H-ISAC™

HEALTH - ISAC

Overview

Denise Anderson – President & CEO H-ISAC

Why ISACs?

- **Trusted** entities established by CI/KR owners and operators.
- Comprehensive **sector** analysis aggregation /anonymization
- **Reach**-within their sectors, with other sectors, and with government to share critical information.
- **All-hazards** approach
- **Threat** level **determination** for sector
- **Operational**-timely accurate actionable

Why ISACs?

- Most ISACs have global members and operations
- Most ISACs are not-for-profit (501c6 or 501c3)
- Most ISACs are private sector organizations that rely on member dues for funding
- ISACs collaborate through the NCI

H-ISAC

Founded in 2010

Global Member Organizations:

- Providers
- Health System Payers
- EHR/EMR Developers
- Lab/Radiological
- Biotech/Pharma
- Academia
- Medical Device Manufacturers
- Pharmacy

Trust community, forum for information sharing including:

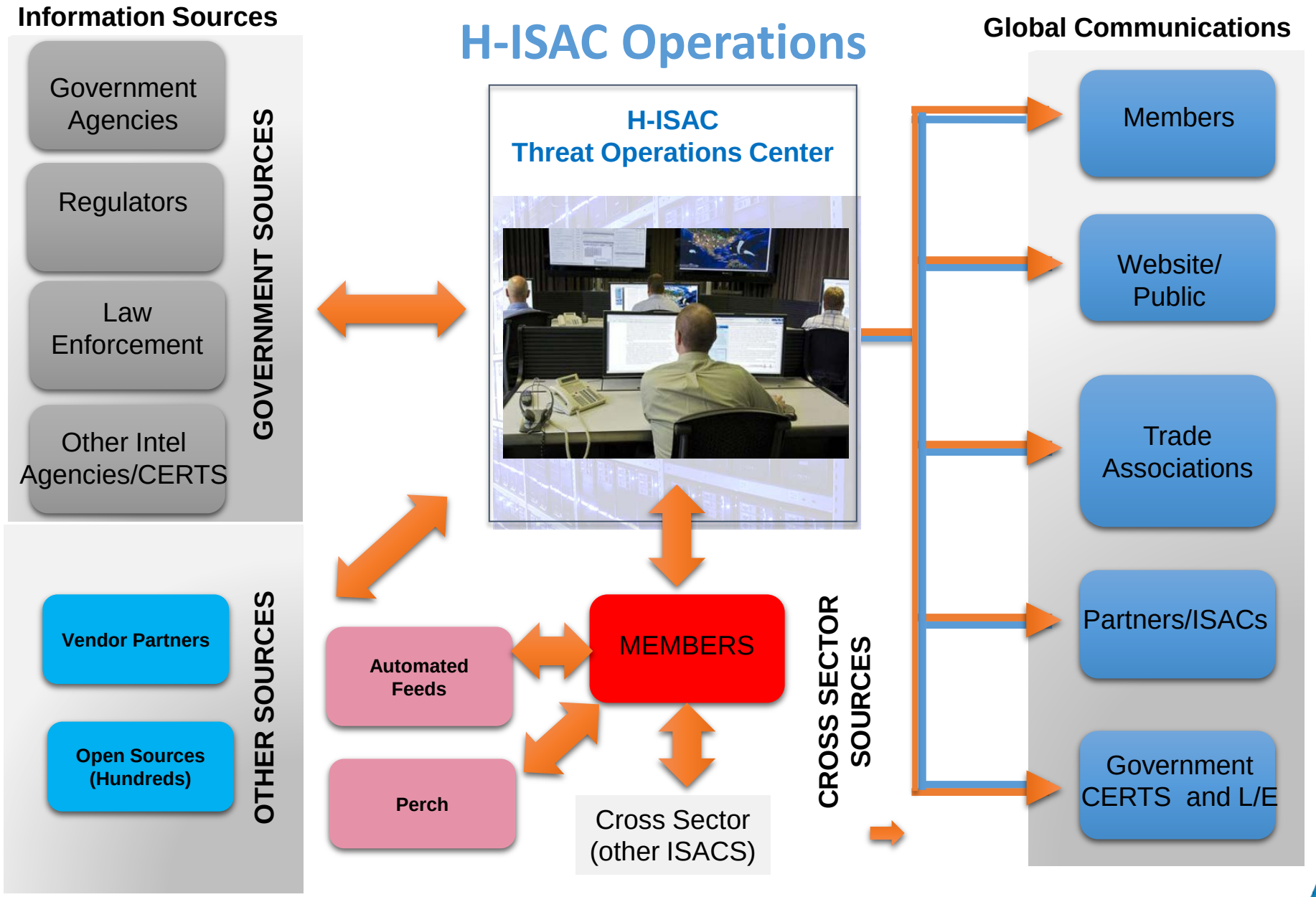
- Situational Awareness,
- Threats,
- Vulnerabilities,
- Best Practices
- Mitigation Strategies

H-ISAC Threat Operations Center (TOC)

Dedicated staff of security analysts, an extension of the security team

2020 Statistics

- Victim notifications - **798**
- Threat Bulletins - **77**
- Vulnerability Bulletins - **51**
- Member shared IOCs - **185,413**


Information Sources
H-ISAC Operations
Global Communications
Government Agencies
Regulators
Law Enforcement
Other Intel Agencies/CERTS
GOVERNMENT SOURCES
H-ISAC
Threat Operations Center
Members
Website/ Public
Trade Associations
Partners/ISACs
Government CERTS and L/E
Vendor Partners
Open Sources (Hundreds)
OTHER SOURCES
Automated Feeds
Perch
MEMBERS
Cross Sector (other ISACS)
CROSS SECTOR SOURCES

Cyber Threats, Vulnerabilities, Incidents

- ✓Malicious Sites
- ✓Threat Actors, Objectives
- ✓Threat Indicators
- ✓TTPs, Observables
- ✓Courses of Action
- ✓Exploit Targets
- ✓Attacks

- ✓Malicious Emails: Phishing/ Spearphishing
- ✓Software Vulnerabilities
- ✓Malicious Software
- ✓Analysis and risk mitigation
- ✓Incident response

Primary Ways Information Is Shared With Members/Partners

- ✓Portal/Alerts
- ✓Listservers/Secure Chat
- ✓Automation
- ✓Briefings
- ✓Daily Products, Alerts and Bulletins
- ✓Monthly Threat Briefings
- ✓Cyber Threat Level

For Public: H-ISAC.ORG

BazarCall Targets Healthcare Entities

H-ISAC™ HEALTH - ISAC

The operators of the BazarLoader malware are working together with underground call centers to trick the victims of their spam campaigns into opening malicious Office documents and infecting themselves with malware. The new malware was discovered being distributed by call centers in late January and is named BazarCall, or BazaCall, as the threat actors initially used it to install the BazarLoader malware.

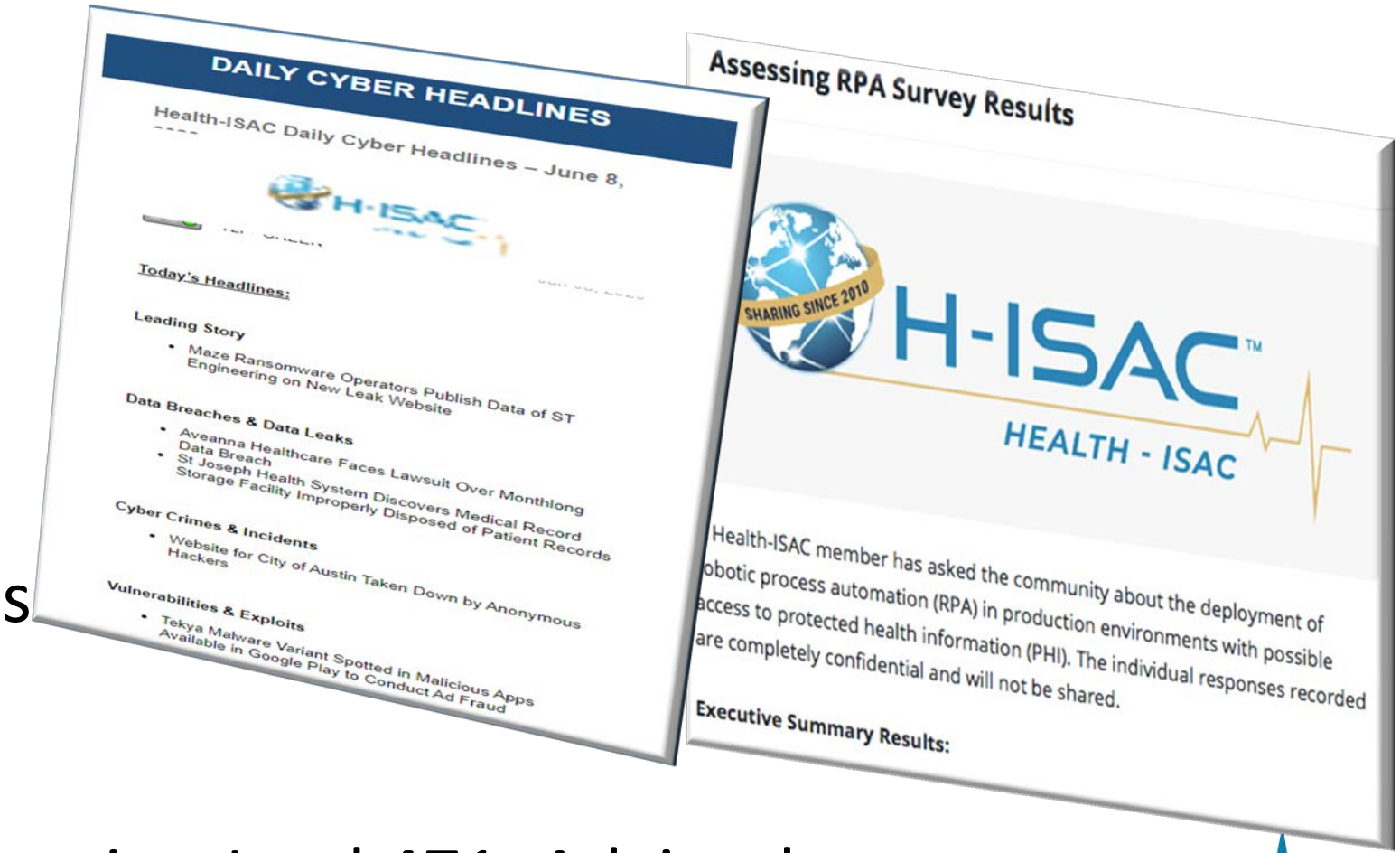
While this is not the first time when cybercrime gangs have worked together with underground call centers, this is the first time when we see a major malware distributor, such as the BazarLoader gang, use this tactic on a large scale.

Like many malware campaigns, BazarCall starts with a phishing email but from there deviates to a novel distribution method; using phone call centers to distribute malicious Excel documents that install malware.

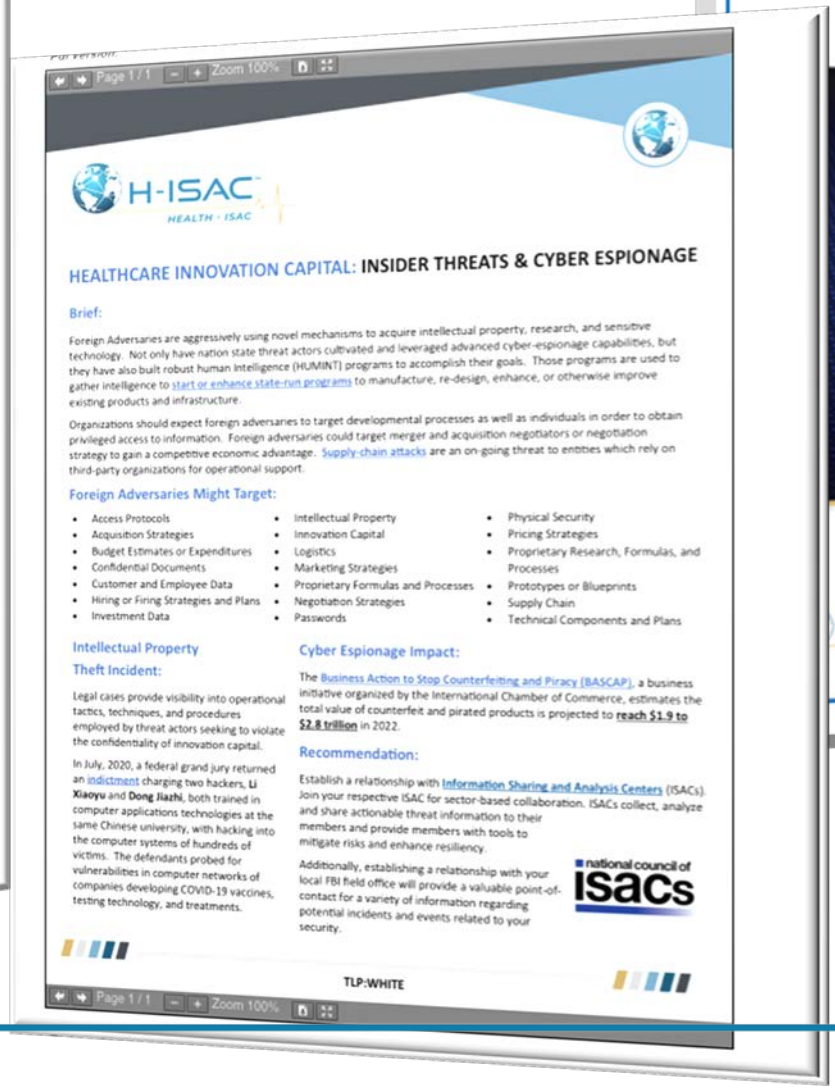
The emails then prompt the user to contact a listed phone number to cancel the

Other H-ISAC Intelligence Offerings

- Daily Reports
- -Cyber and Physical
- Surveys
- Table-Top Exercises
- After Action Reports
- Patch Tuesday podcasts
- Weekly IOC Report
- Hacking Healthcare
- Partner Reports – Flashpoint, Intel 471, Advintel



H-ISAC White Papers

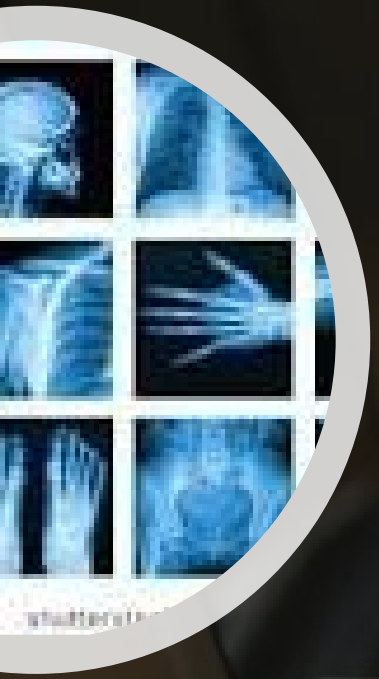


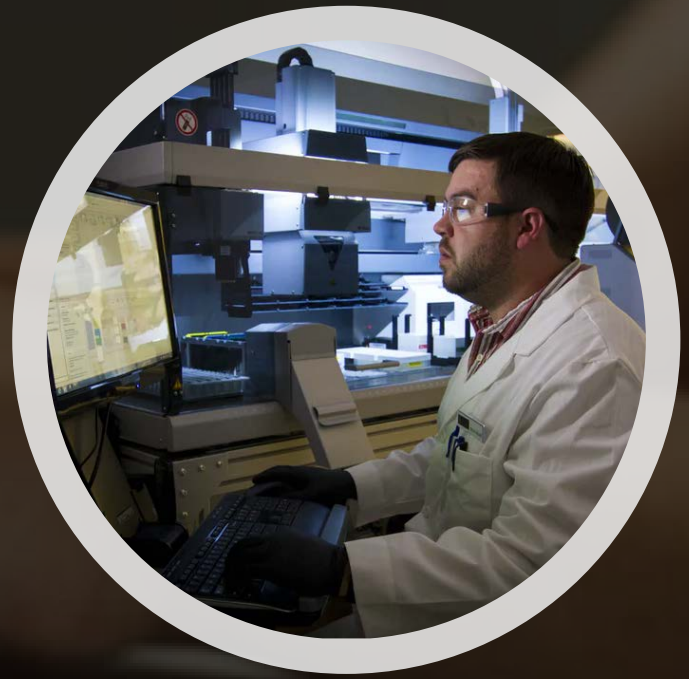
Networking/Collaborating

- ✓Educational Events
- ✓Committees & Working Groups
- ✓Community Shared Services
- ✓Exercises

Threat Landscape for the Health Sector

Remember This?





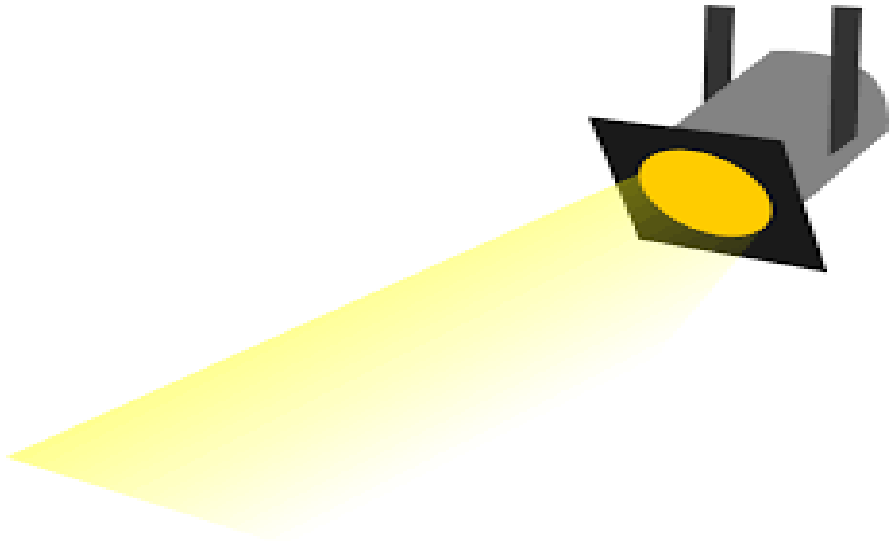
It’s Now This…

It Started with A Good Idea

13-50 years=200 million

HITECH ACT of 2009

Health Information Technology for Economic and Clinical Health ACT



- Financial Incentives and Penalties
- Focus on Data and Privacy

…..Not on Cybersecurity

Other Factors

- ❑ Realization of the value of the data
- ❑ Technology Evolution – Medical Devices
- ❑ Evolution of Actors and Threats
- ❑ Nature of Healthcare:
  - ➢ Paper to Data
  - ➢ Connecting to the Internet
  - ➢ Data Portability
  - ➢ Lack of Cyber Security Expertise
  - ➢ Thin Margins – End of Life
  - ➢ 24-Hour Operations
  - ➢ Open Environment
  - ➢ Compliance Culture
  - ➢ Silos Between:
    - Staff
    - Divisions/Functions
    - MDMs/HDOs

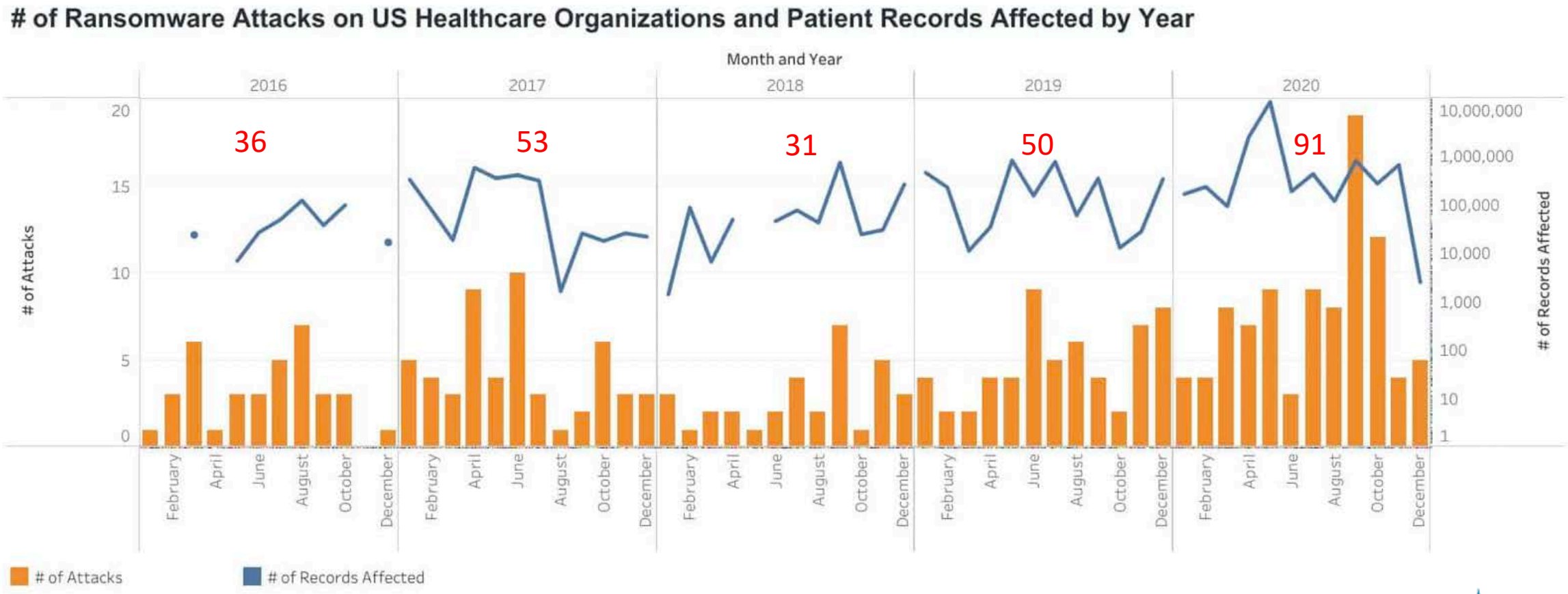
Incidents

Anthem

NHS NHS

NUANCE

Timeline of Ransomware Attacks



Comparitech.com 3/10/21

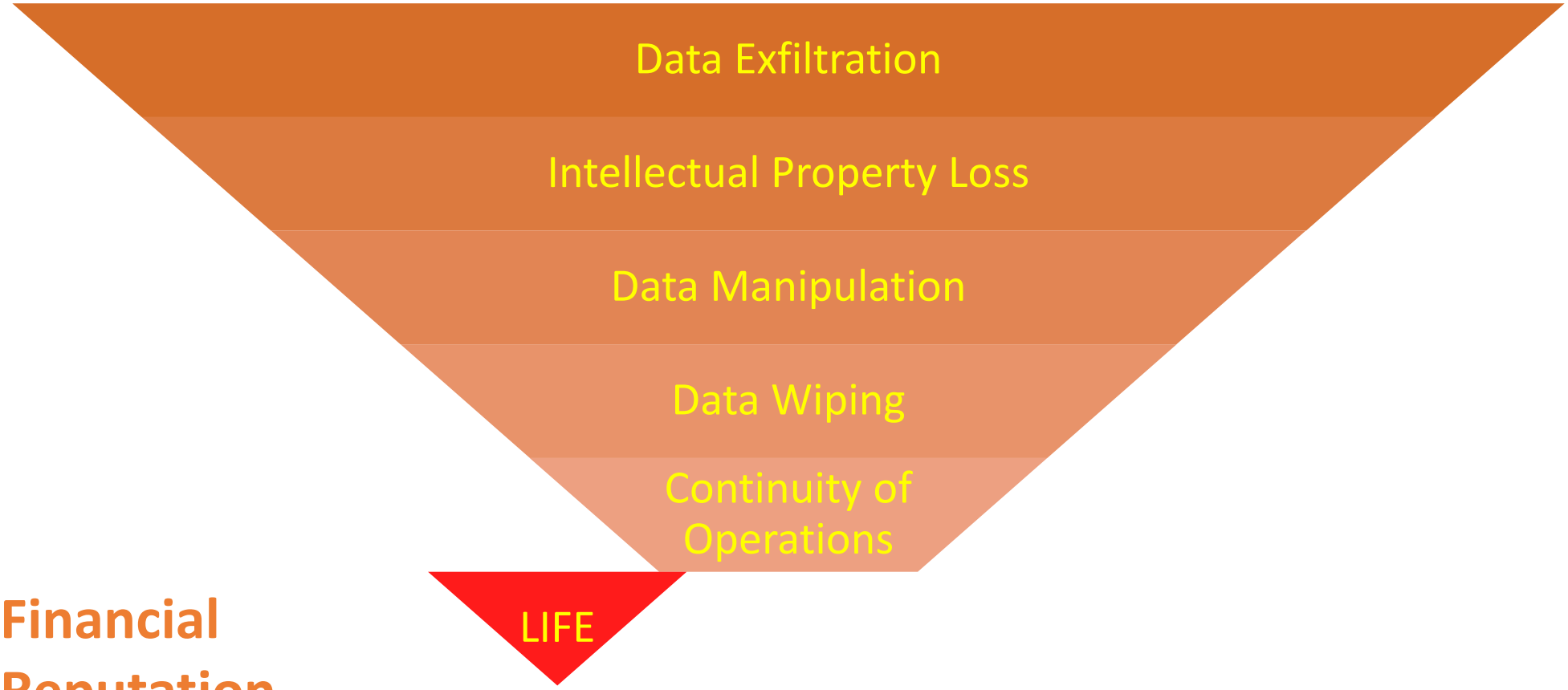
Ransomware Trends

- Targets have Evolved
- Specialized Marketplace
- Ransomware as a Service
- Extortion and DDoS
- Reconnaissance
- Multiple Malware
- MSSPs
- Prices Climbing

Other Threat Trends in the Healthcare Sector

- Third Party Risk and Concentration Risk
- Insider Threat
- Blended Threats
- BEC
- Social Engineering
- Remote work environment/Telehealth
- Phishing
- Vulnerabilities (many critical) & Network Scanning – Citrix, MS (printer nightmare), Pulse VPN, RDP
- Physical/Blended

It’s Not About the Ones & Zeroes



-Financial
-Reputation

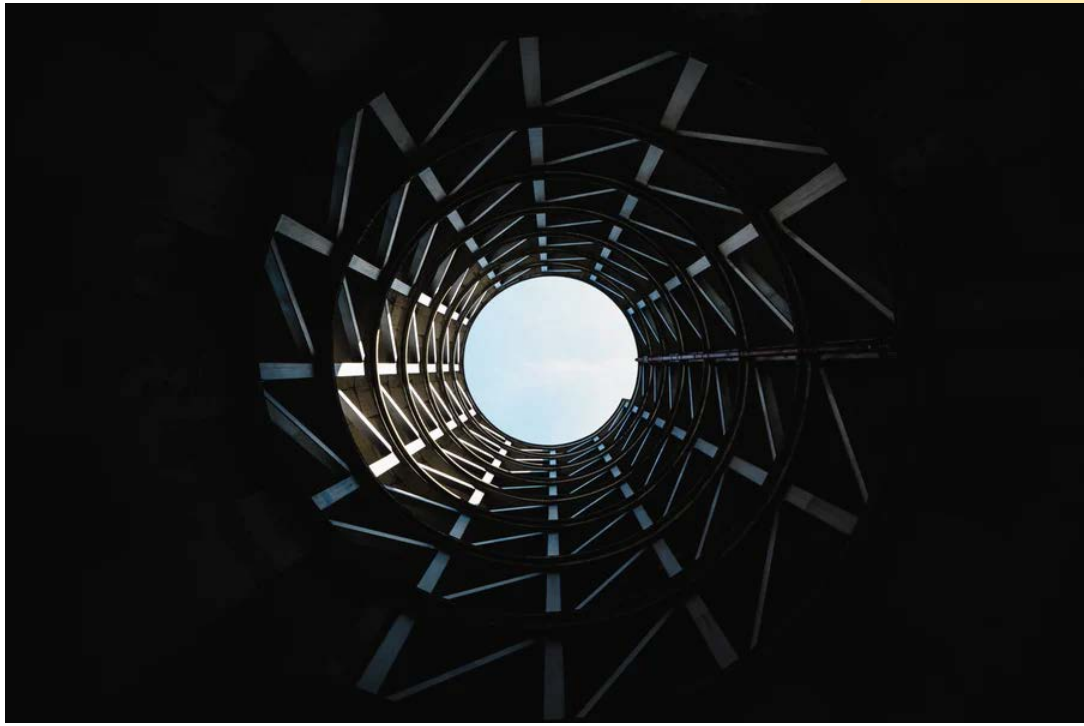
The Future

What Can We Do?

- Enterprise Risk Management – Crown Jewels
- Understand Environment/Threat Surface
- Board and Executive Support/Commitment
- Patching and Budget Cycles
- Threat Intelligence/Situational Awareness – Information Sharing
- Ecosystem Training/Awareness
- Tear Down Silos

Summary

- Old Threats Still Exist – Can’t Ignore
- Need to Stay Abreast of Evolving Threats
- All-Hazards, Enterprise Risk Management Approach
- Cascading Impacts - Ecosystem
- Same Team
- Share, Share, Share



Thank you!