LOUISVILLE-JEFFERSON COUNTY METRO GOVERNMENT METRO TECHNOLOGY SERVICES

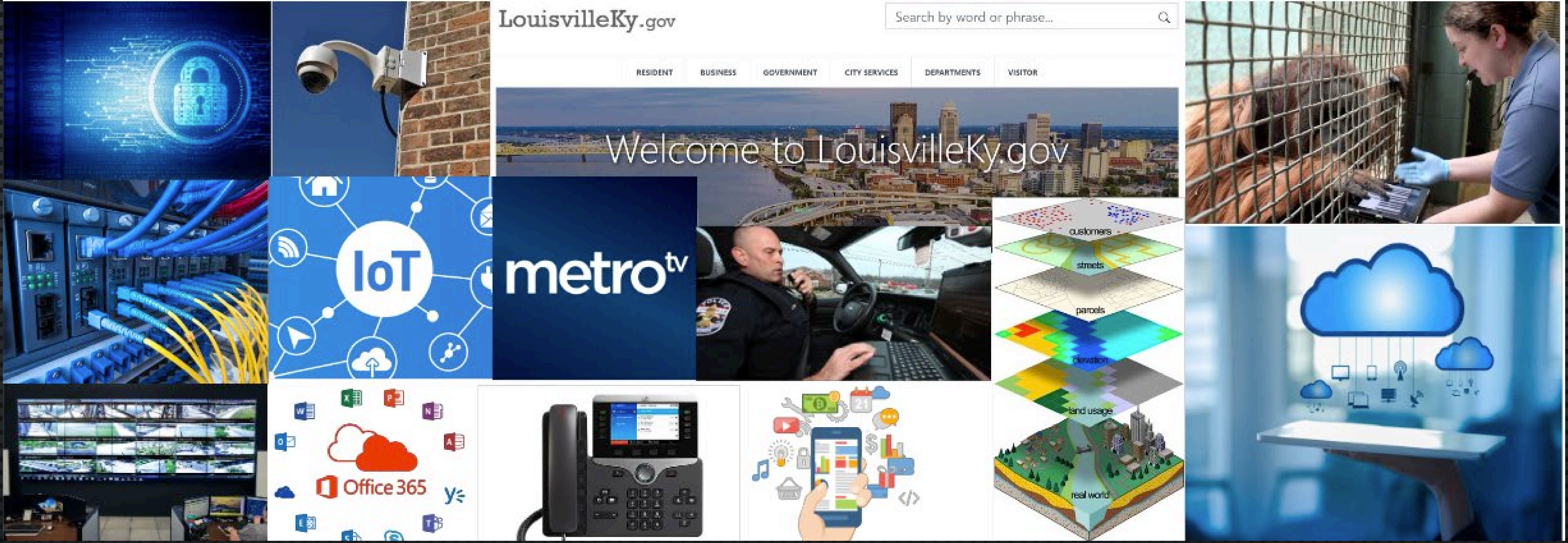
August 2024

Presenters

Chris Seidt
Executive Director/Chief Information Officer
22 Years with LMG

James Meece
Chief Information Security Officer
9 Years with LMG
(Retired) Cyber Officer KYARNG

What we do


LouisvilleKy.gov
Search by word or phrase...
RESIDENT
BUSINESS
GOVERNMENT
CITY SERVICES
DEPARTMENTS
VISITOR
Welcome to LouisvilleKy.gov
IoT
metro tv
Office 365
customers
streets
parcels
elevation
land usage
real world

By the Numbers

21,000 IP connected devices

2.5 PB of data stored

3 data centers

6,000 users

128 linear miles of fiber optic cable

41,000 help desk calls per year

82 fulltime employees

20 contractors

185 connected buildings

216 Million Annual Cyber Security Events

Our Approach to Cyber

Confidentiality

Integrity

Availability

DEFENSE IN DEPTH
CONTINUOUS IMPROVEMENT

Continuous Improvement

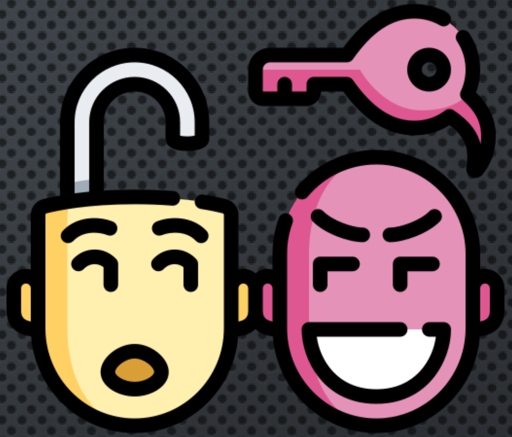
FY 15-17	FY 18-19	FY 20-21	FY 22-23	FY 24+
• Intrusion protection • Web security • Email security • Modern antivirus • Mobile device management • Admin account protection	• Cloud Security • Strategic partnerships • Vulnerability management • Disaster recovery • Continuity of Government • Continuous assessments	• COVID! • Protecting telework • 24X7 operations • Benchmark against peers • Vendor risk management • Policy and governance review • Incident detection and response	• Data encryption • Malware analysis • Critical application assessments • Tabletop exercise • Zero trust • Email spoofing prevention • Asset management	• Password free login • Reassess and refine security architecture • Digital forensics • Rogue device detection • Kentucky Cyber Threat Intelligence Cooperative (KCTIC)

Threat Landscape

What are the top cyber threats that we face as a city government?

Ransomware and Scareware

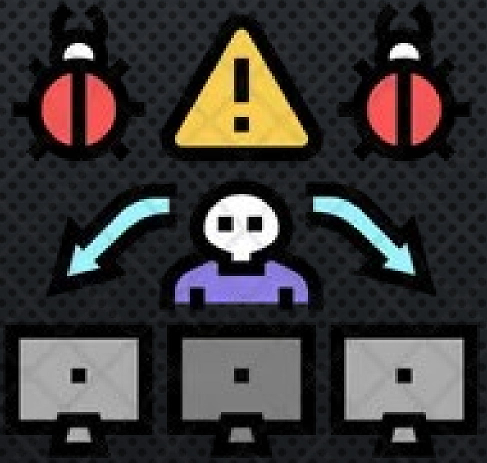
Data Breach



Social Engineering

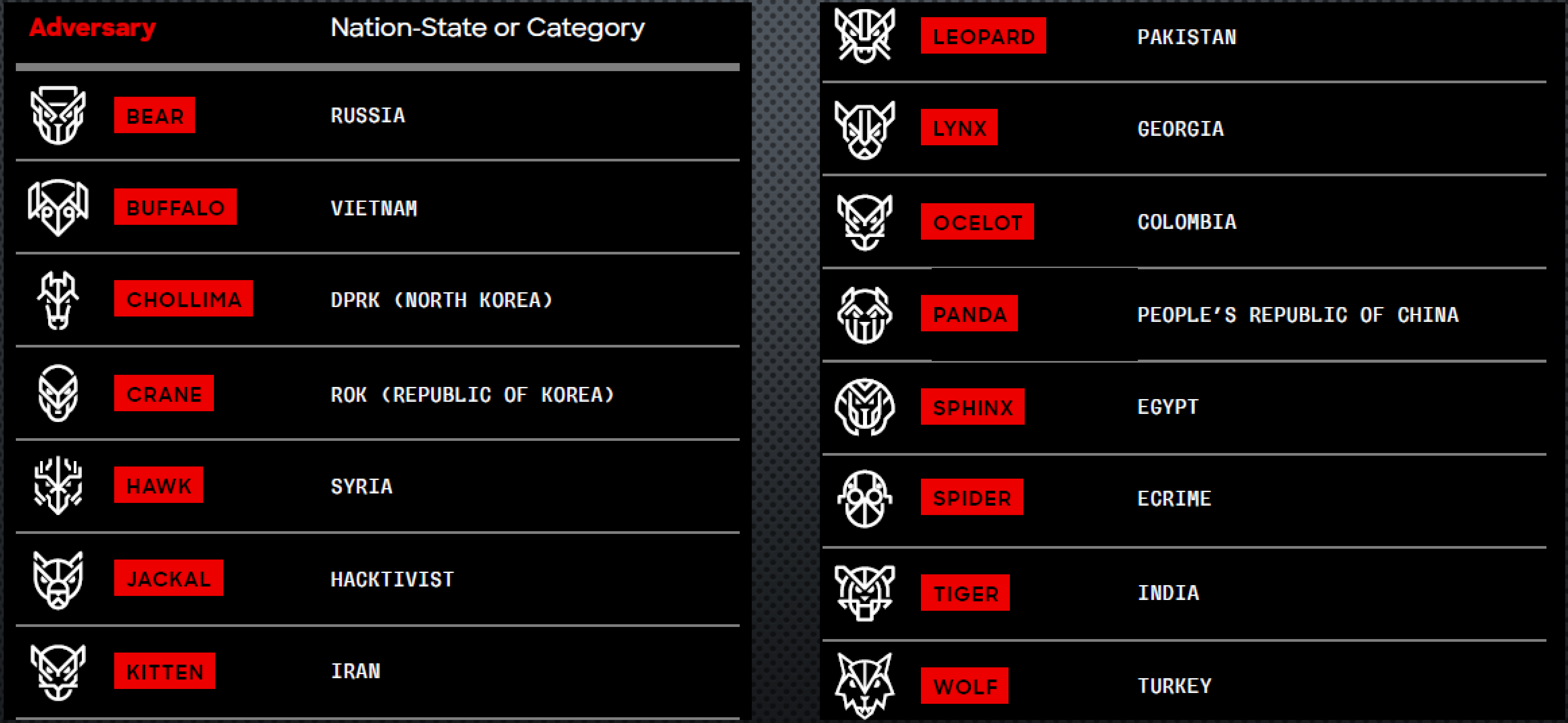
Zero Day Exploits

Denial of Service Attacks



Insider Threats and Human Error

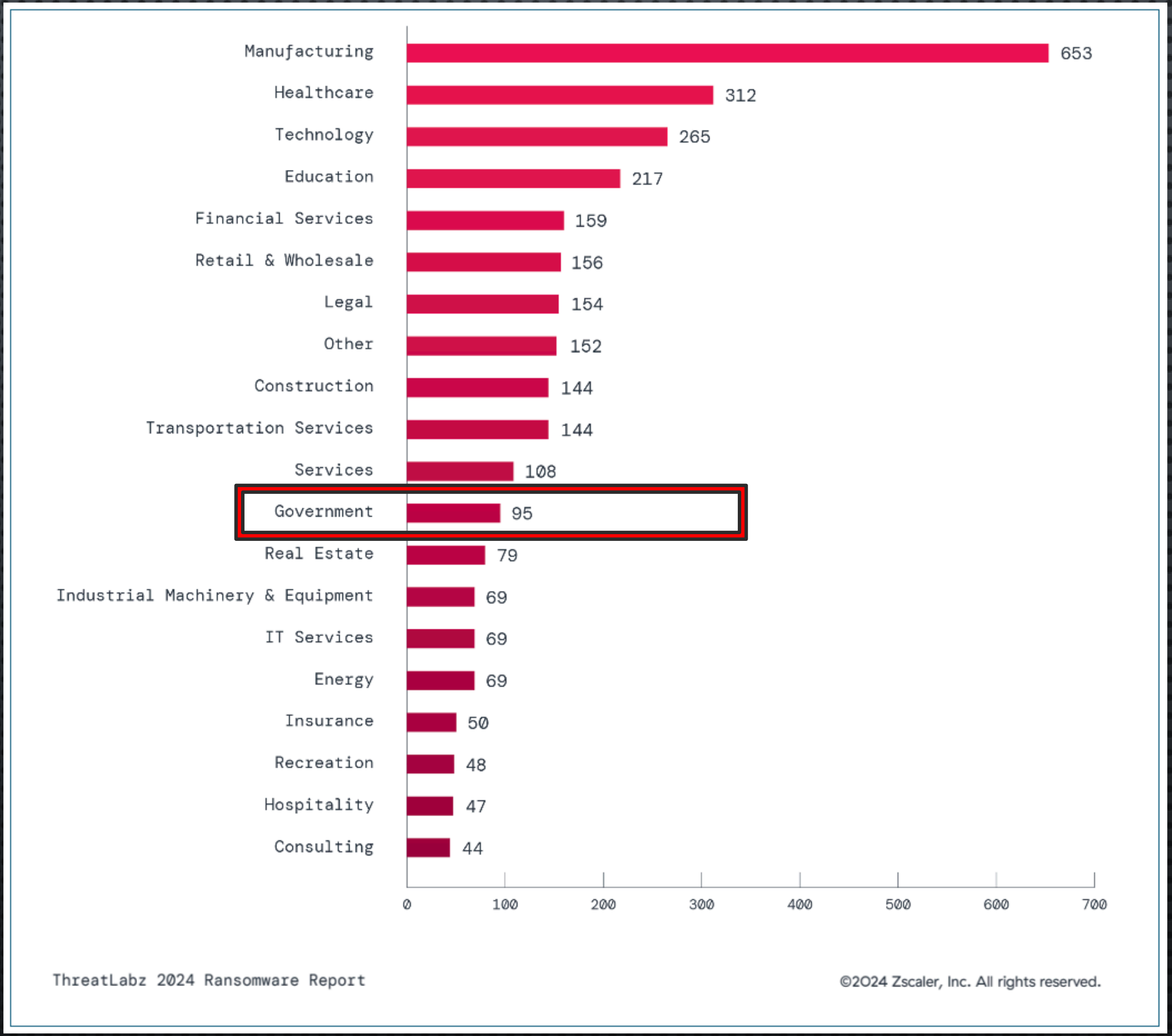
Who is behind these attacks?



Adversary	Nation-State or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPHINX	EGYPT
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY

Source: CS 2024 Global Threat Report

2024 Ransomware Report



ThreatLabz 2024 Ransomware Report

Global Cyber Incidents

Ransomware attacks on Governments and other organizations continue.

Recent Ransomware Attacks:

- Meat processor JBS, Colonial Pipeline, Houston Rockets, CNA Financials, Oldsmar Florida Water Processing Plant, Kia Motors, Acer Computer Corporation, Baltimore, Dallas, Fort Worth PD, Atlanta and Fulton County, Anchorage, **Norton Healthcare, and many others.**

Other Notable Incidents:

- SolarWinds and Microsoft attacks occurred months before the vulnerabilities were publicly released to partners (lack of consistent communication)
- Microsoft Azure and Office 365 outages
- Crowdstrike worldwide outage causes Billions in damages July of 2024
- McAfee configuration issue in 2011
- **98% percent of cyber incidents involve preventable human error.**

Local Gov Impacts of Global Incidents

- **Pensacola City Government – Days after a shooting on a Naval base, ransomware impacts 311, medical records, phones, and other public services.**
  - Pensacola refused to pay, and the hackers started leaking data online
- **Baltimore – 2019, 911 systems shut down during citywide protests due to cyber attack**
  - Attacks used to disrupt emergency services responding to rioters.
- **Monroe County, IN and Columbus, OH ransomware attacks**
- **Jefferson County Clerk's Office and PVA office ransomware attacks.**

- **Louisville Metro Government**
  - 81 home rule cities, municipalities, fire districts, and quasi-governmental agencies greatly increase the risk
  - Mass spam and phishing
  - Attacks from local law firms, quasi-government agencies, and financial partners of Metro
  - Local law firms and quasi-governmental agencies used as staging point for attacks
  - **Cyber incidents increase up to 200% during events that generate a news cycle**

City/County Capabilities and Needs

What can we do and not do?

- **We can:**
  - Increase collaboration with regional partners, both private and government, through strategic partnerships
  - Apply limited amount of available Federal grant funding to increase collaboration and capabilities
  - Advise and mentor
  - Help remove impediments to effective information sharing
    - **Kentucky Cyber Threat Intelligence Cooperative (KCTIC)**

- **We cannot:**
  - Run or fund cyber programs for home rule cities and counties at present staffing and funding levels
  - Support KCTIC long term without financial support

What Can you Do?

- **Incentivize collaboration with regional partners, both private and government, in the KCTIC**

- **Consider legislation outlawing paying ransom, but also fund cities and counties to a level that positions them to not have to pay ransom by funding:**
  - Backups of critical systems
  - Modern antivirus and firewall
  - Disaster recovery plans
  - Outsourced IT and Cyber where applicable
  - Cyber insurance

- **Consider legislation creating an approved IT vendor and product process and list**

- **Consider legislation supporting continued funding for KCTIC**

Questions

LOUISVILLE

1778 1778

JEFFERSON COUNTY