TESCO METERING

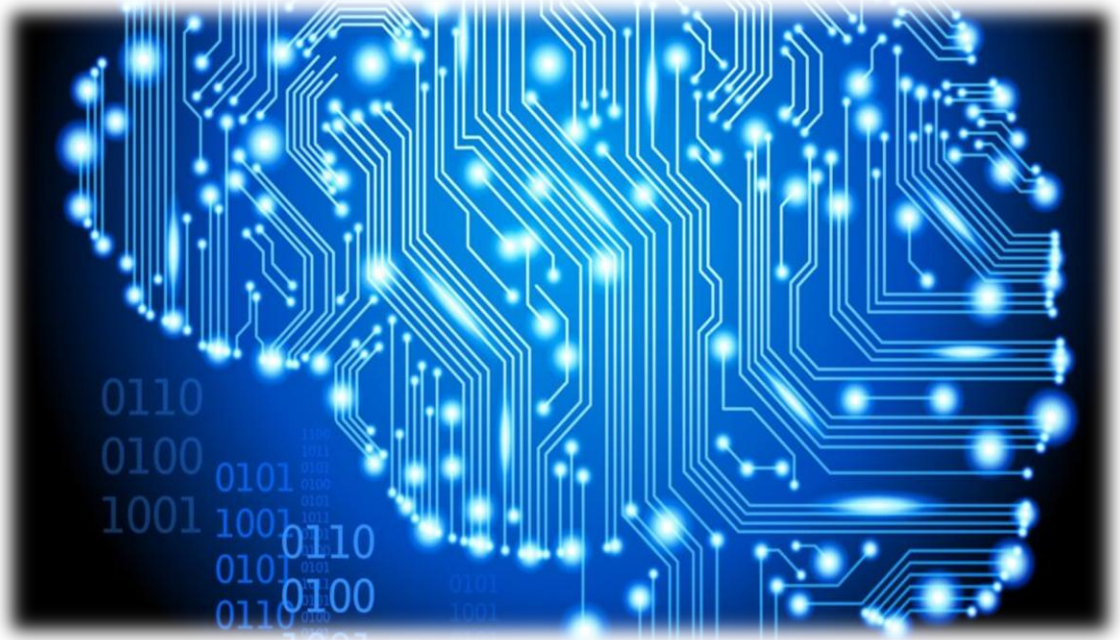
CYBER SECURITY
FOR METERING AND DISTRIBUTION

Prepared by Perry Lawton
TESCO Metering

North Carolina Meter School Management
Wednesday, June 12, 2025
8:00 AM

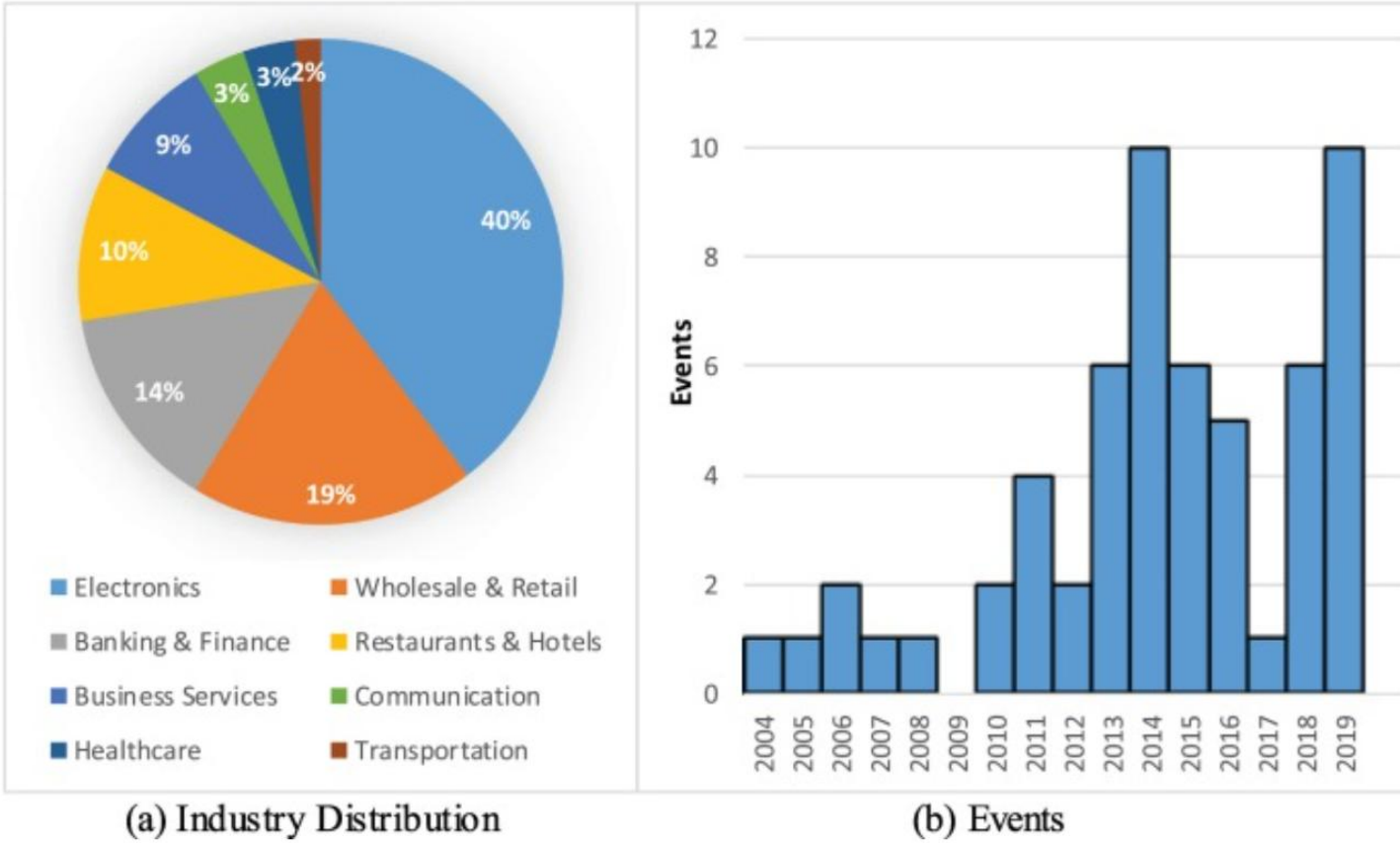
Introduction

Software and computing technologies **have changed and will continue** to change the world - but not without new risks



Introduction

- Highest average cost in 17 years, rising YOY
- United States of over $8.63 million on average
- An attack on one company affect firms in that vertical
  - Returns drop, premiums up
  - Affects reputation
  - Market reactions



(a) Industry Distribution (b) Events

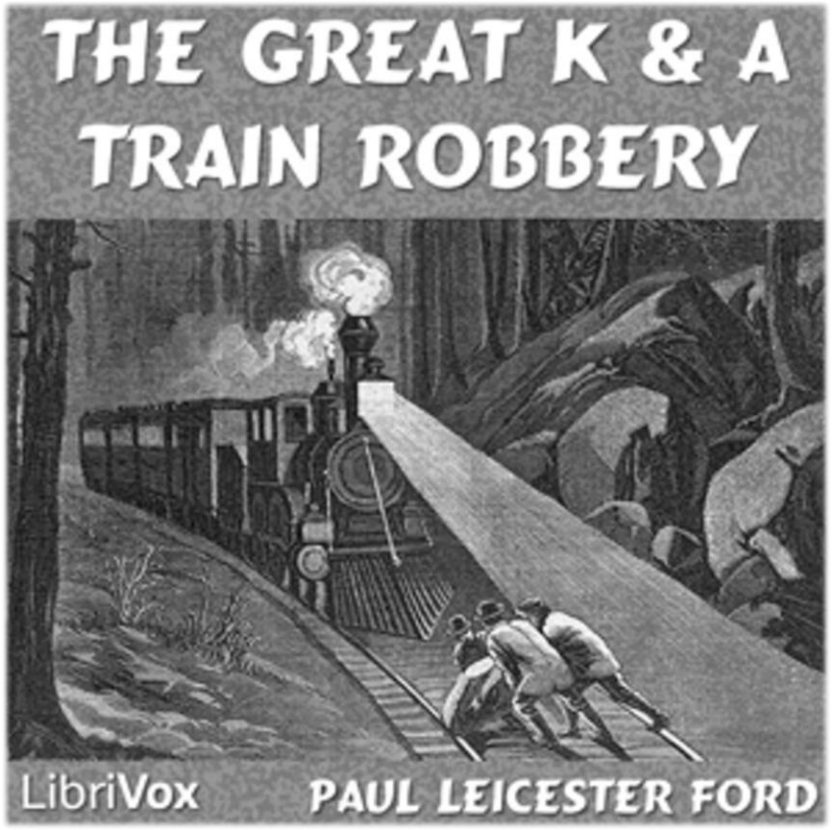
TESCO METERING

DATA AS A COMMODITY

Introduction

The only way to create an **impenetrable system** is to never let a person use it

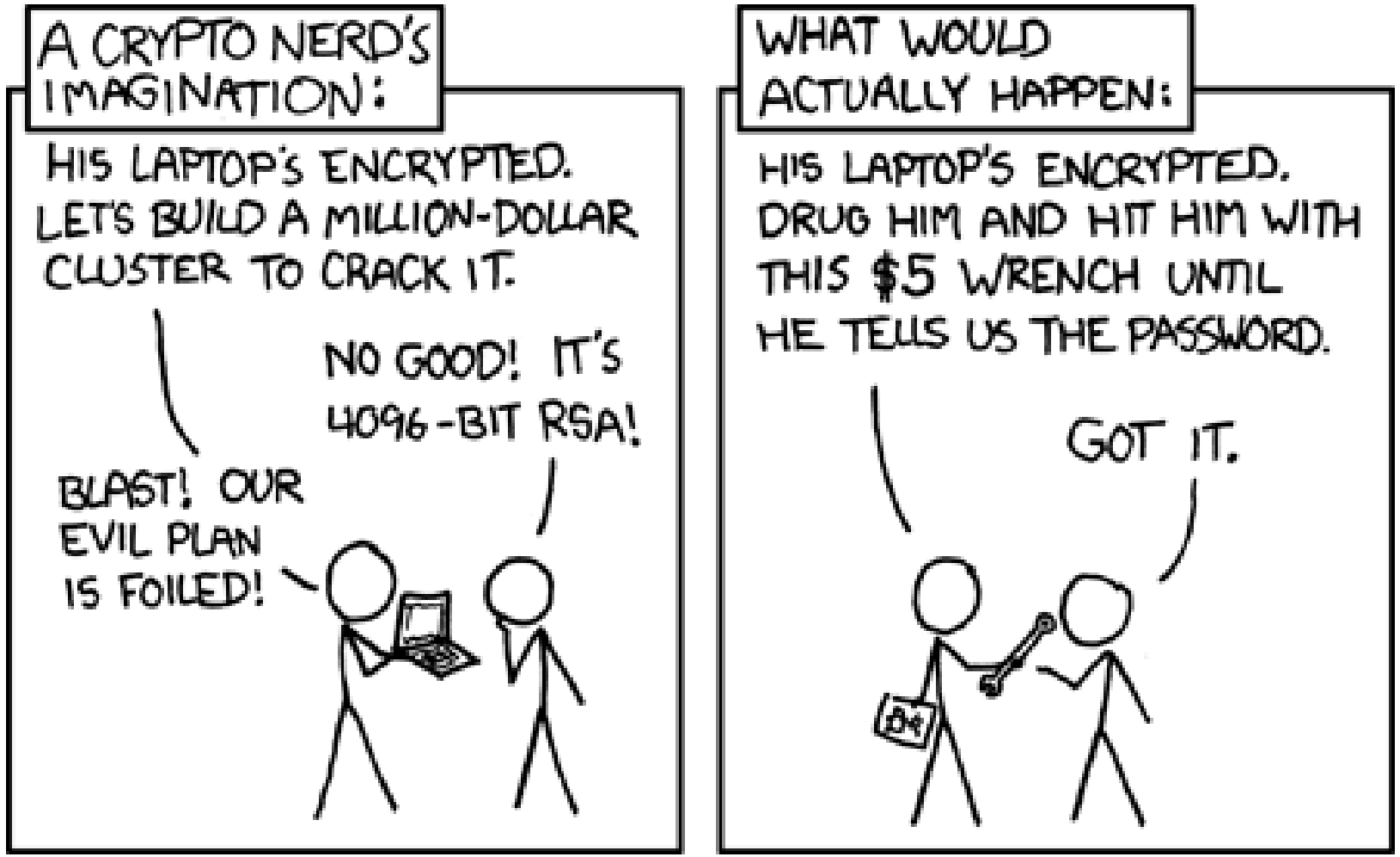
MONETARY THEFT



DATA BLACK MARKET

CRIMINALS

Introduction



https://xkcd.com/538/

RANSOMWARE

Introduction

HIGHER EDUCATION

Lincoln College to Close Permanently After Ransomware Attack

The Illinois college, which opened in 1865, said recent financial troubles and projected enrollment shortfalls were exacerbated by a ransomware attack last semester that rendered systems inoperable.

May 10, 2022 • News Staff

Introduction

Cyber attacks are showing up in larger and more critical areas, by larger and more persistent actors

- Israel/Saudi and/or Russia/Ukraine
- North Korea / Sony
- Colonial pipeline
- Log4J / Log4Net / Solarwinds

STATE BASED ACTORS

Persistent actors with unlimited funds

RBV or TCE?
State Paid, State Sponsored, or blind eyes?
Are they any worldwide regulations?

Cyber Cold War, Arms Race

Methodology

Obtaining data

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

*US based **nonprofit** policy research organization, whose purpose is to define the future of national security.*

- **835** cyber-attacks
- Occurred during the last **19 years**

Focus

- government agencies, defense, high-tech companies, or over $1M

Cleaning and searching

PROPOSED SEC CYBERSECURITY RULES

The proposed U.S. Securities and Exchange Commission cybersecurity rules would require companies to report material incidents on a Form 8-K and provide periodic disclosure on issues including:

- ☑ Policies and procedures to identify and manage cybersecurity risks.
- ☑ Management's role in implementing cybersecurity policies and procedures.
- ☑ The board of directors' cybersecurity expertise and oversight.
- ☑ Updates on previously reported material cybersecurity incidents.

- Data analysis
- Researching each case in public sources
- Identify
  - Data
  - Type of Attack
  - Motivation
  - Mechanism

Methodology

3

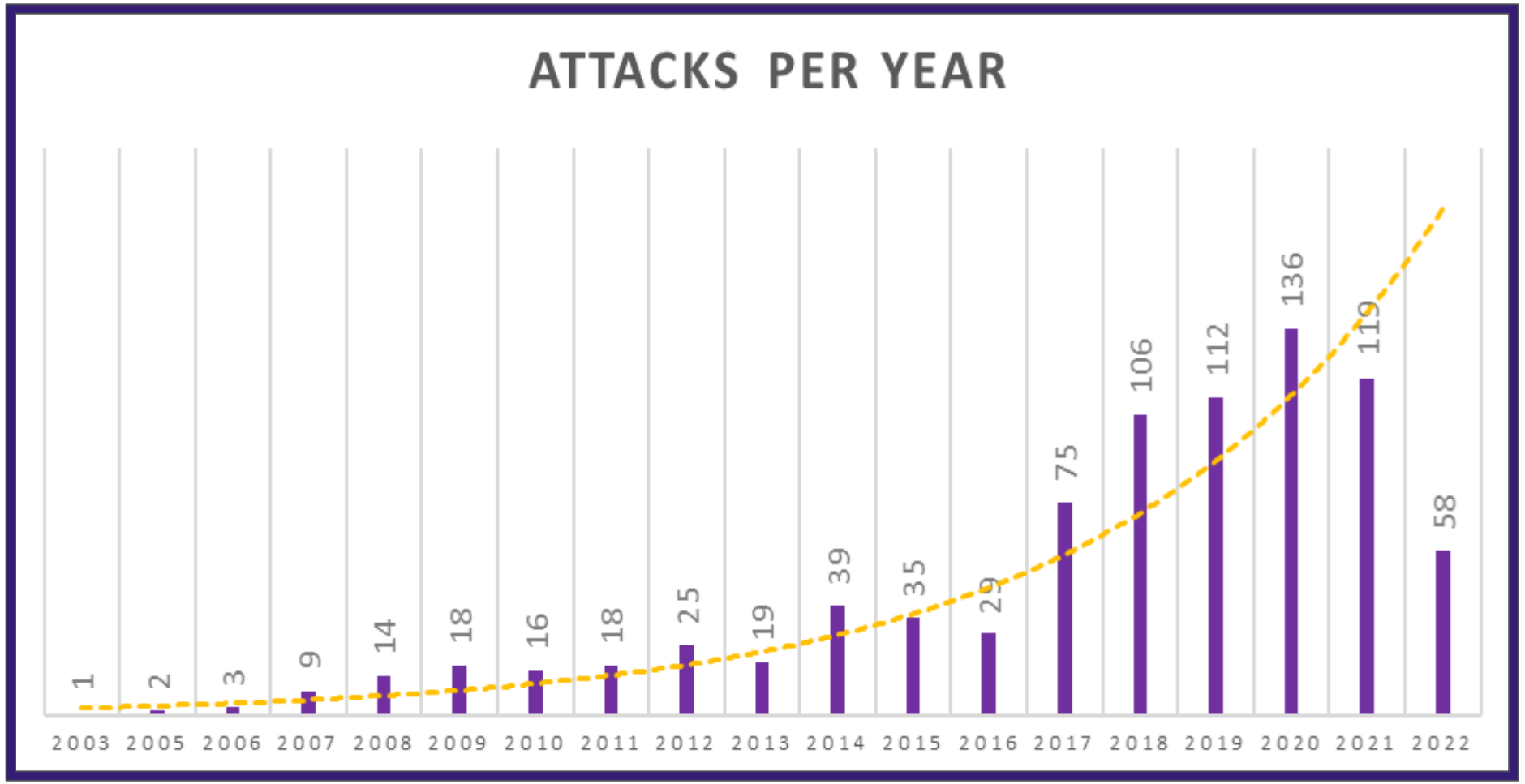
Categorizing

Demographics	Year, Perpetrator, Sector, Victim, Sponsored, Criminal
Type of Attack	Disruption, Leak, Unclear, Espionage, Sabotage, Theft
Motivation	Economic, Political, Information, Terrorism
Mechanism	Campaign, Malware, DDoS, Phishing, Ransomware, Remote Access

Analyzing

- Distribution
- Correlations
- Trends
- Forecasts

Results



835
Events

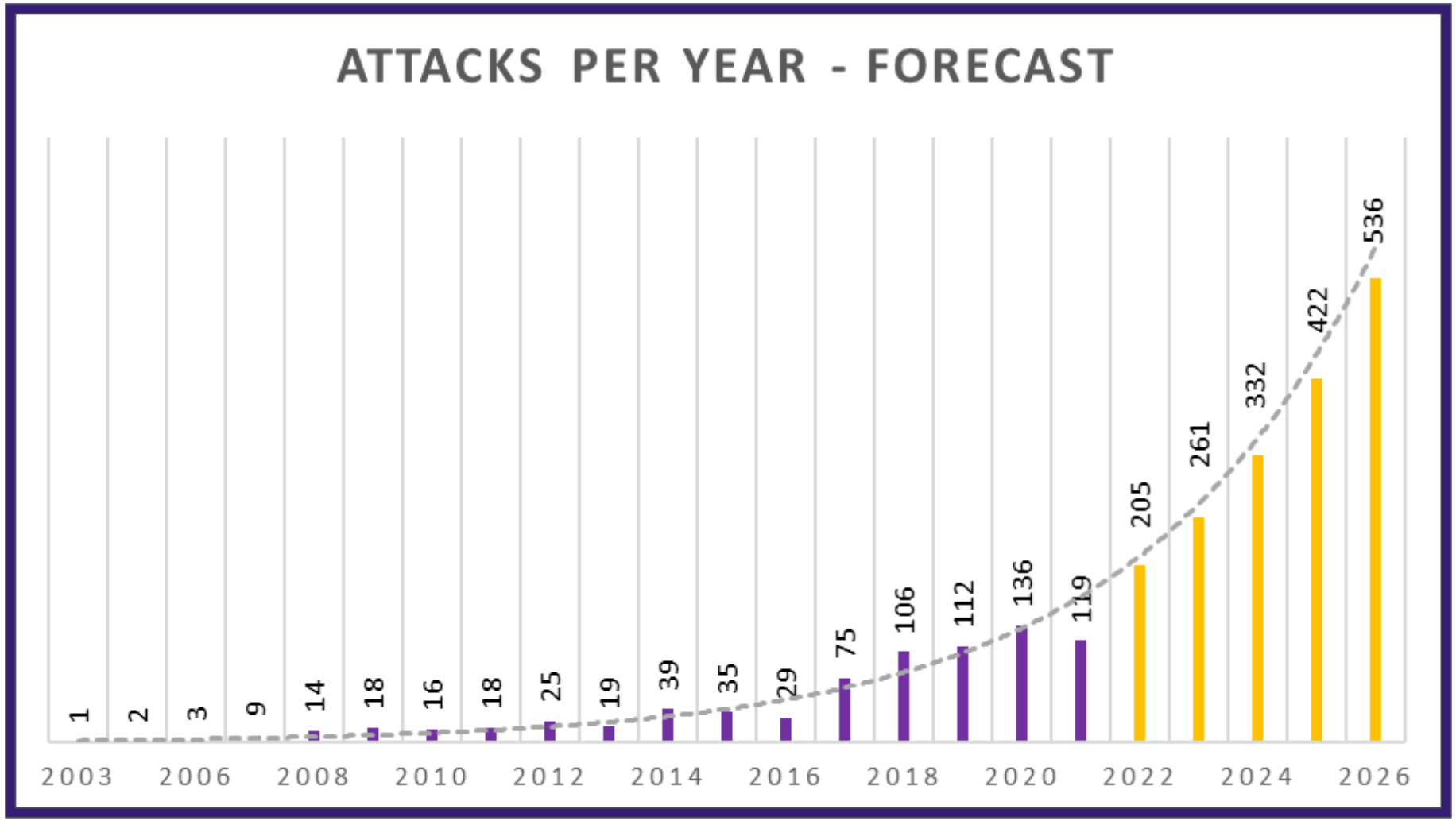
32%
Ave. Growth

87
Victim Countries

36
Perpetrator Countries

* 2022 data of Q1 (First Quarter)

Results



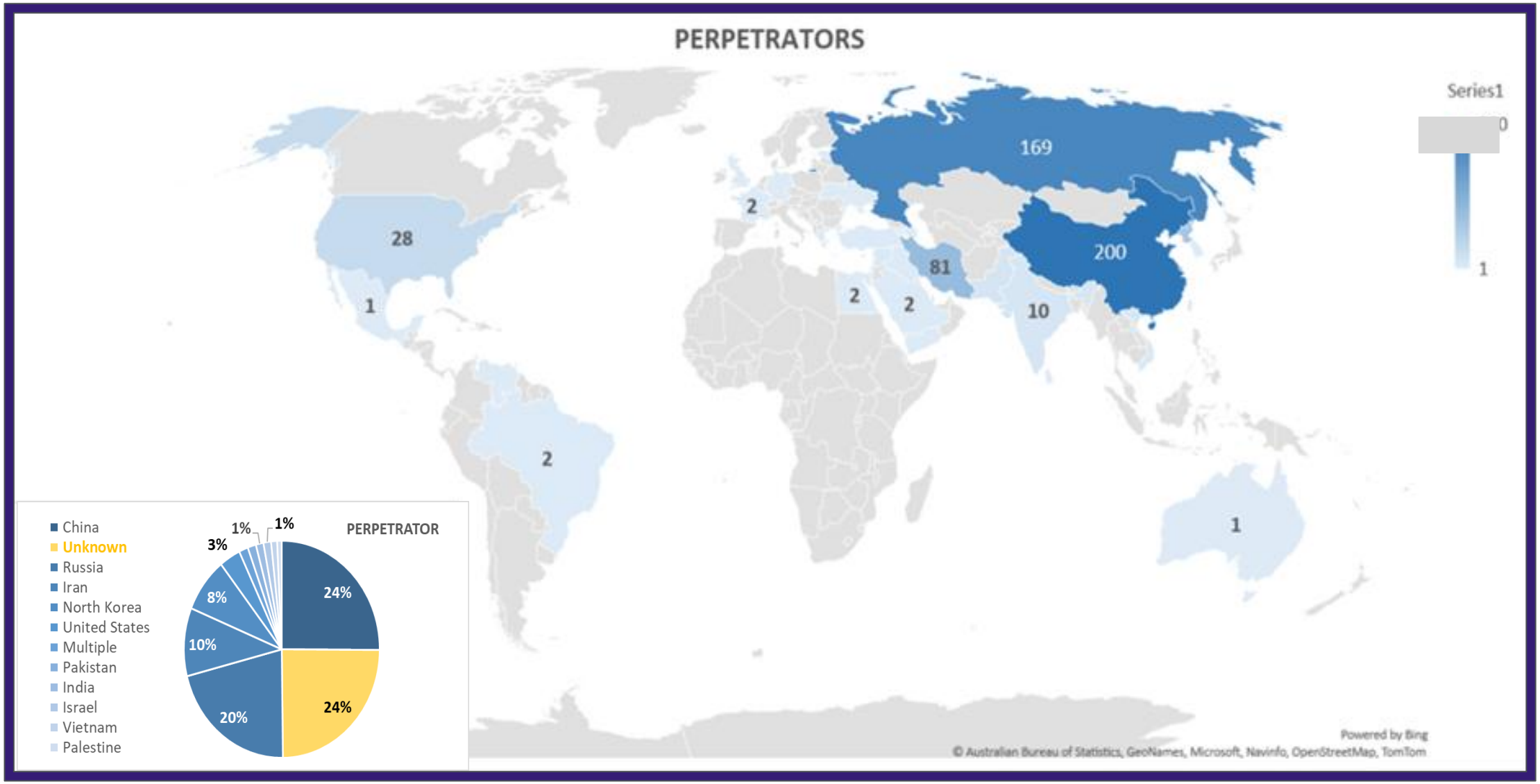
2,592

Events by 2026

Double

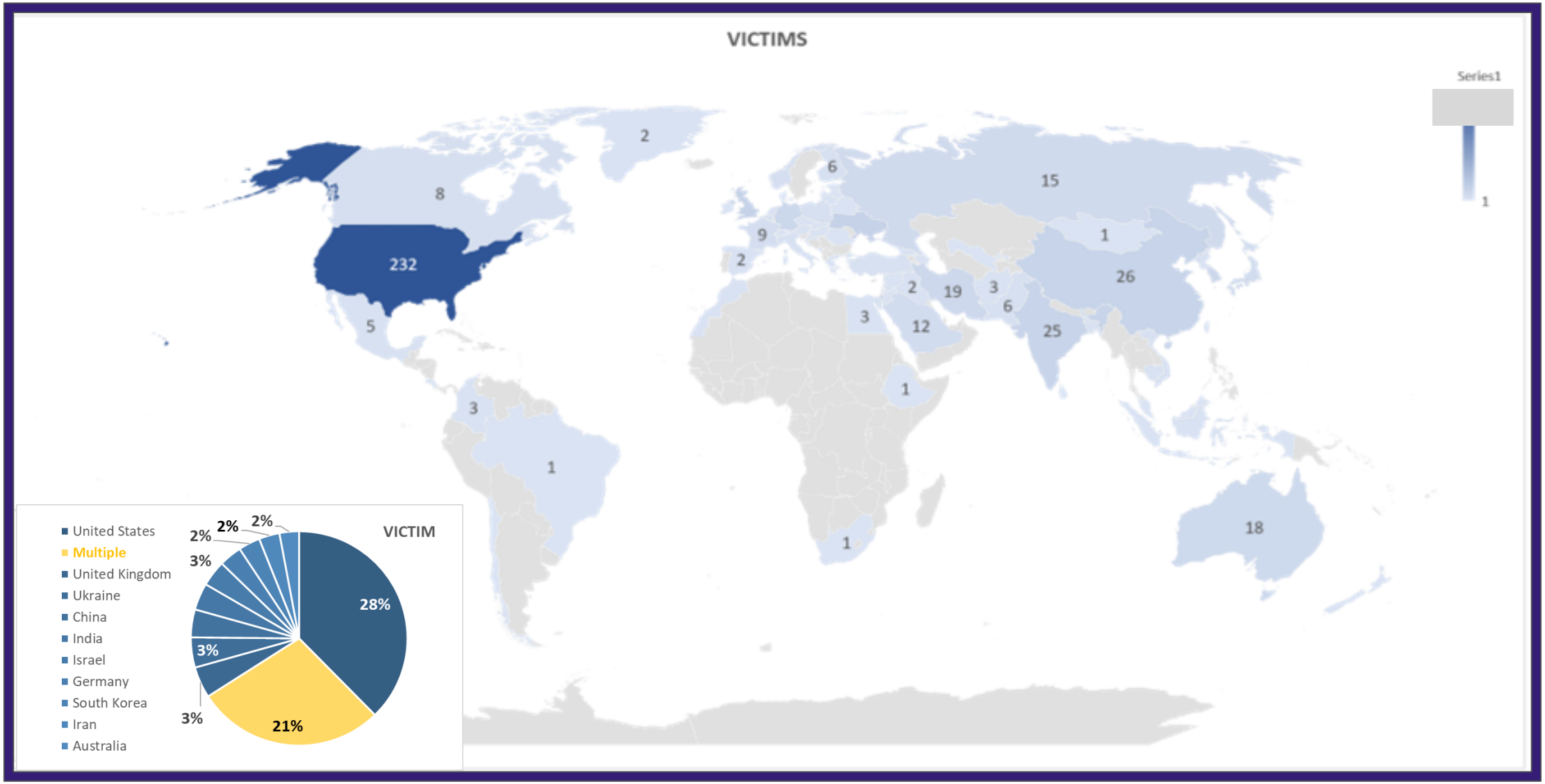
2022 events by 2026

Results

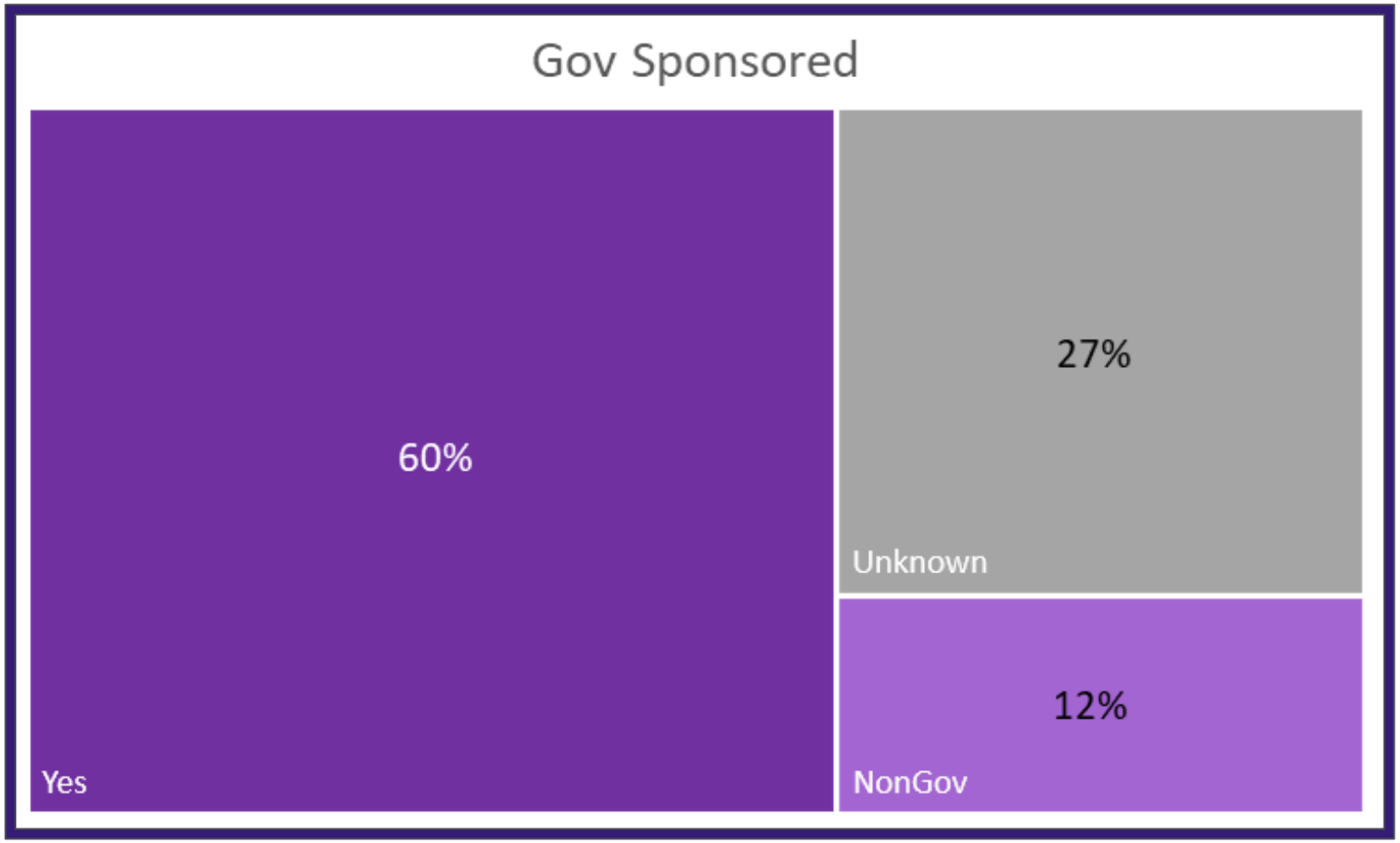

PERPETRATORS
Series1
0
1
169
200
81
28
1
2
2
2
10
2
1
China
Unknown
Russia
Iran
North Korea
United States
Multiple
Pakistan
India
Israel
Vietnam
Palestine
PERPETRATOR
24%
24%
20%
10%
8%
3%
1%
1%
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Ranking of the perpetrators countries

Results



Results

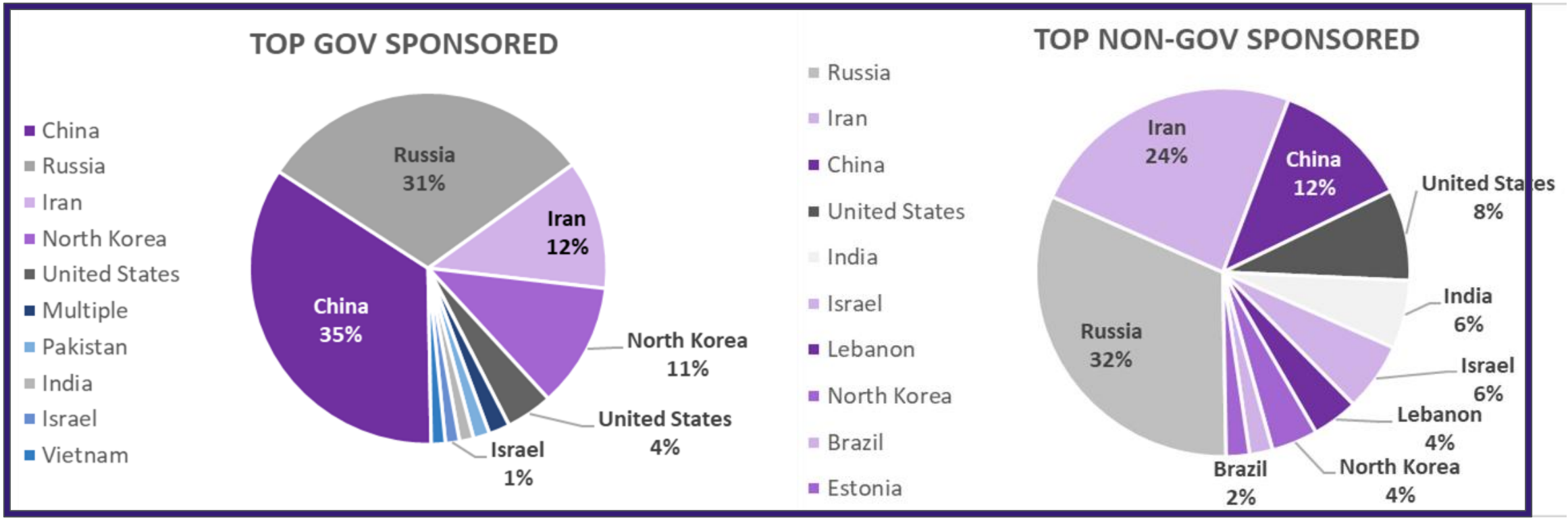


60%
Gov Sponsored

12%
Non-Gov

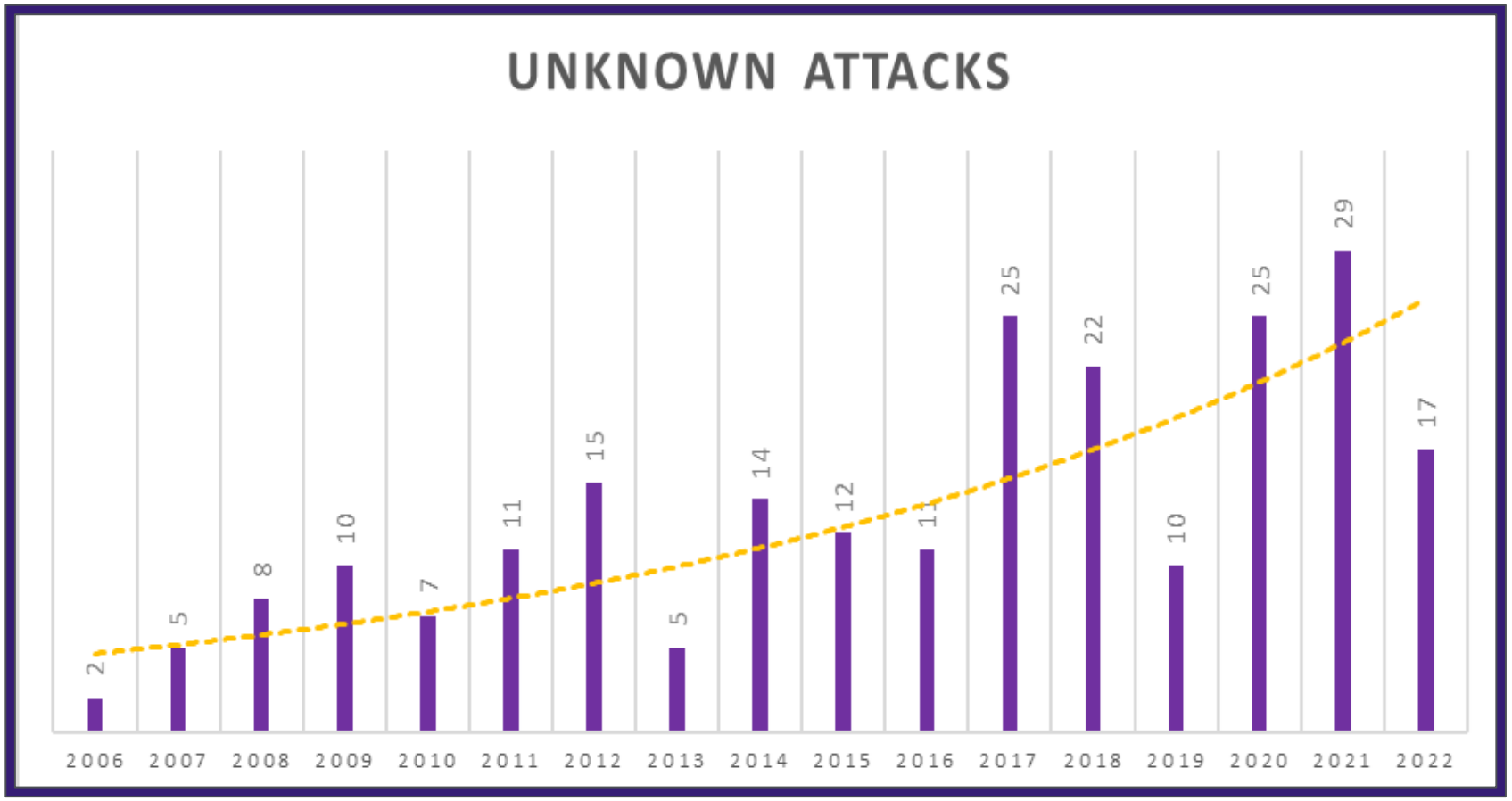
27%
Unknown

Results


TOP GOV SPONSORED
China
Russia
Iran
North Korea
United States
Multiple
Pakistan
India
Israel
Vietnam
Russia 31%
Iran 12%
China 35%
North Korea 11%
United States 4%
Israel 1%
TOP NON-GOV SPONSORED
Russia
Iran
China
United States
India
Israel
Lebanon
North Korea
Brazil
Estonia
Iran 24%
China 12%
United States 8%
India 6%
Israel 6%
Lebanon 4%
North Korea 4%
Brazil 2%
Russia 32%

TESCO METERING

Results



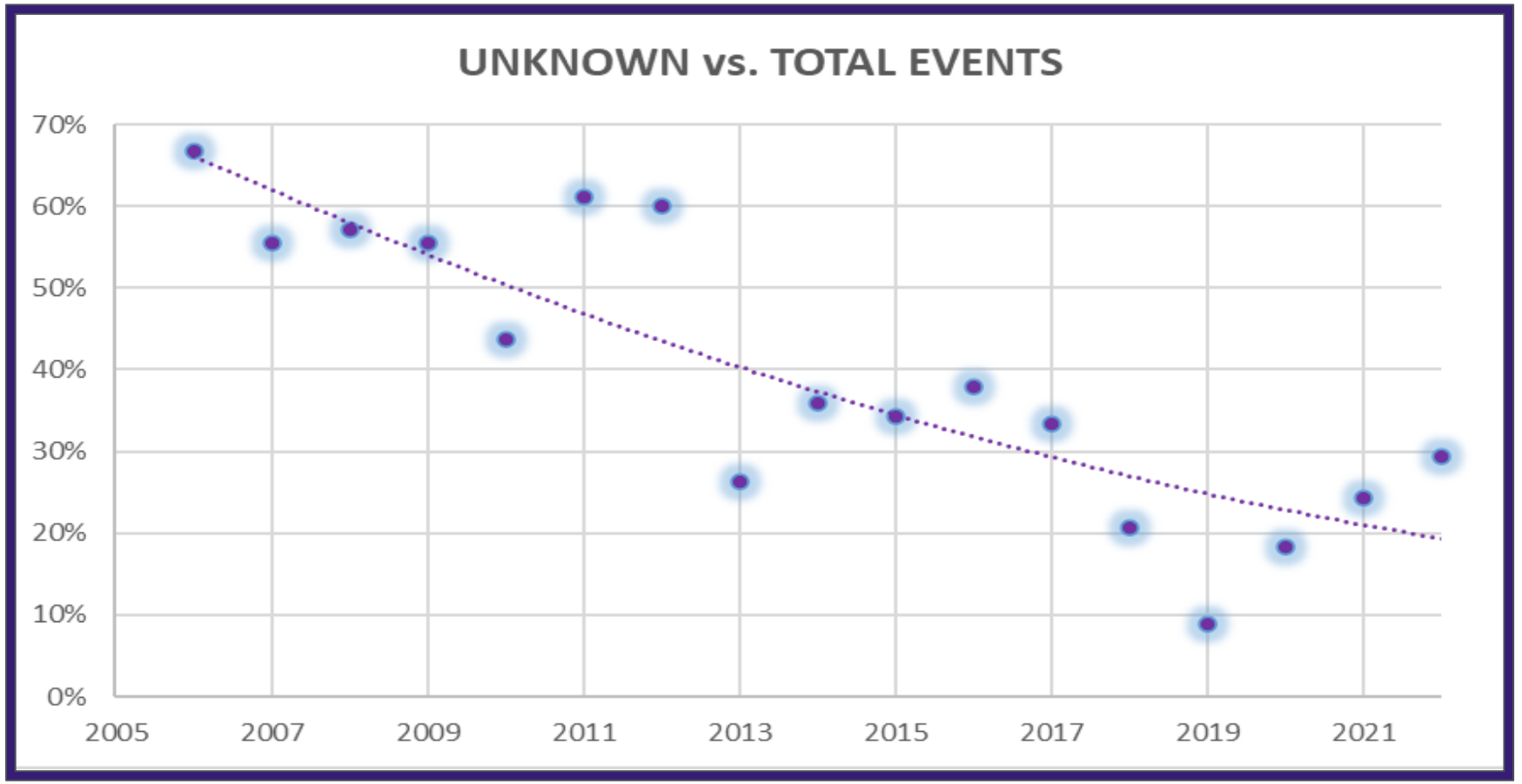
228

Events

20%

Ave. Growth

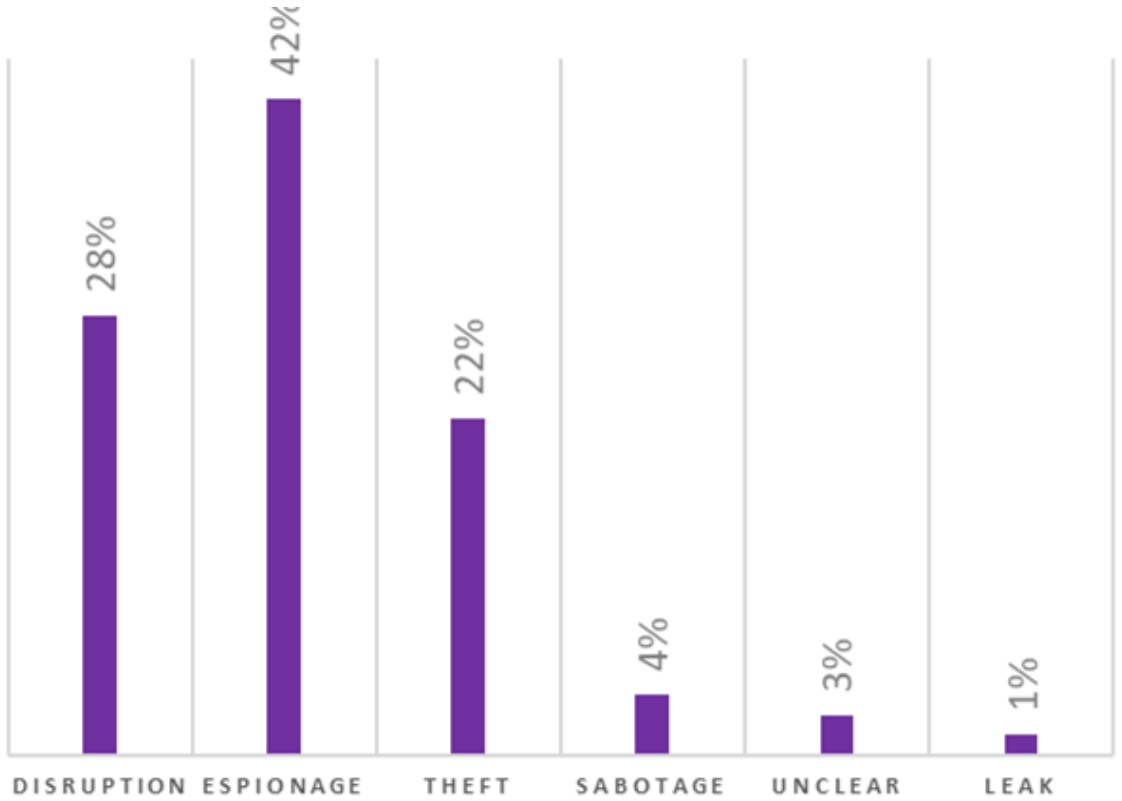
Results



67%
2006

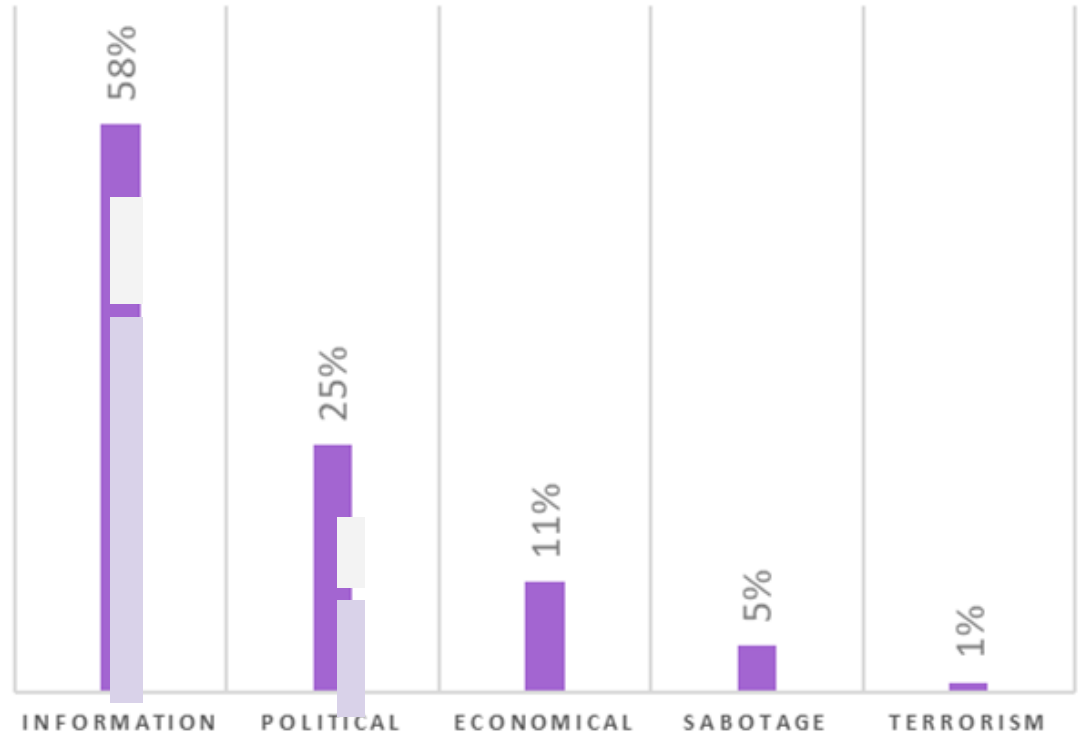
24%
2022

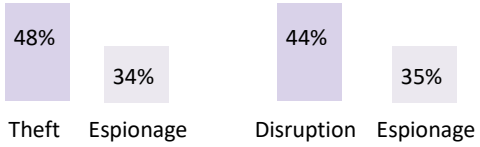
Results



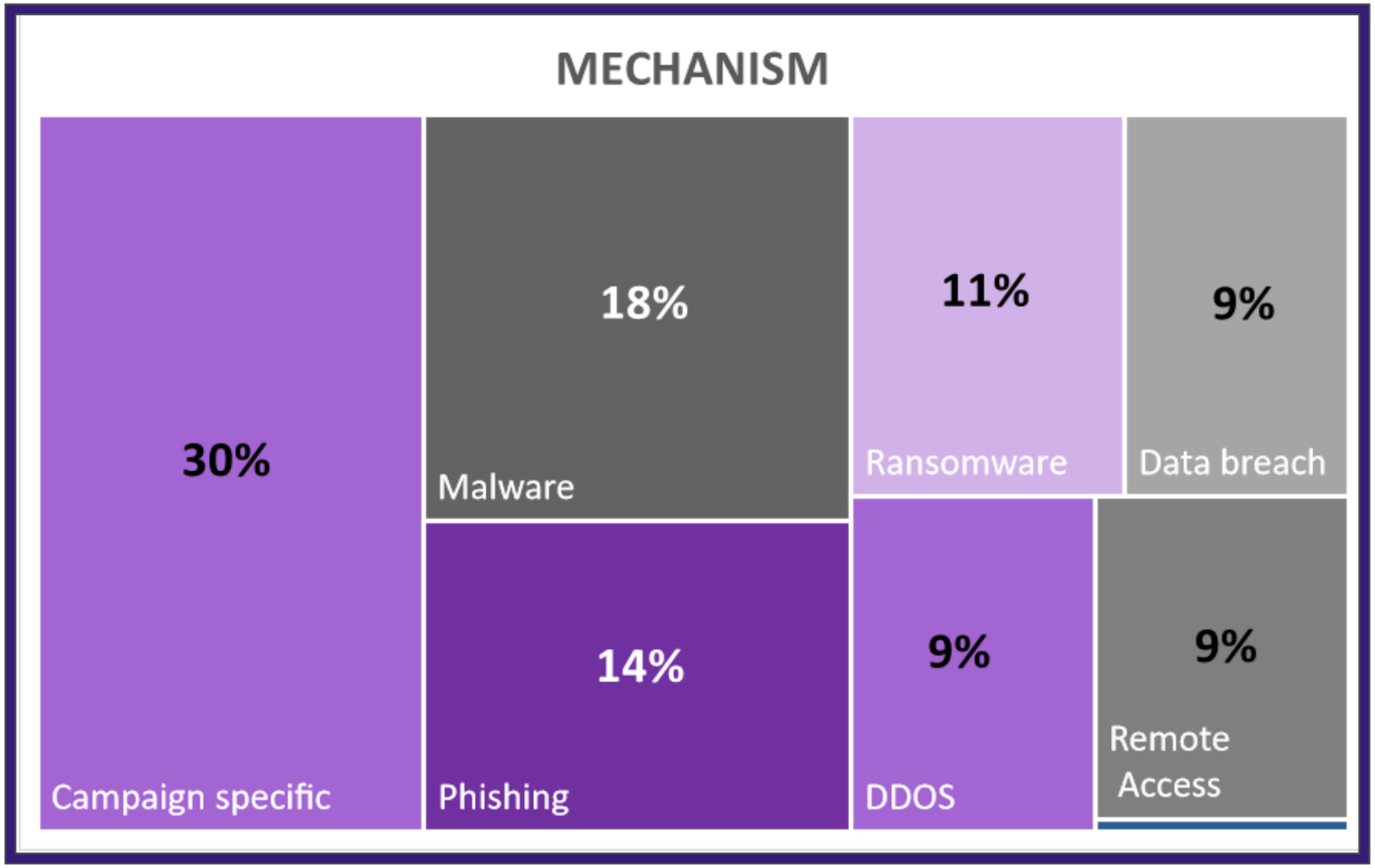
TYPE OF ATTACK

MOTIVATION





Results



60%
Phishing Average Growth

58%
Malware Ave. growth

126%
Ransomware Ave. Growth

CYBER SECURITY

- Cyber standards : ISO 27001, NIST 800-53r3, SOC 2
- Knowing your organizations risks
- Backup and Recovery
- Reducing cyber risk with tools
- Identifying attack vectors for your organization
- Patch Management
- Securing IOT and SCADA
- Security first mindset
- Staying informed with latest threats

CYBER SECURITY STANDARDS

- NIST 800-53r3
- ISO 27001
- SOC 1 – 3
- PCI
- GDPR
- UL 2900

- NIST CSF
- - Coop And Cyber Insurance

TESCO METERING

PROTECTING YOUR DATA

Knowing what kind of data you store,
how its collected and accessed.

Backup and Recovery

- How often can you take backups
- Local backups
- Off-Site backups
- Type of Backups
- Off-Line Backups

- How long can we afford to be down
- How long will it take to recover your data
- Where will you recover to

KNOWING YOUR RISKS

- What kind of data is stored
- Who is accessing your data
- What methods are used to secure access to data or resources

- Open incoming firewall ports
- Web / SFTP / public facing servers
- Data Exchange

Identifying Attack Vectors

- Pen Testing
- Email
- Endpoint Scanners
- End User
- Vendors
- Endpoints
- Exposed SCADA

Patch Management

- Get a baseline of devices
- Assign Responsibilities
- Patch Testing
- Maintain Update Schedule
- Software Standardization
- CVE – Critical Vulnerability and Exposure

Tools and Resources

- Firewalls
- Anti-Virus , EDR , XDR
- RMM
- 2fa whenever possible

- Pen Testing
- Nessus Scanner
- cisa.gov
- haveibeenpwned.com

Summary of Results

- Cyber-attacks are increasing, with not signs of slowing down. CSIS is in line with other data sets.
- Attacks at least will be **double** by 2026.
- **State sponsored** cyber attacks are increasing and represent more than **60% of total case**s.
- **China** is the largest perpetrator, followed closely by **Russia**. **Iran** is slightly ahead of **North Korea** for a third position, and then other nations follow more distantly behind.
- Most of the attacks aim to get **Information** from governments and organizations by espionage and theft **(64%).**
- Attacks are now easily tracked and **just 24% are from unknown** perpetrators compared to 67% in 2006
- **Campaigns** are the common path that perpetrators are using to obtain large amount of data during prolonged periods of time.
- **Ransomware** is the type of attack with higher growth rate in the last five years **(126%).**

More Research

- Cost / benefit to countries
  - Gain - information, monetary value, strategic?
  - Cheaper than other means?
- Will we see this trend continue? Will other countries commit more cyber attacks?
- Why aren’t weaker cyber countries attacked?

CONCLUSIONS

- Digital transformation may put at risk many businesses who may not prioritize, lead, or better manage the risk of their digital assets and dependencies against things like persistent threats.
- The number of attack vectors available in the digital age has increased the number of opportunities for theft and exploitation
- The digital age presents new challenges at a faster pace, and businesses and states may not be adapting quickly enough in the face of a persistent and active threat.
- Risk management practices have been adopted to secure currency and commodities in the financial sector, but this is not in place in the same way for the technology sector. As data is a commodity, perhaps this type of security should be more closely addressed.
- In the face of advanced persistent threats from state actors, additional regulations and state-based support may be needed until a peaceful accord can be reached globally.

SUGGESTIONS FOR WHAT TO DO NOW

- Add a Risk Management program to software and information technology departments

  - Software first, not hardware or networks
  - Systems engineering - DevSecOps
  - Audits and Standards
  - Operational principles like banks
  - Operational Risk management

  - Trade based risk management
  - Economic risk management
  - Regulatory risk management
  - Reputation risk management

- Global regulation - virtual borders

Questions and Discussion

Perry Lawton

Northeast Regional Sales Manager

perry.lawton@tescometering.com

TESCO Metering *Bristol, PA*

215.500.7511

This presentation can also be found under Meter Conferences and Schools on the TESCO website: tescometering.com

ISO 9001:2015 Certified Quality Company
ISO 17025:2017 Accredited Laboratory