Measurability – CyberSecurity Ratings and Its Application to Large Network Infrastructures

William Yurcik */ Centers for Medicare & Medicaid Services (CMS) - USA*

Collaborators:

Rhonda O'Kane */ Bitsight Technologies - USA*

Stephen North */ Infovisible - USA*

O. Sami Saydjari */ Dartmouth College - USA*

Fábio Miranda, Rodolfo Avelino, & João Vieira */ Insper - Brazil*

Gregory Pluta */ University of Illinois @ Urbana-Champaign - USA*

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Official Organizational Disclaimer:

"The views presented herein do not represent the views of the Federal Government."

Quote - 1

"If you can't measure it then you can't manage it."

falsely attributed to Peter Drucker and/or W. Edwards Deming

Quote - 2

"Risks cannot be managed better until they can be measured better."

Ross Anderson and Tyler Moore,
"The Economics of Information Security,"
Science, Nov 2006.

Quote - 3

"One of the most dangerous aspects of … security … is that you can almost measure it."

Matt Blaze,
"Afterword" within Bruce Schneier's
"Applied Cryptography 2nd Edition." 1996.

Quote - 4

"It is a capital mistake to theorize before one has data.

Insensibly one begins to twist facts to suit theories, instead of theories to suit facts."

Sir Arthur Conan Doyle, 1887.

Dogbert on Measured Data

Agenda

Problem Introduction

Metrics

Ratings

Application to a National Infrastructure

Summary

Agenda

Problem Introduction

Metrics

Ratings

Application to a National Infrastructure

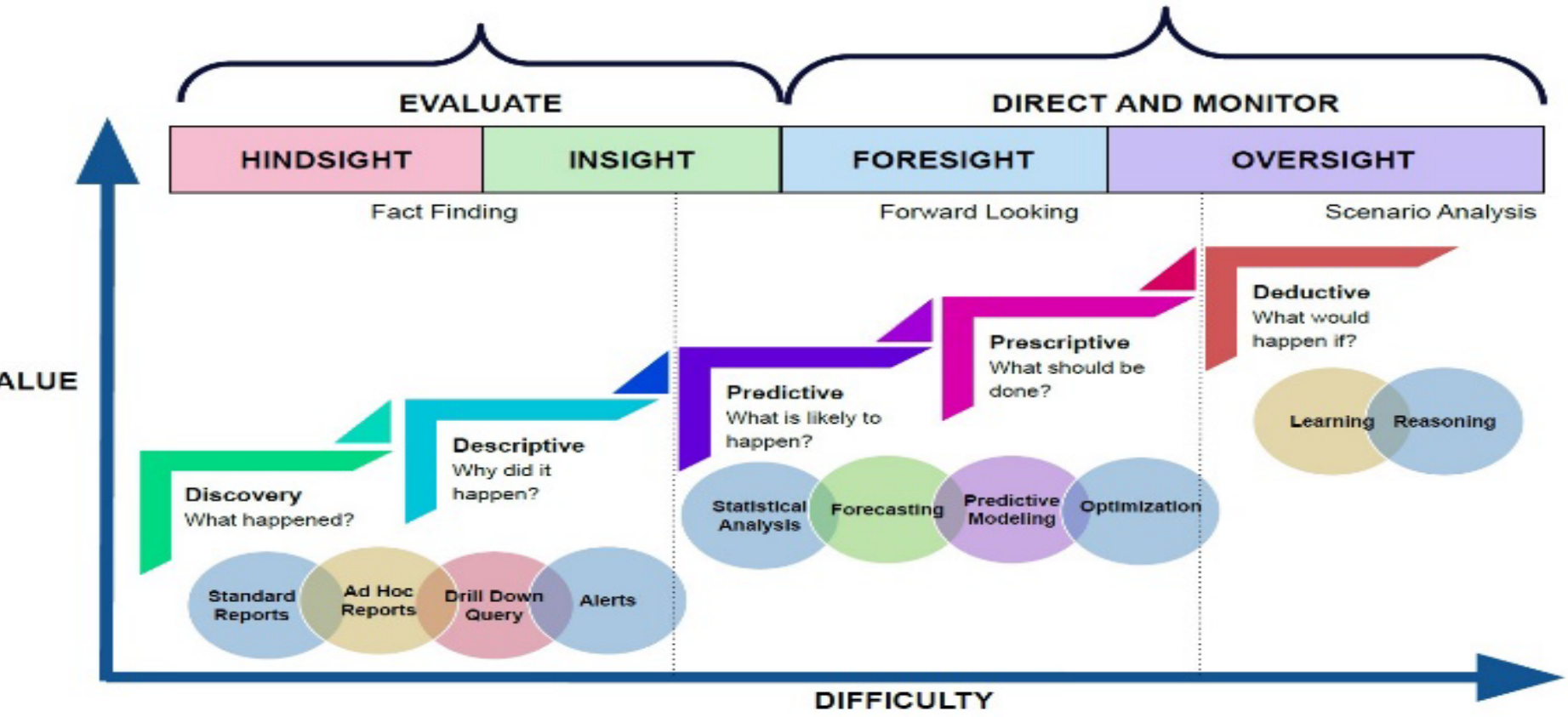
Summary

Introduction

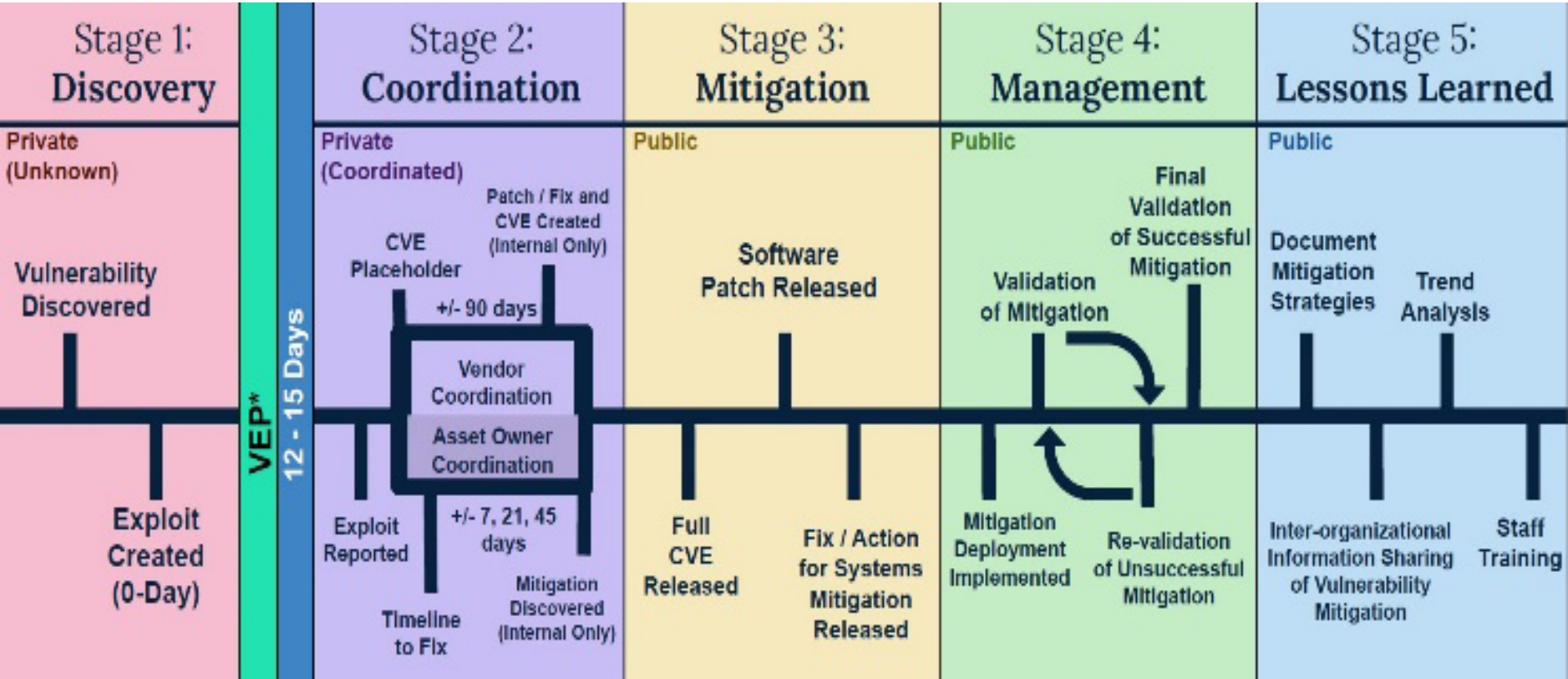
- **There is an important need to understand an enterprise's security posture – how are we doing?**

- **<u>Quantitative</u> security measurements are needed**
  - **Benchmarking for comparison**
  - **Return-On-Investment (ROI)**

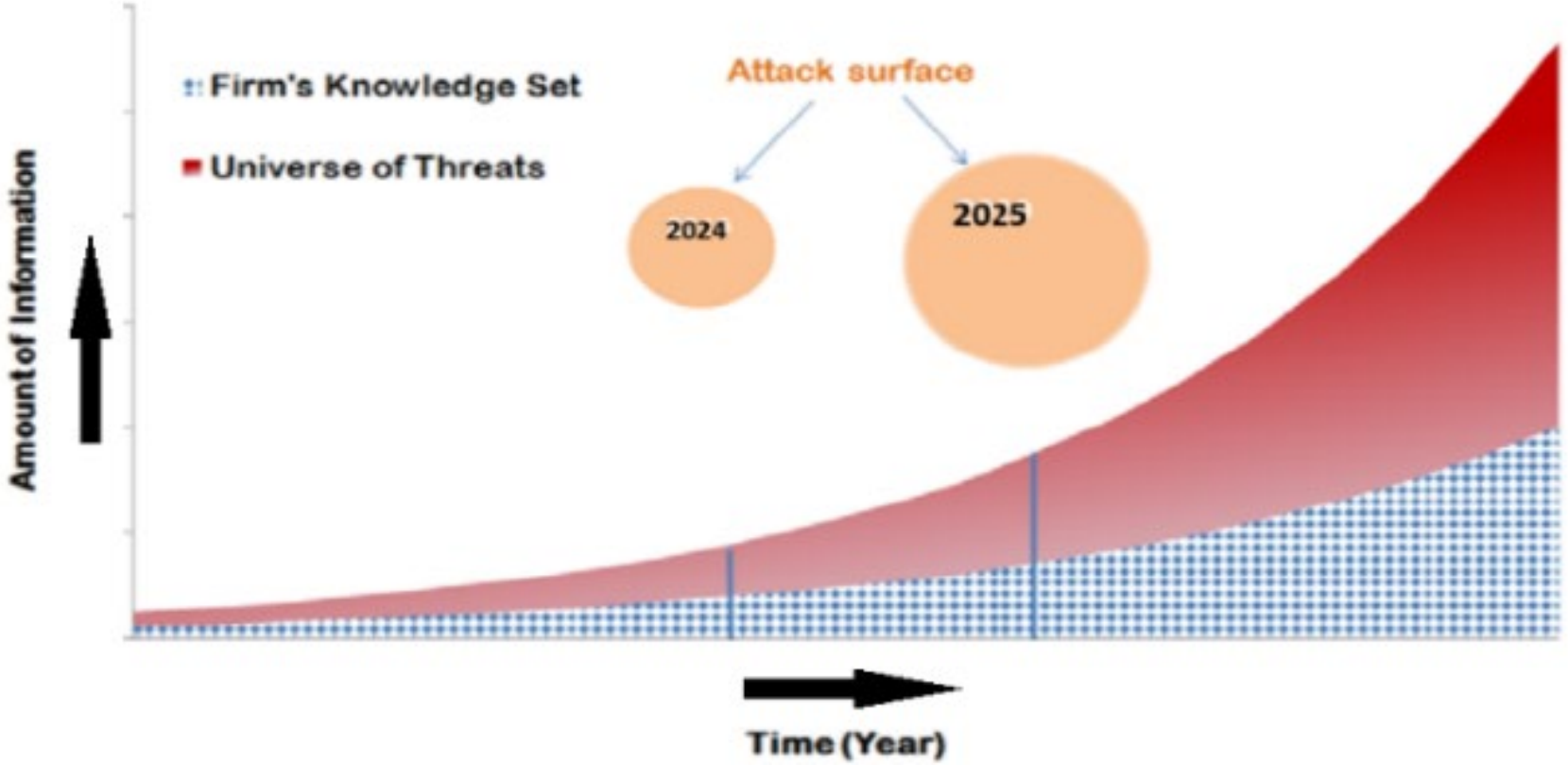
Security Operations



Software Vulnerability Mitigation



Attack Surface Knowledge Gap



Introduction

- **How do we measure security?** ***(hint: metrics)***
- ***"Perfect"*** **is the enemy of the** ***"Good-Enough"***
- **Which Metrics??????**

Agenda

Problem Introduction

Metrics

Ratings

Application to a National Infrastructure

Summary

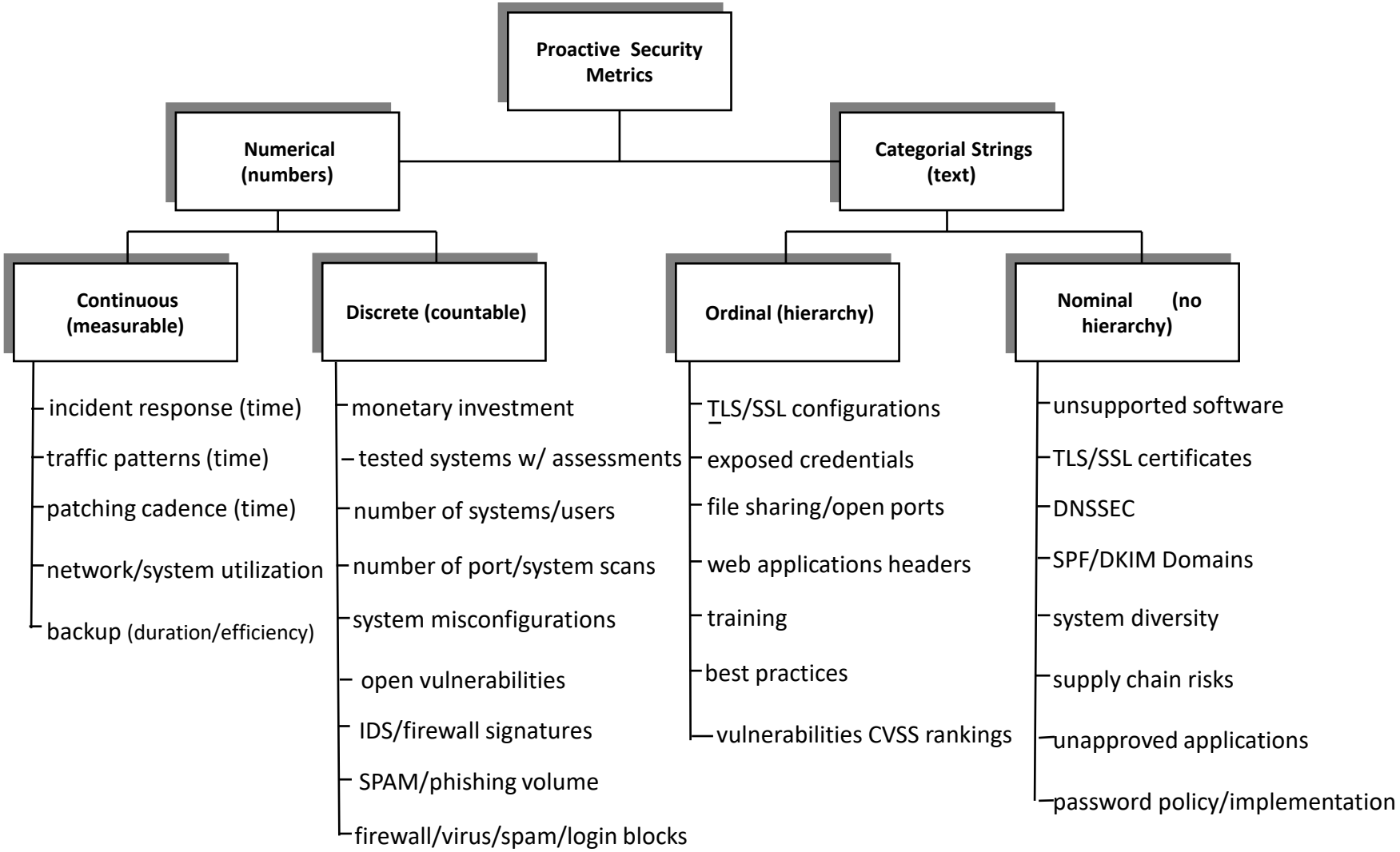
Which Metrics???

NIST Computer System Security and Privacy Advisory Board (CSSPAB) ***"Approaches to Measuring Security"*****, June 2000**

Workshop on Security Metrics (MetriCon) **2006-2019**

International Workshop on Security Measurements and Metrics (MetriSec) **2010-2012**

International Workshop on Quantitative Aspects in Security (QASA**) 2012-2017**


Proactive Security Metrics
Numerical (numbers)
Categorial Strings (text)
Continuous (measurable)
Discrete (countable)
Ordinal (hierarchy)
Nominal (no hierarchy)
incident response (time)
traffic patterns (time)
patching cadence (time)
network/system utilization
backup (duration/efficiency)
monetary investment
tested systems w/ assessments
number of systems/users
number of port/system scans
system misconfigurations
open vulnerabilities
IDS/firewall signatures
SPAM/phishing volume
firewall/virus/spam/login blocks
TLS/SSL configurations
exposed credentials
file sharing/open ports
web applications headers
training
best practices
vulnerabilities CVSS rankings
unsupported software
TLS/SSL certificates
DNSSEC
SPF/DKIM Domains
system diversity
supply chain risks
unapproved applications
password policy/implementation

“Good Enough” Cybersecurity Metrics

01	Bitsight Security Rating	08	Web Application Headers
02	Patching Cadence	09	User Behavior
03	Desktop Software	10	TLS/SSL Configurations
04	Potentially Exploited Systems	11	Open Ports
05	Mobile Software	12	TLS/SSL Certificates
06	Botnet Infections	13	Spam Propagation
07	Insecure Systems	14	Unsolicited Communications

Source: Independent analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Assign Weights to Metrics

Rating Overview

Rating Overview Panel shows how well this company is managing each risk vector. Click on a risk vector to see more details about the risk.

Compromised Systems=27%

- Botnet Infections
- Spam Propagation
- Malware Servers
- Unsolicited Communications
- Potentially Exploited

User Behavior=2.5%

- File Sharing 2.5%
- Exposed Credentials **

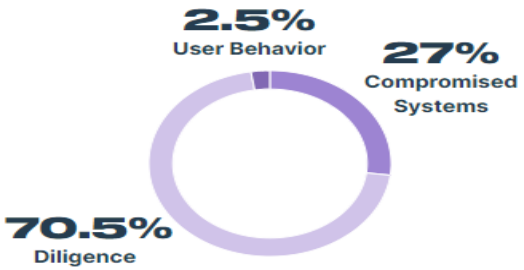
Public Disclosures

- Security Incidents/Breaches
- Other Disclosures *

Diligence=70.5%

- SPF Domains 1%
- DKIM Records 1%
- TLS/SSL Certificates 10%
- TLS/SSL Configurations 15%
- Open Ports 10%
- Web Application Headers 5%
- Patching Cadence 20%
- Insecure Systems 2.5%
- Server Software 2%
- Desktop Software 3%
- Mobile Software 1%
- DNSSEC *
- Mobile Application Security *
- Web Application Security *
- Domain Squatting **

What Makes A Security Rating?



Weight of each risk category on the rating. Public disclosures may impact the Bitsight rating, but risk vectors in this category do not have a fixed weight.

Learn more about how ratings are calculated.

Learn more about every risk vector.

Agenda

Problem Introduction

Metrics

Ratings

Application to a National Infrastructure

Summary

A Cybersecurity Rating is a data-driven dynamic measurement of an organization's cybersecurity performance used to manage enterprise and third-party cyber risk.

Systematized Weighted Algorithm

The overall / headline rating is calculated based on the risk vector grades and adjusted to spread out the range between 300 - 820.

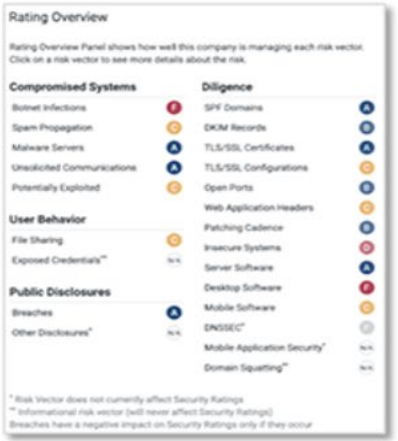
The platform stores a perpetual history of all events and diligence observations, and displays a 12 month rolling history.

BitSight maps all distinct entities of the organization and provides context through operational entity breakouts.

Headline ratings and risk vector grades are calculated for each entity for granular oversight and management.

Letter grades (A, B, C, D, F) assigned to each of the 21 risk vectors (2 additional risk vectors are informational only)

Grades are normalized across organizations by size and to the average across our inventory.



Compromised / infected systems
- Bots/malware
- Adware / spyware
- Port scanning
- Hosted exploits
- Spam

Derived from our own botnet sinkhole infrastructure, honeypots, spam traps, and MalTracker.net

File sharing, analysis of BitTorrent directories

Publicly Disclosed Breaches

Exposed credentials (paste sites, dark web)

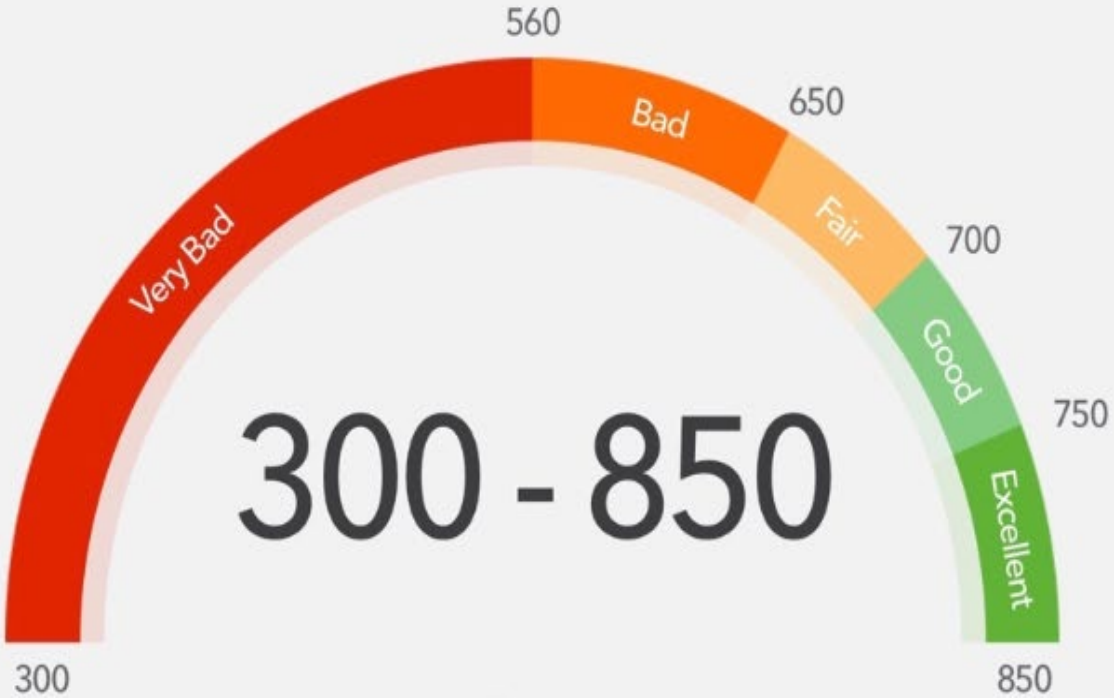
Configuration hygiene, including
- Open ports
- Encryption (certs, configs)
- Patching / unsupported software
- Email security
- Web application security
- Mobile application security

Derived port scanning and protocol / banner analysis, passive DNS analysis, web request analysis, and mobile app analysis.

Each observation is assigned a severity of Good, Fair, Neutral, Warn, or Bad

Consumer Credit Score

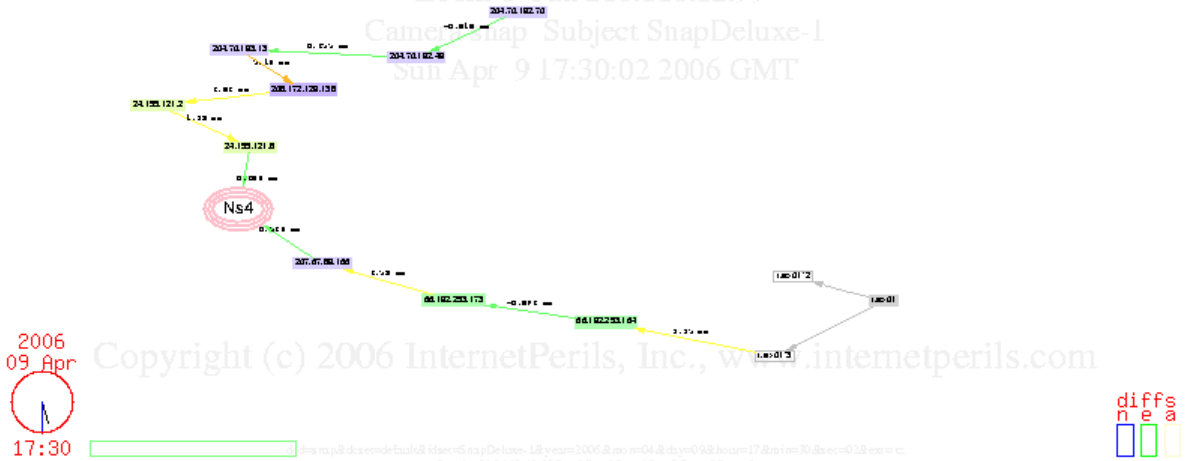
Credit Scores Factors



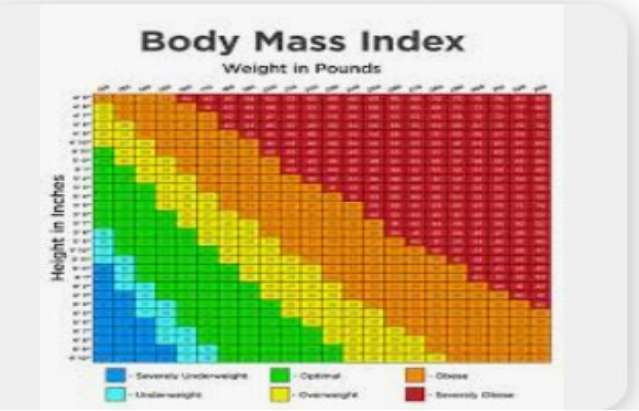
Payment history	35%
Amounts owed	30%
Length of credit history	15%
New credit	10%
Types of credit used	10%

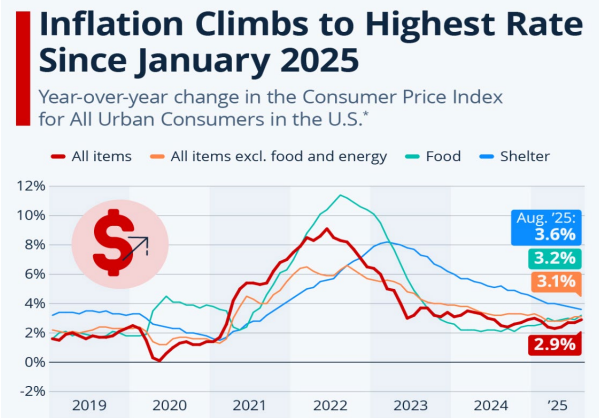
A Cybersecurity Rating is a data-driven dynamic measurement of an organization's cybersecurity performance used to manage enterprise and third-party cyber risk.

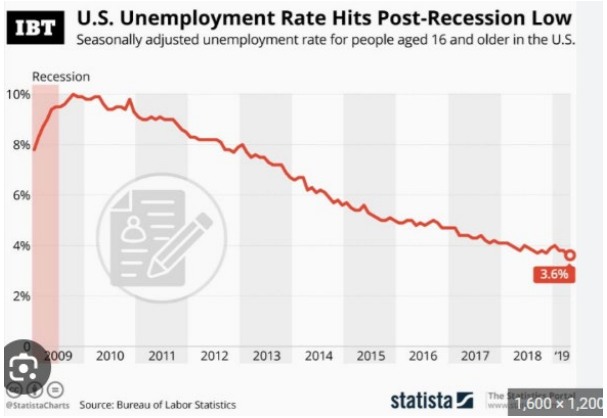
Continuous Monitoring in Time

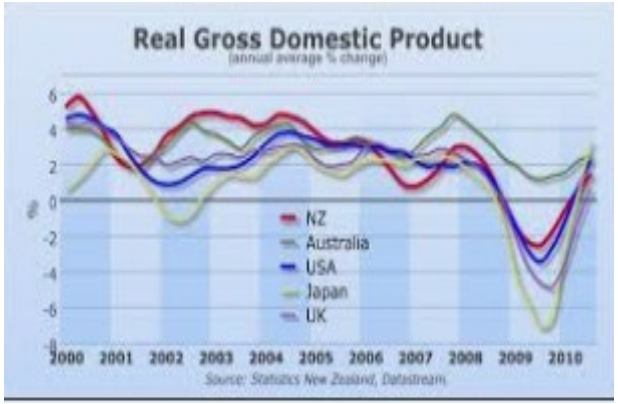


Dynamic Ratings & Indexes

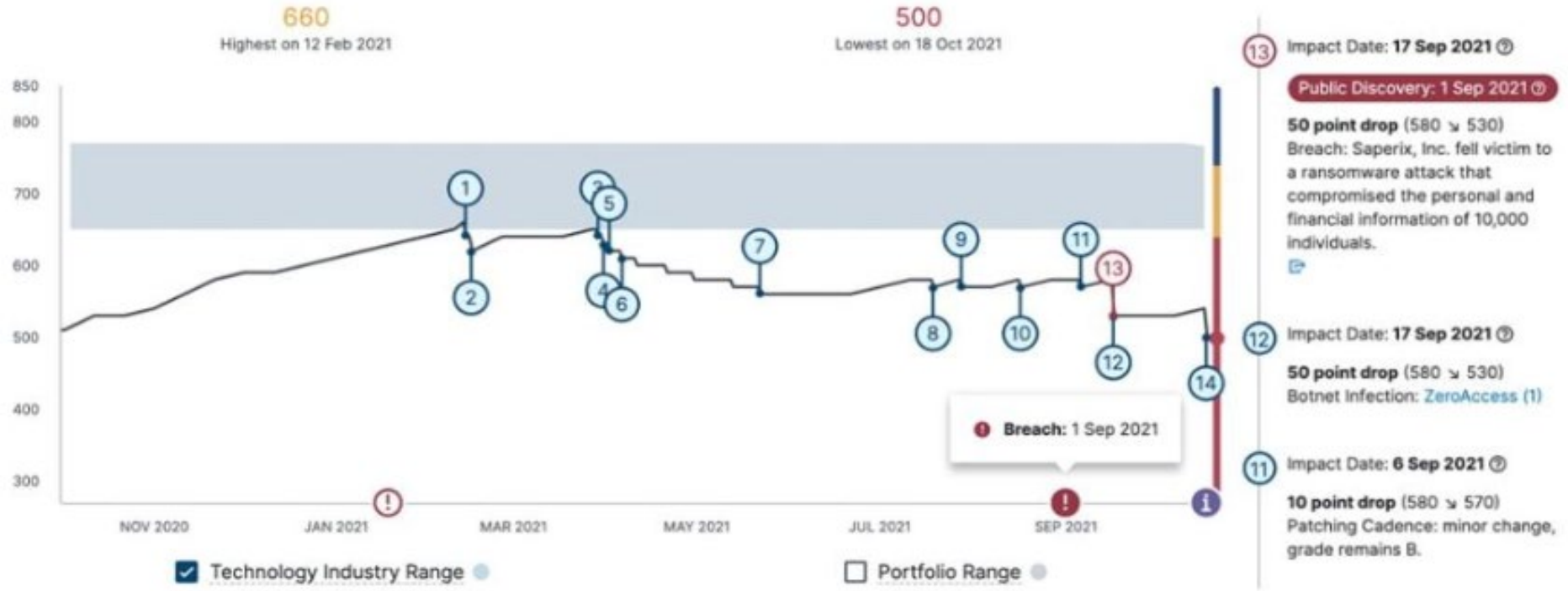








Longitudinal Rating Sparkline



Agenda

Problem Introduction

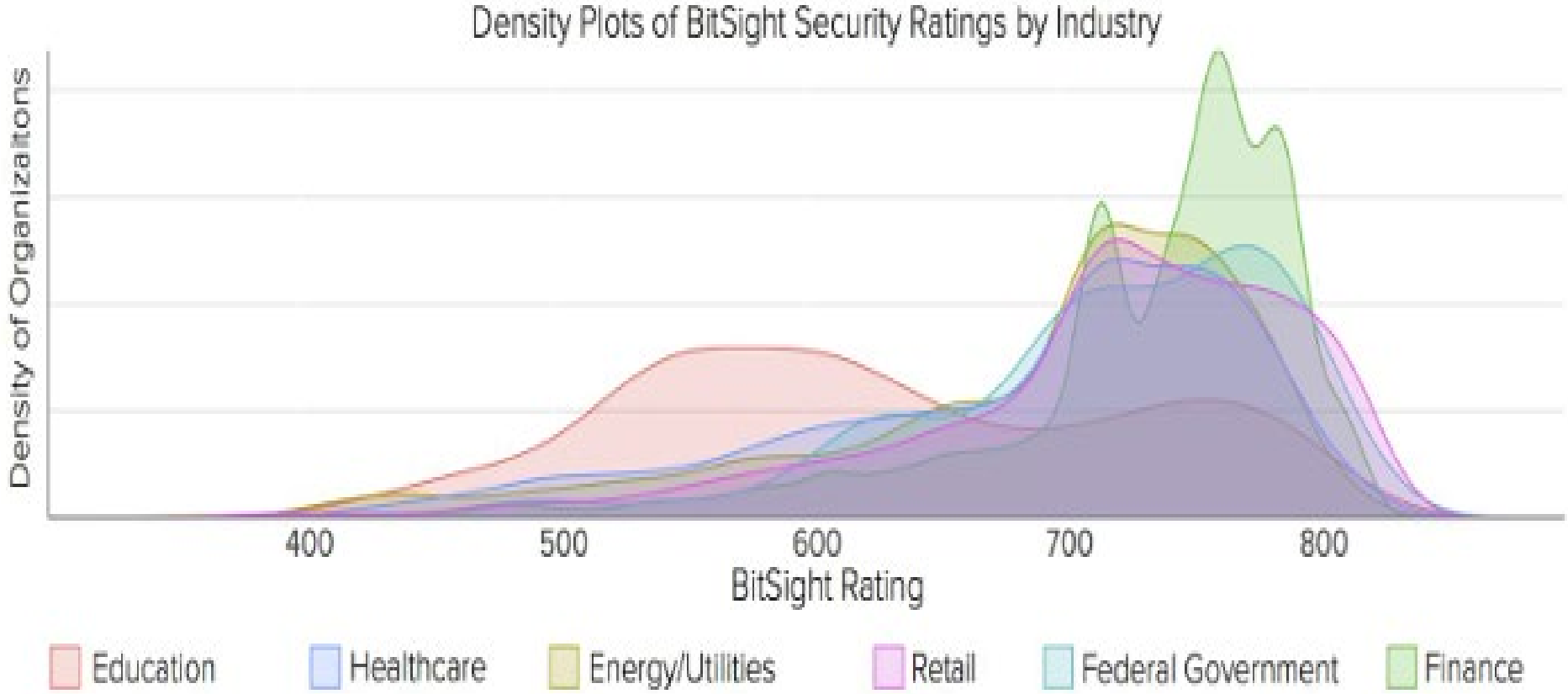
Metrics

Ratings

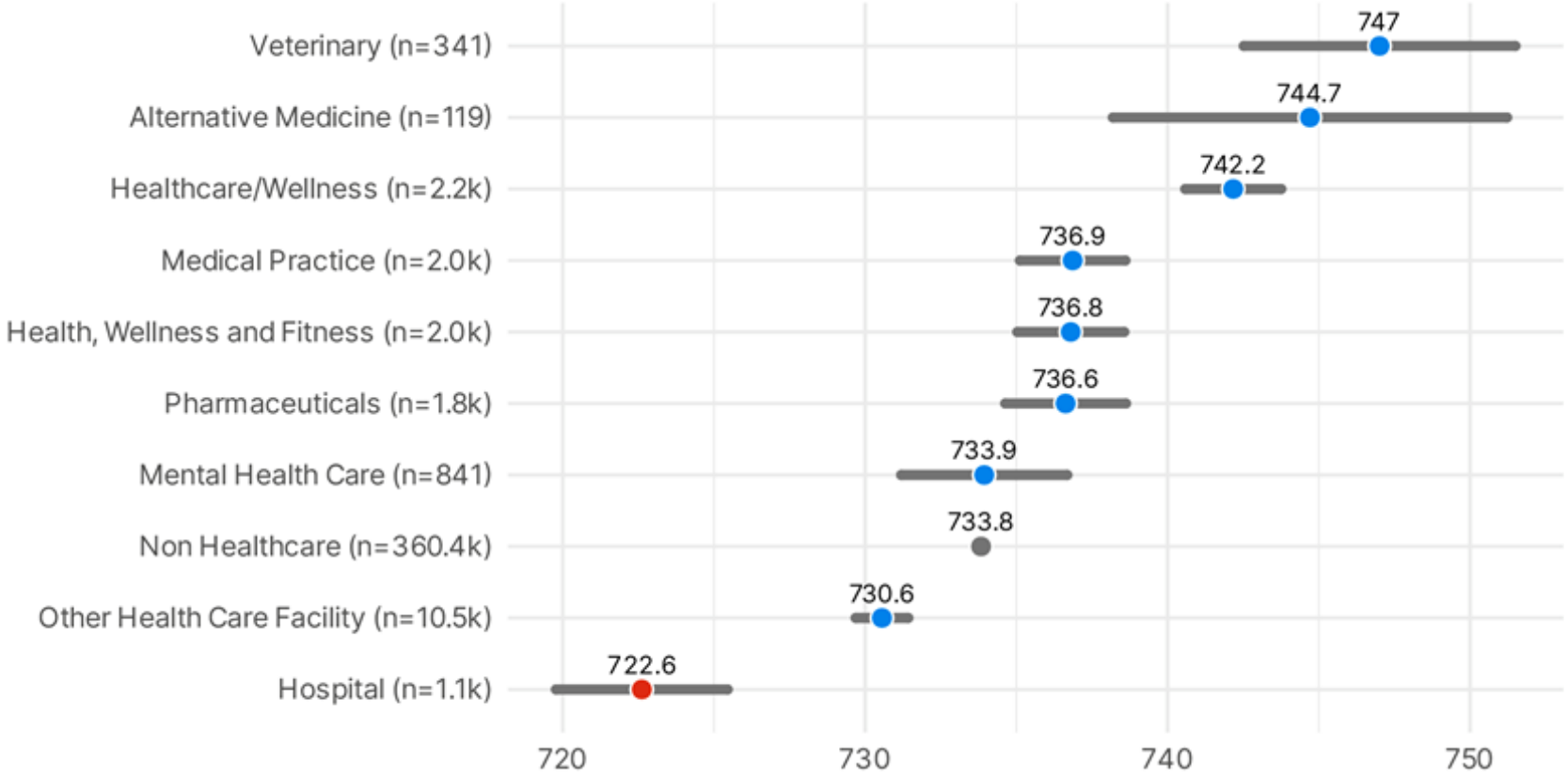
Application to a National Infrastructure

Summary

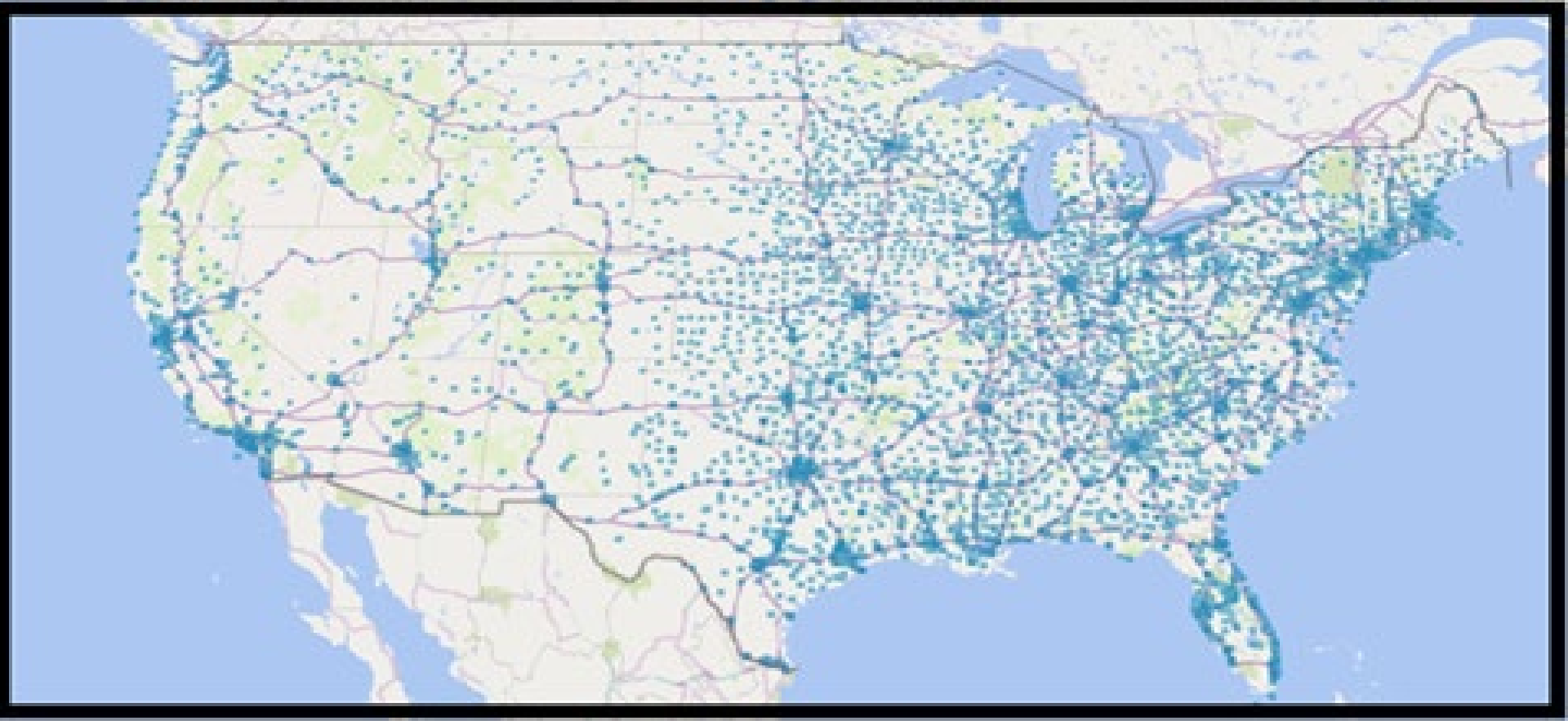
Application Domain?



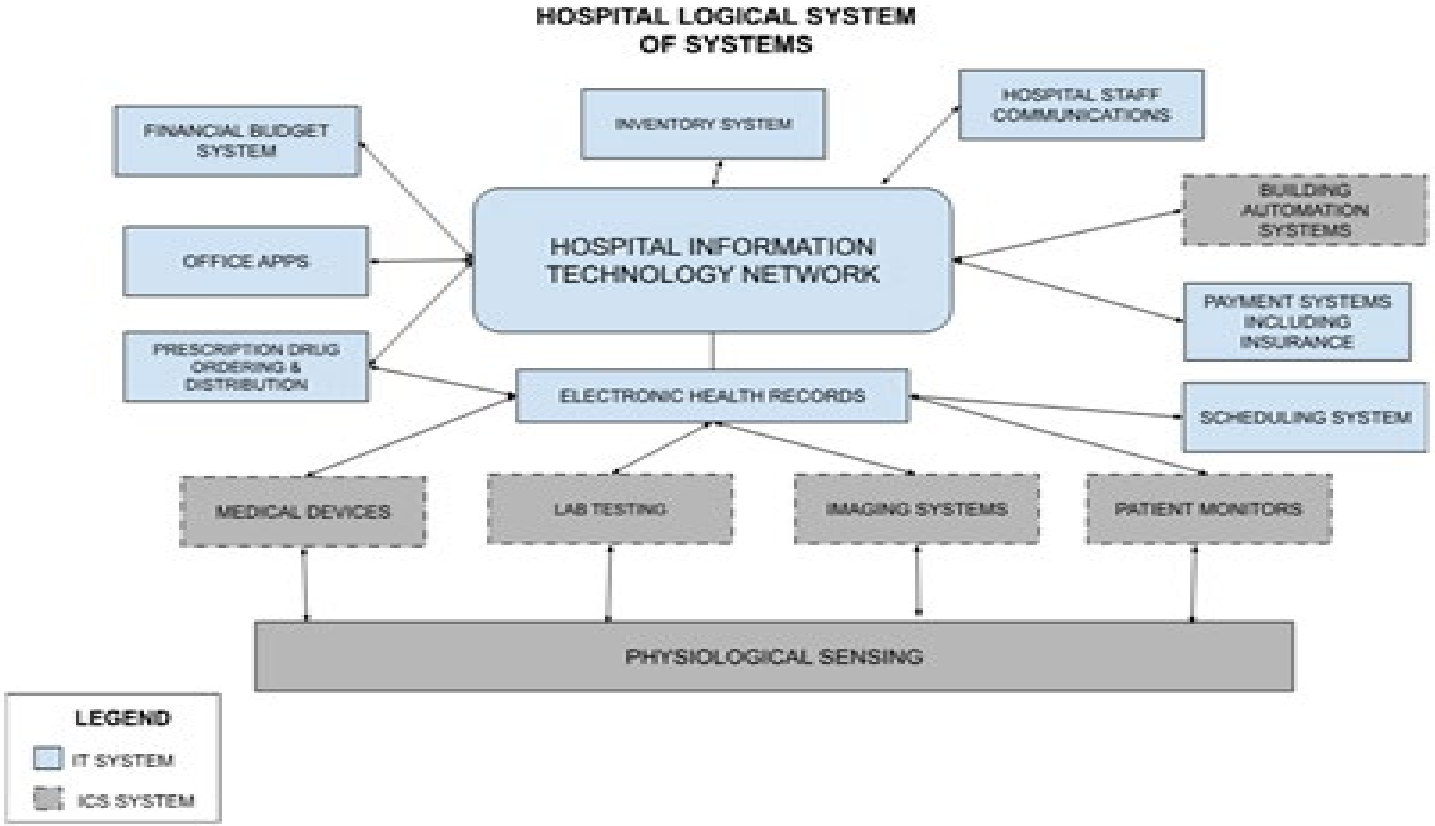
U.S. Healthcare



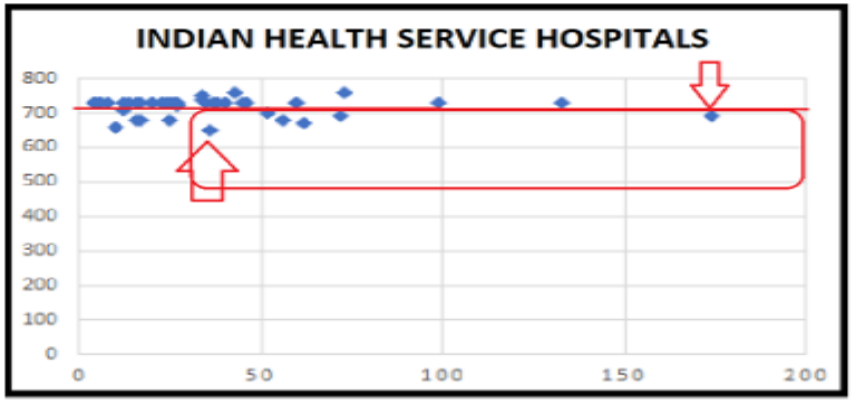
U.S. Healthcare National Infrastructure

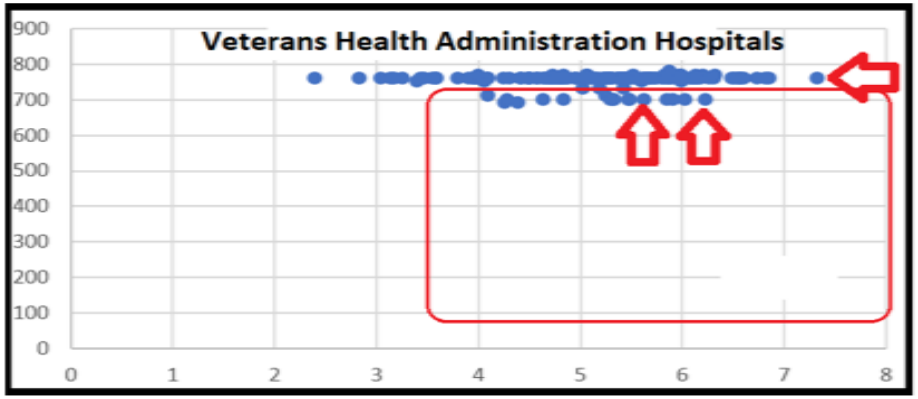


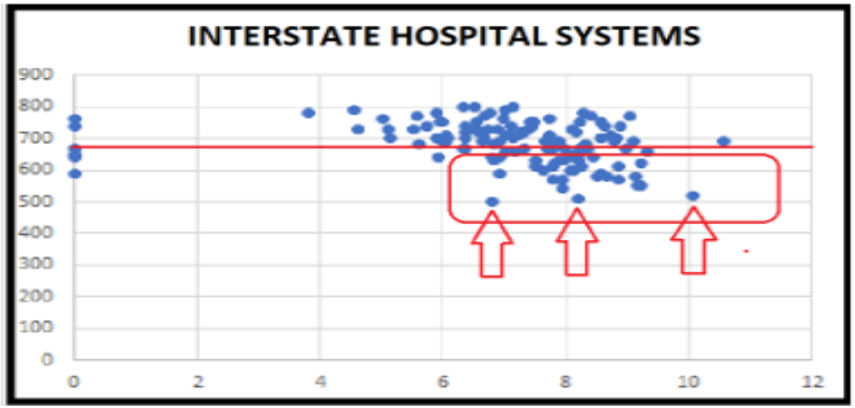
Hospital System-of-Systems

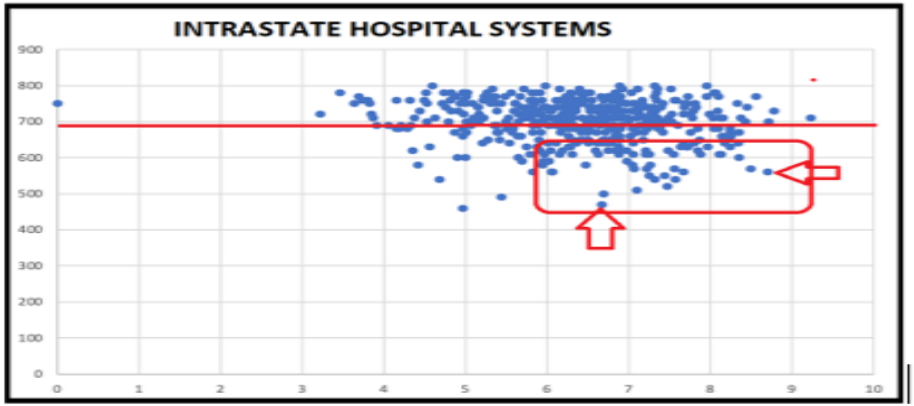


Results – Large Hospital Systems



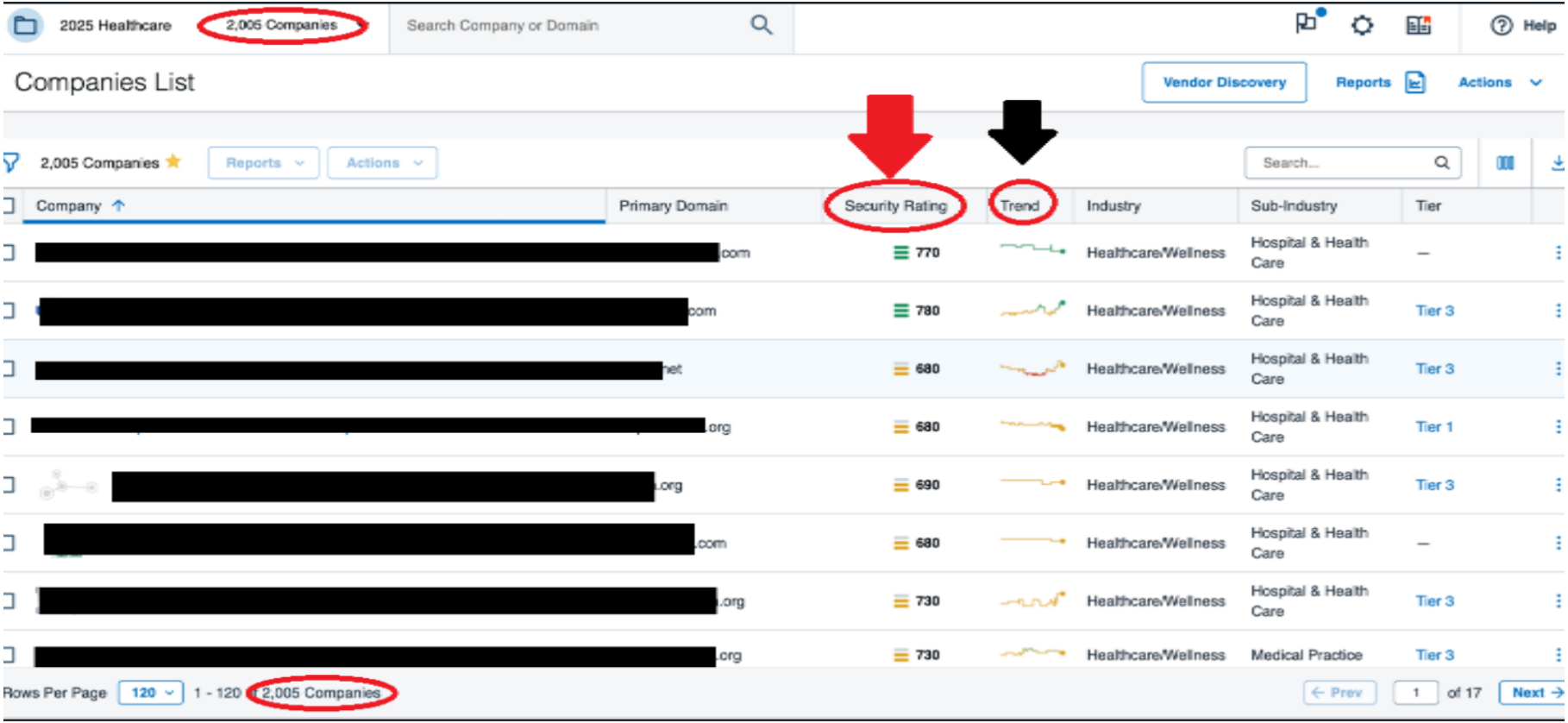




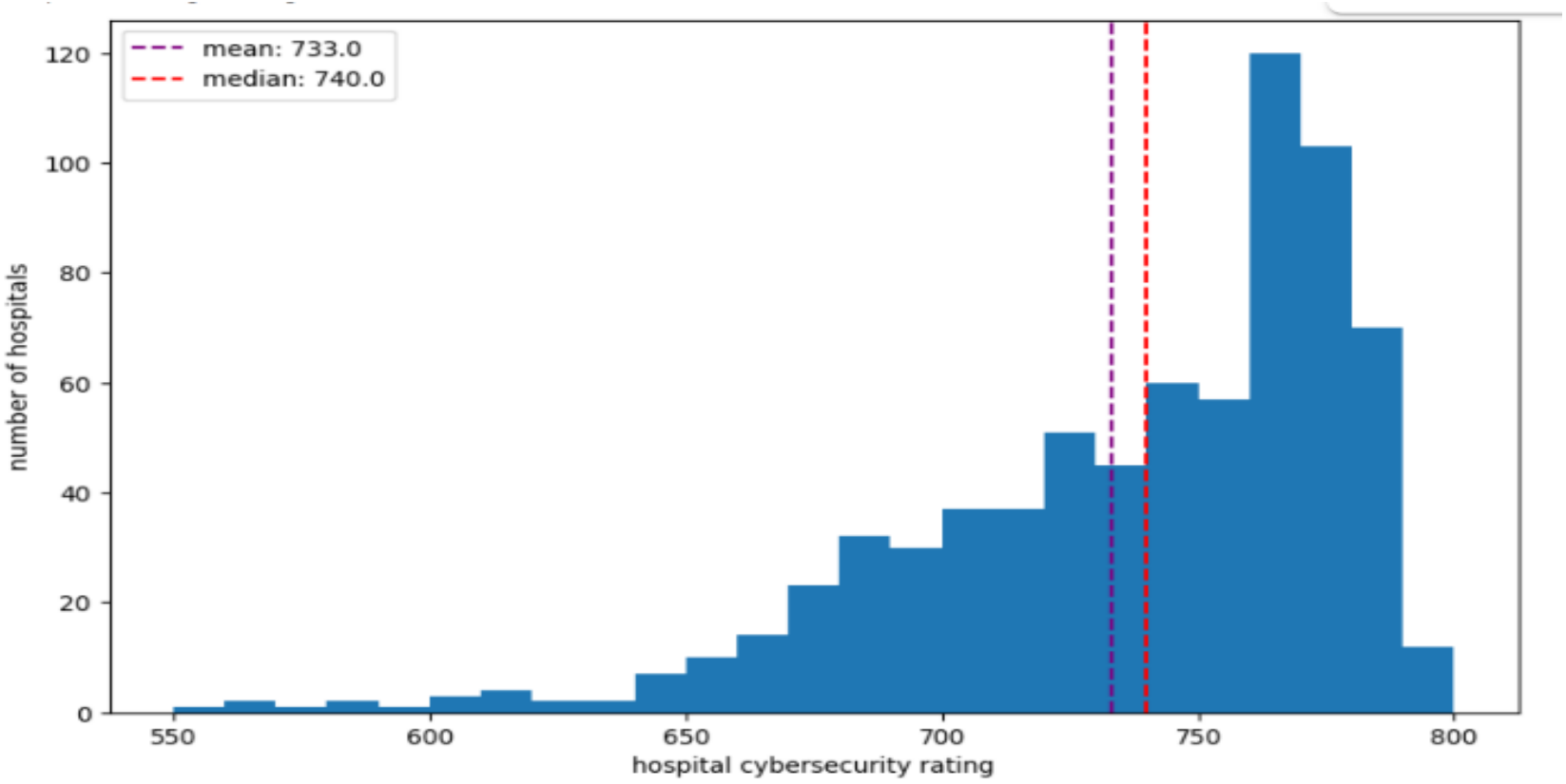


U.S. Rural Hospitals

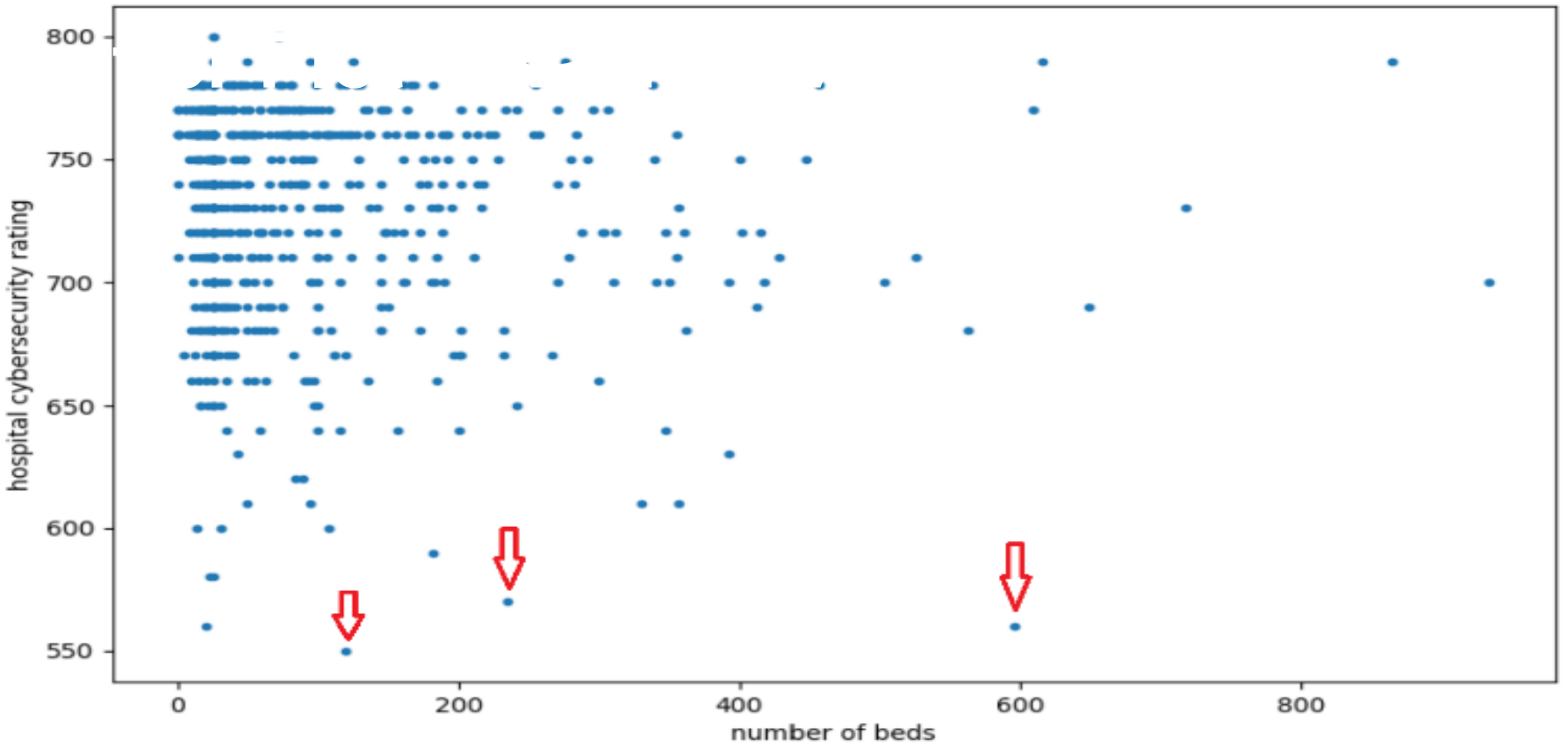
Rural Hospital Ratings



Rural Hospital Rating Freq Distr



Scatter Plot – Ratings vs Hosp Size



Agenda

Problem Introduction

Metrics

Ratings

Application to a National Infrastructure

Summary

Summary

- ***Cybersecurity assessment can be imperfectly measured by cybersecurity ratings***
    - ***cybersecurity ratings currently underpin the growing cyberinsurance industry***
- ***Cybersecurity ratings are dynamic in time demanding automation***
- ***Cybersecurity ratings enable easily measurable Return-On-Investment (ROI) calculations***

Thank You!
for feedback my email address is below:

William Yurcik*

Centers for Medicare & Medicaid Services (CMS)

< william.yurcik@cms.hhs.gov >

**** Official Organizational Disclaimer: "The views presented herein do not represent the views of the Federal Government."***

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES