as a major concern. This increased connectivity between systems and users, makes it easier for malware and viruses to spread and harder for the operators to isolate an attack.

Responding to an increasingly dangerous cyber world would be easier if customers put a consistently high value on cybersecurity and were willing to pay for it. One topic that everyone agrees on: cybersecurity is going to become a more dominant issue in the future. The Internet of Things (IoT) is not going to make life any easier.

There are also signs that satellite networks may not remain exempt for long. In 2013 a network security company called IOActive set out to test a selection of widely deployed satellite terminals. Its report described multiple vulnerabilities in all the devices tested. In the future as today, vigilance and education will be the key to protecting the satellite network from cyber threats.

About the Report


van Herck


Tweedie


Bell

Cybersecurity for Teleport Operators was developed under the direction of WTA's Research Committee, led by Serge van Herck, CEO of Newtec. Elisabeth Tweedie of Definitive Direction conducted the interviews and wrote the report, which was edited by WTA Executive Director Robert Bell.

About the World Teleport Association

Since 1985, the World Teleport Association (WTA) has focused on improving the business of satellite communications from the ground up. At the core of its membership are the world's most innovative operators of teleports, from independents to multinationals, niche service providers to global carriers. WTA is dedicated to advocating for the interests of teleport operators in the global telecommunications market and promoting excellence in teleport business practice, technology and operations. Members benefit from the opportunity to:

- *Collaborate for Mutual Benefit*, from maintaining a level playing field for competition to implementing management practices that reduce costs.
- *Network Within the Sector*, to identify business opportunities, strategic partners and market insights.
- *Improve Their Global Profile*, through WTA-hosted events, listings in WTA's buyer's guide and placement in WTA's publications.
- *Raise Their Competitive Game* with free access to WTA research, white papers and market studies.

World Teleport Association
+1 212-825-0218 wta@worldteleport.org www.worldteleport.org