

# Cybersecurity for Service Providers

Alexandro Fernandez, CISSP, CISA, CISM, CEH, ECSA, ISO 27001LA, ISO 27001 LI, ITILv3, COBIT5  
Security Advanced Services  
February 2018

“There are two types of companies: those that have been hacked, and those who don't know they have been hacked”

John Chambers



# All Data has Monetary Value



## Welcome to the Hackers' Economy

# It's a Complex World

## The world has gone mobile

Changing  
Customer  
Expectations

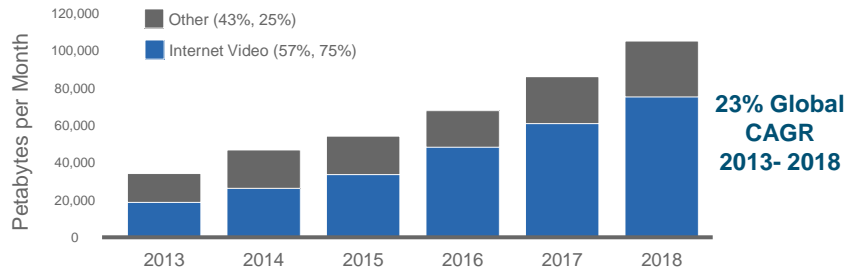


**10X Mobile Traffic Growth  
From 2013-2019**



**Ubiquitous Access  
to Apps & Services**

## Traffic growth, driven by video



## Rise of cloud computing

Soon to  
Change SP  
Architectures/  
Service  
Delivery



**Changing Enterprise  
Business Models  
*Efficiency & Capacity***

## Machine-to-Machine

Emergence of the Internet of Things



People



Process



Data



Things

# Shift to 5G Will Be Led by New Services

Ultra Reliability  
(Wherever + Whenever)

Ultra Capacity  
and Coverage

Ultra High-Speed  
(up to 10 Gbps to cell site)

Ultra Low Latency  
(1 ms End-to-End)

Massive Device  
Connectivity

Broadband access  
in dense areas



Pervasive Video

Broadband access  
everywhere



Average 1 Gbps per  
device

Higher  
user mobility



High Speed Train

Massive  
Internet of Things



Sensor Networks

Extreme real-time  
communications



Tactile Internet

Lifeline communications



Natural Disaster

Ultra-reliable  
communications



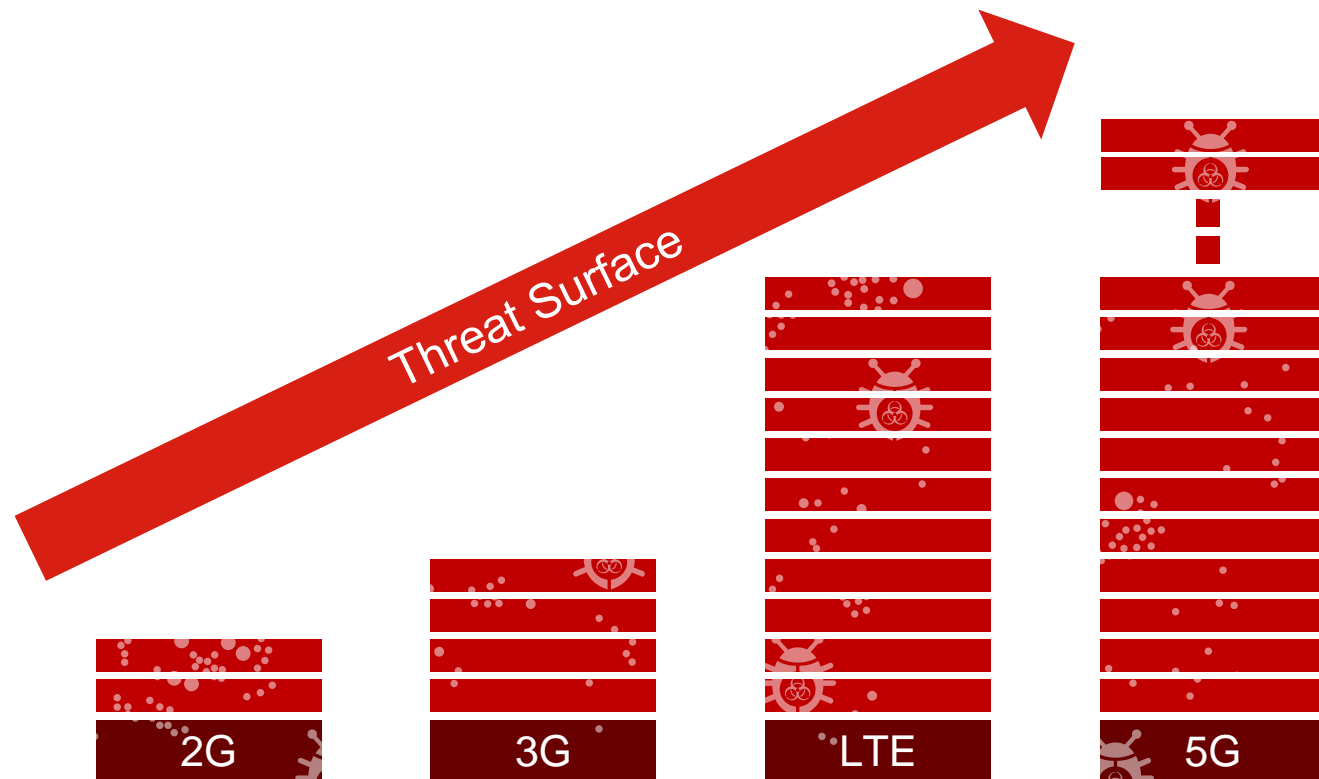
E-Health Services

Broadcast-like services



Broadcast  
Services

# New Services Mean New Threats



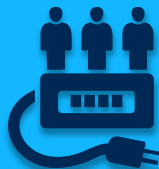
# SP Common Security Threats



**Denial Of Service**



**Ransomware**



**Third Party Security**



**IoT / IoE**



**Segmentation  
Issues**



**Phishing**



**Theft of service /  
Fraud**



**Credential Theft  
and Exposure**



**Malware /  
Botnets**



**Known  
Vulnerabilities**

# Cellular SP Unique Security Threats



**Services** - (e.g. Web, Messaging, Voice, Video vulnerabilities)



**Core** – (e.g. compromise of hosts in Packet Switched Routing, Billing and Accounting)



**Access** – (e.g. RAN protocol abuse)



**Devices** — (e.g. Service bypass for Mobile Devices, Laptops)





# Service Providers Facing Unique Security Challenges

# Overcome Changing Market Dynamics



Need for New Revenue Streams  
A constant security threat is the  
new normal  
Laws & Regulations

## Challenges

Security Operation Center  
Advisory Services  
Compliance services

## Solutions

Incorporate new technology  
security into your network for  
efficiencies and cost savings  
Maintain compliance

## Benefits

# Lead the Innovation Race



Security implications for new technology like 5G are different than LTE

Services are now built in the cloud in minutes vs months

## Challenges

Cloud and IoT Security Strategy

Mobile Network Breakout Assessment

Application Security and Penetration Testing

## Solutions

Build security into the foundation of your services and environment

Understand where your security gaps are so you can make risk-based decisions

## Benefits

# Scale Security for Cost Reduction



Silo's organizational structure can lead to poor security hygiene

Number of security products and vendors in the SP environment is exponentially larger

## Challenges



Service Provider Cybersecurity Maturity Program Assessment

Infrastructure Architecture Assessment

FW Migration / IDS Tuning

## Solutions



Reduce overall security costs with strategic investments

Improve visibility across your network

## Benefits

# Lack of Security Experts



Cybersecurity talent shortage  
leads to a need for automation of  
many security tasks

No amount of personnel can  
watch the SP environment

## Challenges

Security Advanced Services  
Breach Incident Response and  
Retainer  
DDOS Implementation

## Solutions

Free up staff to focus on strategic  
objectives like growth  
Improve response readiness to  
incident breaches

## Benefits

The background is a dynamic, abstract digital composition. It features a deep blue color palette with vibrant, glowing light trails in shades of cyan and magenta that sweep across the frame. Overlaid on these are complex wireframe structures, resembling architectural blueprints or data networks, rendered in a lighter blue. A bright, circular light source on the right side creates a strong lens flare effect, illuminating the surrounding elements. The overall aesthetic is futuristic and high-tech, suggesting themes of innovation, technology, and digital transformation.

How can we help your  
organization?



# Advanced Security Services for SP



- **Security Program and Strategy**
- **SP Segmentation Strategy**
- **5G Readiness Services**



- **Red Teaming for SP's**
- **Incident Response and DDOS**
- **Network Assessment & Hardening**
- **Theft of Service**



- **SP Security Architecture Assessment**
- **Software & Application Security**
- **Core Network Security Assessment**



- **Network Breakout Assessment**
- **End-Point / Subscriber / Customer Security Assessment**
- **Protocol & Signaling Assessment**



- **Security Operation Center**
  - SOC Strategy and Planning
  - SOC Assessment and Benchmarking
  - SOC Implementation
  - SOC for MSSP

# Mobile Provider



## Challenge/Objectives

- Requirement to provide security across cellular network and supporting applications
- PCI Compliance
- Corporate protection of sensitive internal and customer data
- Unknown agent security posture
- Required support for incident response

## Solutions

- Developed and supported delivery of application penetration testing program
- Supported design of PCI compliance strategy
- Performed security program and control gap assessment
- Performed security assessment across independent agents
- Provided incident response services

## Customer Benefit

**Reduction** of network and customer facing application security vulnerabilities

**Achieved** PCI compliance

**Understanding** of network, corporate and agent security risks



# Global Technology Provider



## Challenge/Objectives

Multiple vendor assessment programs

Ineffective prioritization and remediation for vendor risks

Bandwidth challenges had limited the number of assessments

## Solutions

Piloted vendor assessment program including program management

Conduct 30+ assessments per year

Improved program processes, assessment, executive metrics, and program governance

## Customer Benefit

**Greater** management transparency to vendor risks

**Annual** assessments and summary metrics across all programs

**Continuous** improvement in program and assessment efficacy



**Thank You**

**The new wave of threats requires....  
a new wave of **Cybersecurity****