

Well-Ahead Rural Health Workshop: Cybersecurity Hygiene & Digital Vaccine

27 June 2025

//Jtan the Cybersecurity Man



Agenda

- About Me
 - Verizon Data Breach Investigations Report Summary
 - High level cyber risks in the Healthcare Sector
 - Specific cyber risks in the Healthcare Sector
 - Overview of the Communications Sector (you're dependent upon)
 - Healthcare and Cybersecurity parallels and analogies
 - Cybersecurity is a Business Problem
 - Cybersecurity Maturity Strategies
 - History and comparison of the CISO and vCISO Roles
 - vCISO vendors in Louisiana
 - Free resources – CISA/InfraGard/LASG Cyber Reserve
 - Call to Action – Cybersecurity is a Safety Problem Too!
-





About JTan

Joshua (JTan) Tannehill, CISSP ✓ He/Him · 1st
 Brand Ambassador @ Coretechs, Owner @ JTan, LLC, Commander @ Louisiana State Guard Cyber Reserve, President @ Louisiana Chapter of Cloud Security Alliance, VP & Comm Sector Chief @ Louisiana Chapter of InfraGard

Lake Charles, Louisiana, United States · [Contact info](#)

Louisiana State Guard
 Community College of the Air Force



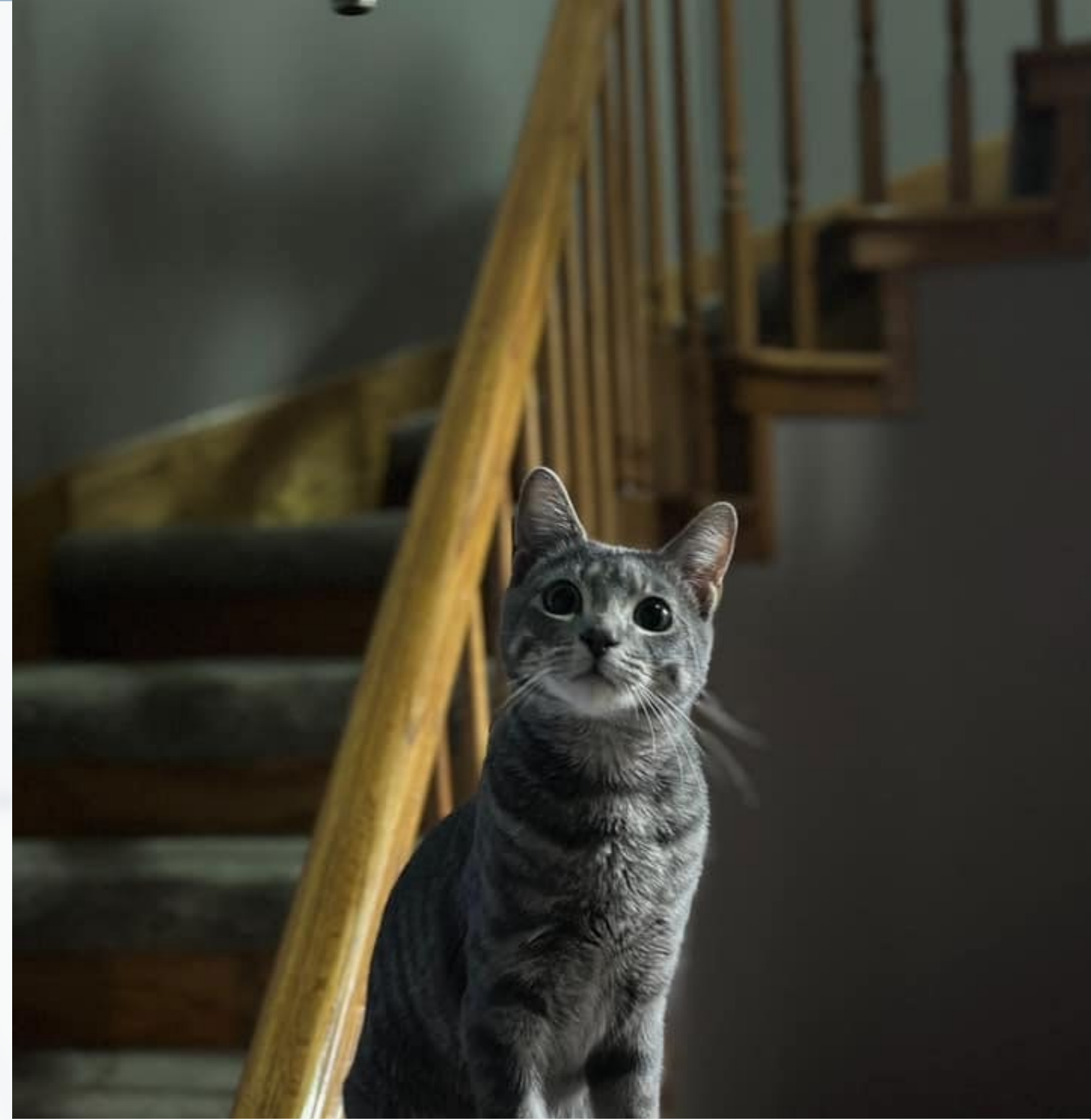
Dad JOKE



PLEASE wait...

A kitten was born in my roof in July 2023. She was later named "Eve".

Anyone know what her favorite color is?



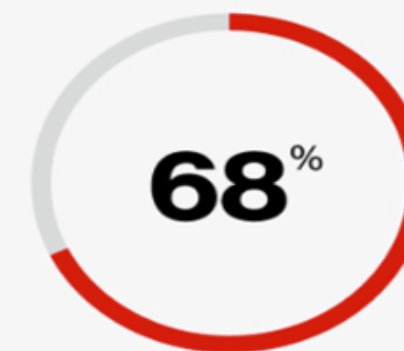
Cybersecurity Threat Brief

Top takeaways

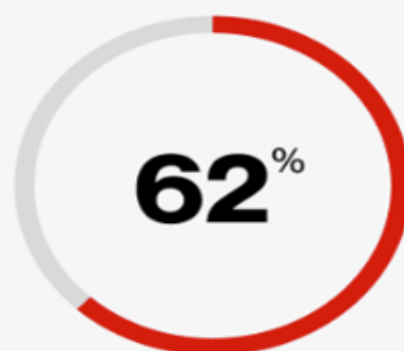
Explore a preview of some of the cybersecurity data uncovered by this year's DBIR.



of breaches involved the exploitation of vulnerabilities as an initial access step, almost triple the amount from last year's report



of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error



of financially motivated incidents involved ransomware or extortion, with a median loss of \$46,000 per breach



of breaches involved a third party or supplier, such as software supply chains, hosting partner infrastructures or data custodians



IT Risks in the Healthcare Sector

Common Threats:

Ransomware attacks: Encrypt patient data and demand ransom for access.

Phishing and social engineering: Target staff to gain credentials.

Malware and zero-day vulnerabilities: Exploit outdated systems.

Consequences:

Loss of patient trust.

Legal penalties under HIPAA or GDPR.

Operational disruption, especially in emergencies.



IT Risks in the Healthcare Sector continued...

Insider Threats

- **Malicious insiders:** Employees stealing or leaking data.
- **Negligent users:** Improper handling of data or weak passwords.
- **Unsecured devices:** Shadow IT/Shadow AI: Use of personal devices or failure to encrypt data.



IT Risks in the Healthcare Sector continued...

System Downtime and Availability Risks

- **EHR system failures:** Interruptions can delay critical care.
- **Network outages:** Affect access to cloud services, telemedicine, or internal systems.
- **Single point of failure:** Poor system design leading to total shutdown during an incident.

Compliance and Regulatory Risks

- **HIPAA (US):** Non-compliance leads to fines and reputational damage.
- **Audit failures:** Inadequate logging and monitoring can lead to failed inspections.



IT Risks in the Healthcare Sector continued...

Outdated or Unsupported Technologies

Legacy systems: Often unpatched and incompatible with modern security tools.

Unsupported software: No longer receives security updates.

Poor Identity and Access Management (IAM)

Overprivileged access: Increases risk of misuse or accidental exposure.

Lack of MFA (Multi-Factor Authentication): Easier to compromise credentials.

Lack of Incident Response Planning

Unpreparedness: Delayed response to data breaches or IT failures.

Inadequate staff training: Staff may not recognize or report incidents promptly.

Medical Device Vulnerabilities

Connected devices (IoMT): Infusion pumps, pacemakers, etc., often lack robust security.

Remote management risks: Misconfigurations or outdated firmware.

Data Integrity and Accuracy Risks

Corrupted or altered patient records: Lead to incorrect treatment decisions.

Improper system integration: Data inconsistencies across platforms.



Emerging Trends and Threats

- **AI-enabled attacks:** Smarter malware capable of evading traditional detection.
- **Supply chain compromises:** Tampering with embedded systems or control components. Segue to Comm Sector Threats





**VP and Communications Sector Chief,
Louisiana Chapter of InfraGard**



Communications Sector Overview

The Communications Sector is closely linked to other sectors, including:

- The [Energy Sector](#), which provides power to run cellular towers, central offices, and other critical communications facilities and also relies on communications to aid in monitoring and controlling the delivery of electricity.
- The [Information Technology Sector](#), which provides critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communications to deliver and distribute applications and services.
- The [Financial Services Sector](#), which relies on communications for the transmission of transactions and operations of financial markets.
- The [Emergency Services Sector](#), which depends on communications for directing resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls.
- The [Transportation Systems Sector](#), which provides the diesel fuel needed to power backup generators and relies on communications to monitor and control the flow of ground, sea, and air traffic.



Emerging Trends and Threats

Communications Network Architecture: Access Networks



BROADCASTING

There are more than 14,000 radio and 1,700 television broadcasting facilities in the United States, sending broadcasts through the air to a frequency network of transmitters.

TV and Radio
One-to-Many, highly survivable



CABLE

The cable industry is composed of approximately 7,791 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

Often provides data networks and "backhaul" for cellular services



WIRELESS

Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

Not "just" modern cellular (4G & 5G)
Includes land mobile radio & microwave



WIRELINE

Over 1,000 companies offer wireline, facilities-based communications services in the United States. Wireline companies serve as the backbone of the Internet.

Modern fiber-optic & backhaul
Legacy copper –voice, DSL



SATELLITE

Satellite communications systems deliver advanced data, voice, and video communications, transmitting data from one point on the Earth to another.

Rapidly evolving – e.g., cube sats
Survivable and good in remote areas
Much lower bandwidth than fiber

Communications Sector Risk Profile

Communications Sector Risk Profile

Natural Disasters and Extreme Weather



Hurricanes, wildfires, and other extreme weather events have increased in frequency and severity in recent years, impacting local and regional communications infrastructure in the United States. On a national level, a geomagnetic solar super storm, such as the one in July 2012, could cause an electromagnetic pulse that collapses electric power grids and triggers a long-term outage (LTO) in national communications.⁹

⁸ These risks were assessed in the 2012 NSRA.

⁹ Information about the July 2012 solar super storm is available at the following URL: http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/. Accessed December 2, 2015.

Communications Sector Risk Profile

Supply Chain Vulnerabilities



The Communications Sector depends on suppliers for the products and services that are necessary to deliver communication services to users. In particular, the sector is dependent on reliable hardware and software. This is an area the sector continues to scrutinize closely.

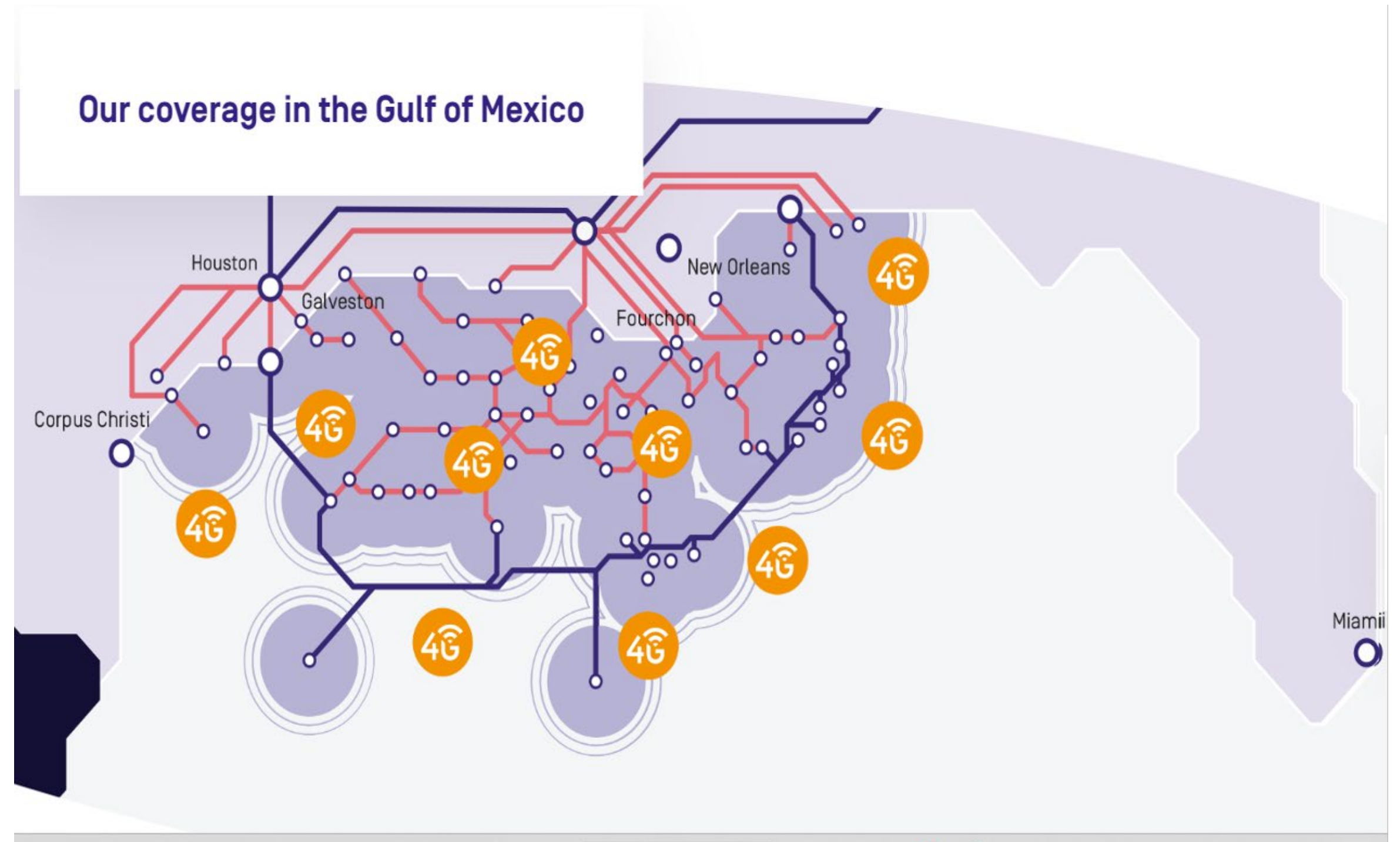
Communications Sector Risk Profile

Cyber Vulnerabilities



The Internet is a complex ecosystem comprising suppliers, networks, and service providers, all of whom are part of the Communications Sector. Any vulnerabilities or threats to functions and capabilities outside of the Communications Sector (e.g., hardware, software, and operating systems) have the potential to affect network provider services and, therefore, require ongoing attention.

Communications Sector Risk Profile



Communications Sector Risk Profile

The Global Internet Is Being Attacked by Sharks, Google Confirms

BY WILL OREMUS AUG 15, 2014 • 3:23 PM



Sharks' attraction to undersea fiber-optic cables has been well-documented over the years.

Screenshot / YouTube

Healthcare & Cybersecurity parallels & analogies

1. Prevention Over Cure

- *Medical hygiene* prevents infections (like handwashing to stop the spread of germs)
- *Cyber hygiene* prevents breaches (like using firewalls and software patches/updates to block cyber threats)

2. Routine Practices

- Brushing your teeth or disinfecting surfaces = installing updates or scanning for malware
 - Daily, small habits build long-term resilience
-

Healthcare & Cybersecurity parallels & analogies

3. Protecting Systems

- In medicine: your immune system, organs, and well-being
- In cybersecurity: your data, networks, devices, and digital identity

4. Risk Awareness

- Both involve **recognizing threats early**—be it a contagious virus or a phishing link
 - Education plays a huge role in staying informed and protected
-

Healthcare & Cybersecurity parallels & analogies

5. Contagion is Real

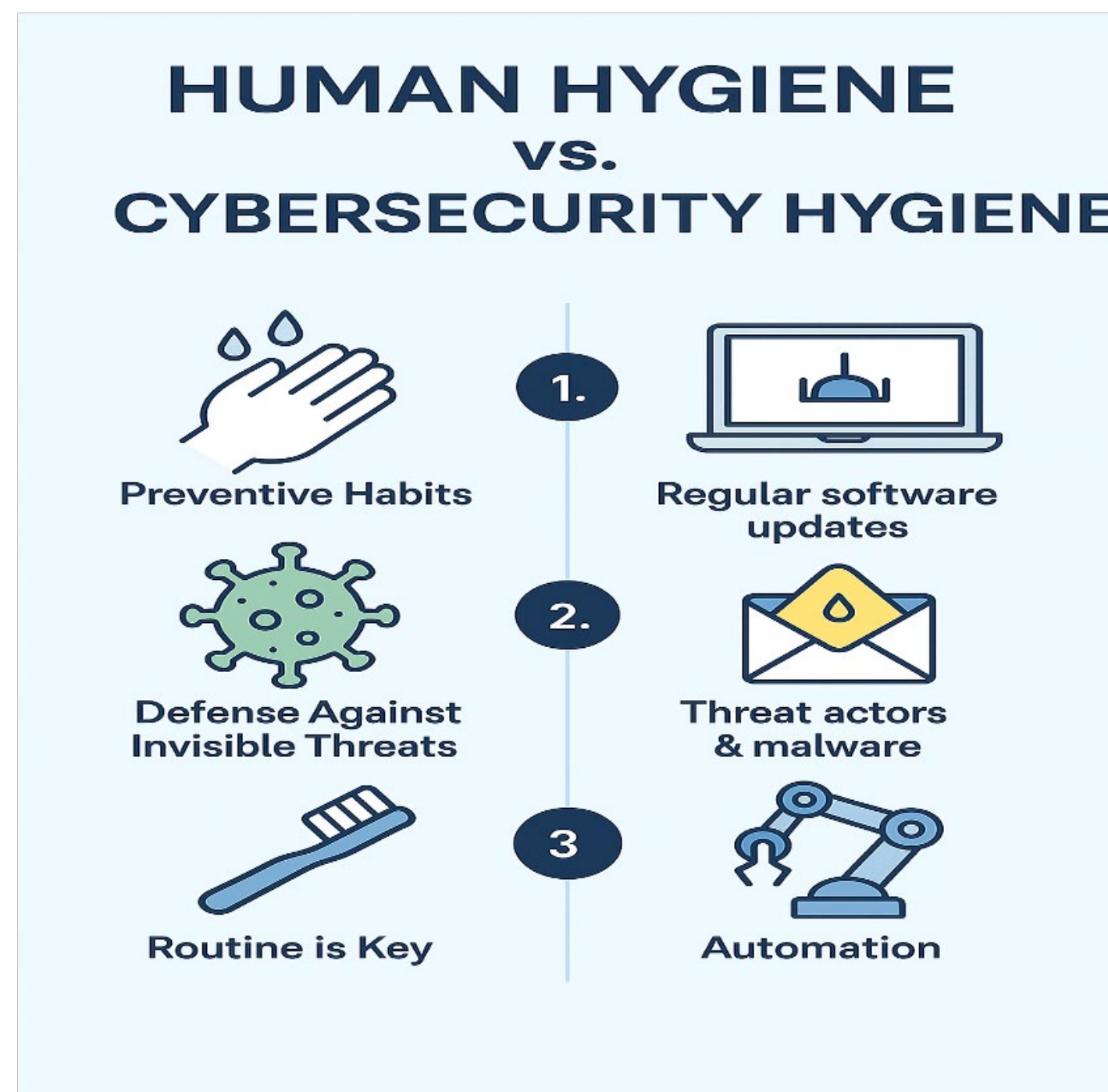
- A virus can spread through populations—or through a network
- Poor hygiene (digital or physical) doesn't just affect you—it puts others at risk too

6. Defense in Layers

- In medicine, that might mean hand hygiene *and* vaccines *and* PPE
 - In cybersecurity, it's antivirus *plus* secure passwords *plus* multi-factor authentication
-

Healthcare & Cybersecurity parallels & analogies

- Both types of hygiene are about **minimizing exposure**, **building resilience**, and **protecting critical assets**—whether that’s a human body or a digital infrastructure.



Cybersecurity Maturity Strategies

Cybersecurity Awareness

Training

A mature cybersecurity awareness program will help you avoid human error as well as lower your cybersecurity insurance monthly premiums



MSSP/vCISO

A vCISO or an MSSP partner can help you implement and verify appropriate hardening measures and mature your cybersecurity posture to meet healthcare compliance guidelines

Cybersecurity Liability

Insurance

Risk can never be 100% eliminated or avoided. That is where the transfer of risk to a cybersecurity insurance provider can help



Evolution of the CISO Role

◆ AI Overview

The Chief Information Security Officer (CISO) role originated in the 1990s as a response to increased cybersecurity threats. The first CISO was Steve Katz, who was appointed to the role at Citicorp in 1995.

Origins

- The CISO role was created to protect an organization's information and operations
- The role was initially known as Information Security Manager (ISM)
- The role evolved into CISO as the responsibilities grew

Evolution

- The CISO role has expanded to include risk management, compliance, data privacy, and more
- The CISO role has become standard practice in business, government, and non-profits
- The CISO role has evolved to include working with suppliers, customers, and partners

Current role

- The CISO role is often considered a critical link between IT and security functions
- The CISO role has broadened to include risks found in business processes, customer privacy, and more
- The CISO role is now focused on being a business enabler

Future challenges

- The CISO role faces challenges such as increased cyber risk, cloud computing, and mobile devices

Comparison of vCISO and In-House CISO Roles

<u>Aspect</u>	<u>vCISO</u>	<u>In-House CISO</u>
Scope	Short term contract with specific goals like compliance or maturing the cybersecurity posture as outlined in a “Statement of Work” document	A long-term business executive responsible for managing strategic and operational aspects of cybersecurity risk with a focus on aligning cybersecurity risk with business goals
Flexibility	Usually, more flexibility than CISO to adapt to evolving threats	Usually, Less flexible due to all responsibilities that come with full-time employment
Operational Involvement	Usually not involved in daily security operations but provides valuable strategic guidance to meet business needs	Key to both daily security operations and strategic long-term planning with other executives

Comparison of vCISO and In-House CISO Roles Continued...

<u>Aspect</u>	<u>vCISO</u>	<u>In-House CISO</u>
Experience/Expertise	Provides high-level security with more insight into cyber crises and potentially backed by the expertise of several certified professionals in the field	Dependent on the officer hired, their expertise can be limited and less flexible
On-boarding process	Once a vCISO partner has been chosen, onboarding is simple as they are not subjected to other internal employee obligations and can hit the ground running	Onboarding can be slower for internal employees due to relocations, internal training obligations, and integration into systems
Cost	Typically, more cost effective due to part-time or “fractional” focus of the engagement.	CISO’s living in big cities working for Fortune 500 corporations typically earn as much as \$380k to \$420k per year...per cyber crime magazine

vCISO vendors in Louisiana

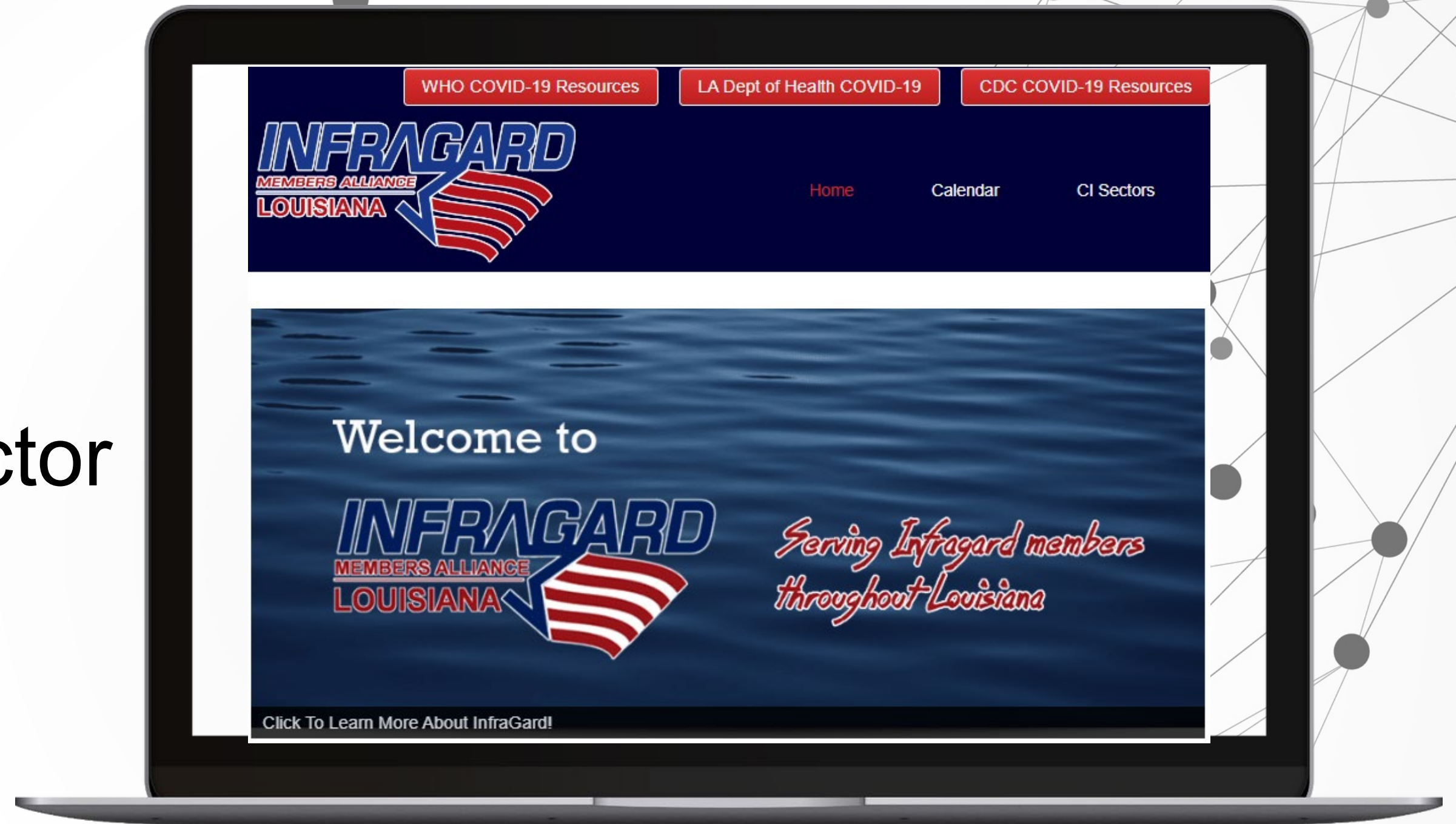


CEO ROUNDTABLE



Free Resources:

VP and
Communications Sector
Chief, Louisiana
Chapter of InfraGard



Chief Warrant Officer 3

Interim Commander
Louisiana State
Guard Cyber Reserve
Team



Call to Action

- Cybersecurity is commonly known as a technology problem, but it is now also known as both a business and a Safety problem too! With the healthcare sector the number one most targeted sector according to the FBI, you need to partner with a strong vCISO now who understands your business needs and can keep you and your patients safe and secure!



Joshua (JTan) Tannehill, CISSP

Brand Ambassador @ Coretechs, Owner @ JTan, LLC, Commander @ Louisiana State Guard Cyber R...

