Cybersecurity Overview & Tabletop Exercises

2022 Community Bankers Workshop

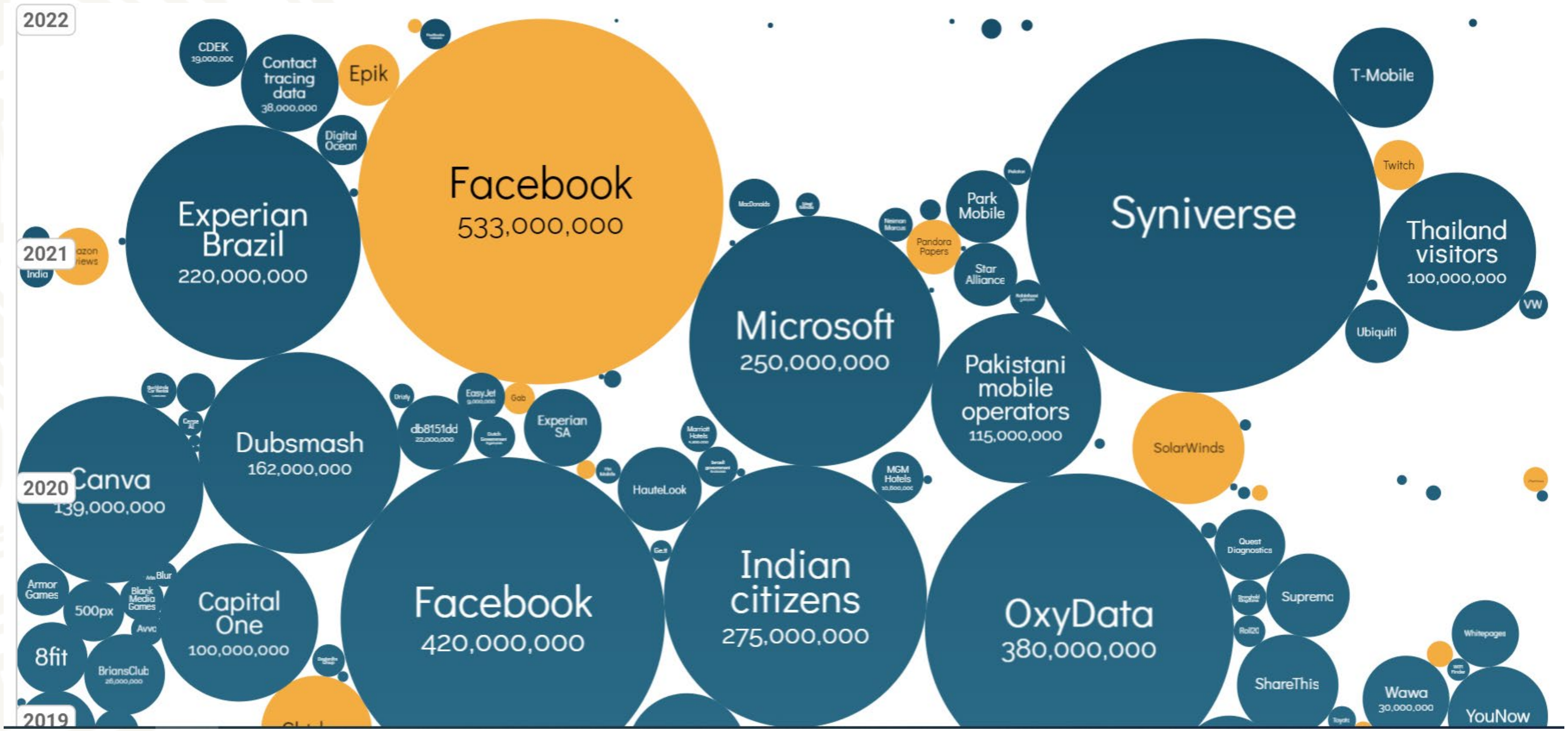
Objectives

- Cybersecurity Breach Statistics
- Cybersecurity Controls Banks can Implement
- Incident Response Plan & Regulatory Notification
- Vignette 7 - Ransomware
- Vignette 9 - Supply Chain
- Cybersecurity Insurance
- Conclusions and Resources

World's Biggest Data Breaches & Hacks

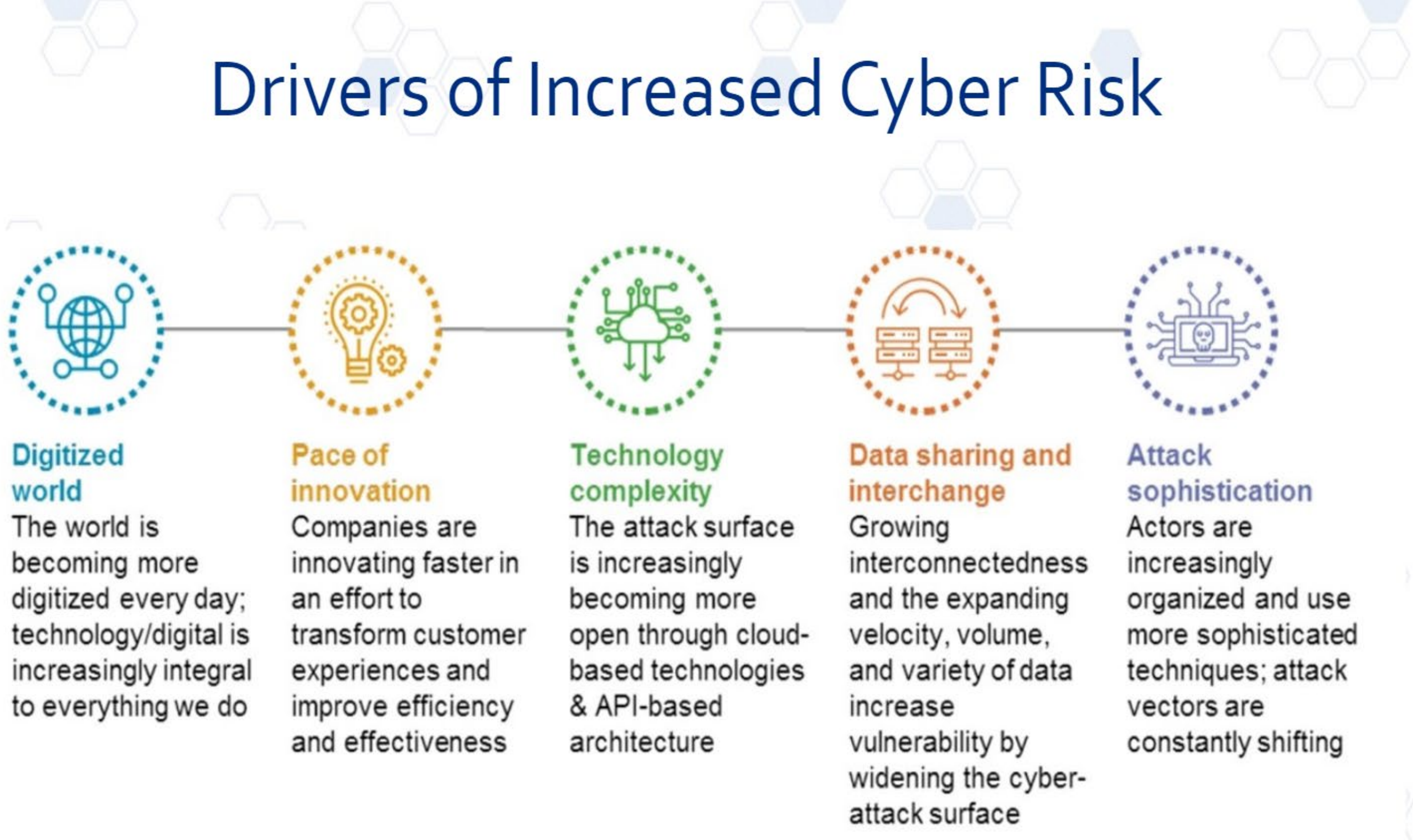
Selected events over 30,000 records

UPDATED: May 2022



Source: www.informationisbeautiful.net

Cybersecurity Breach Statistics



Cybersecurity Breach Statistics

The Verizon Data Breach Investigation Report Annual Publication

- 23,896 security incidents
- 5,212 confirmed data breaches
- Eight common attack patterns
- Attack frequency, threat actors, motives, and data type compromised
- Eleven specific business sectors analyzed, including the financial and insurance sector

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Patterns

All Industries

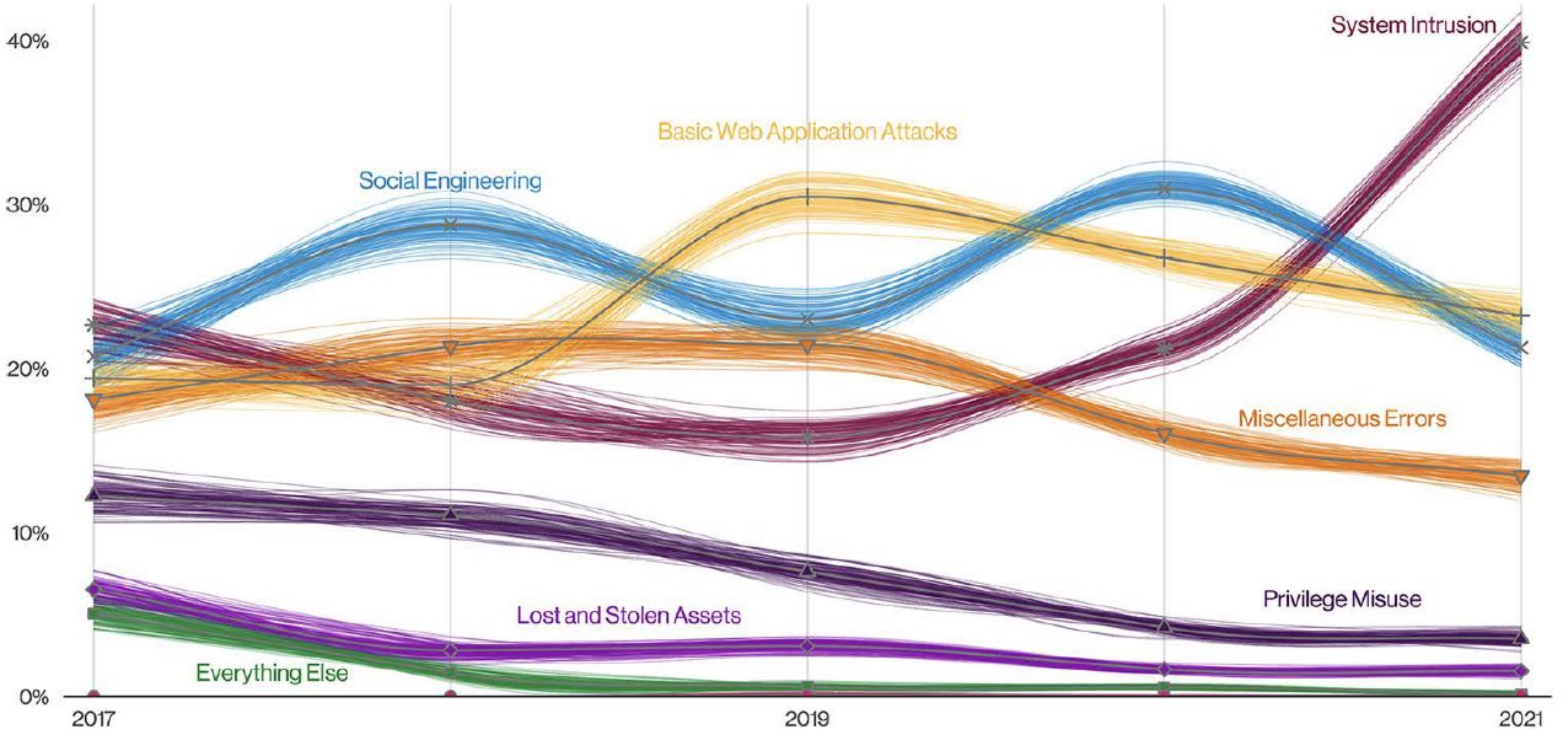


Figure 33. Patterns over time in breaches

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Human Element

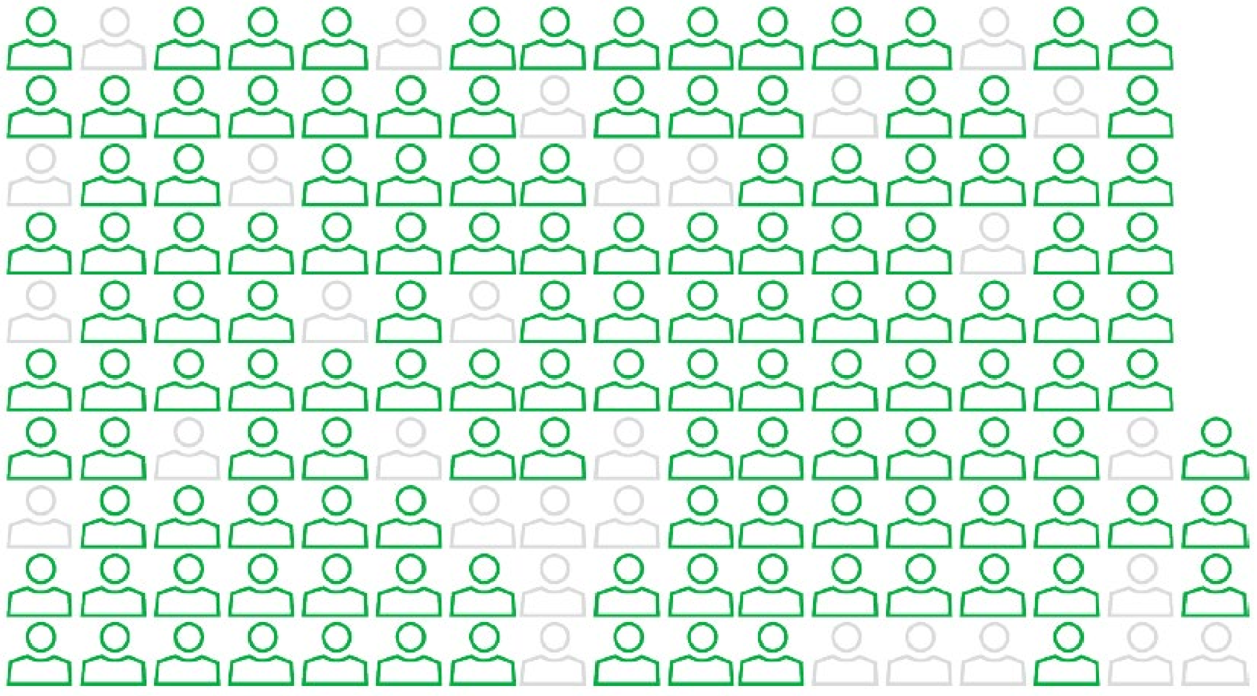
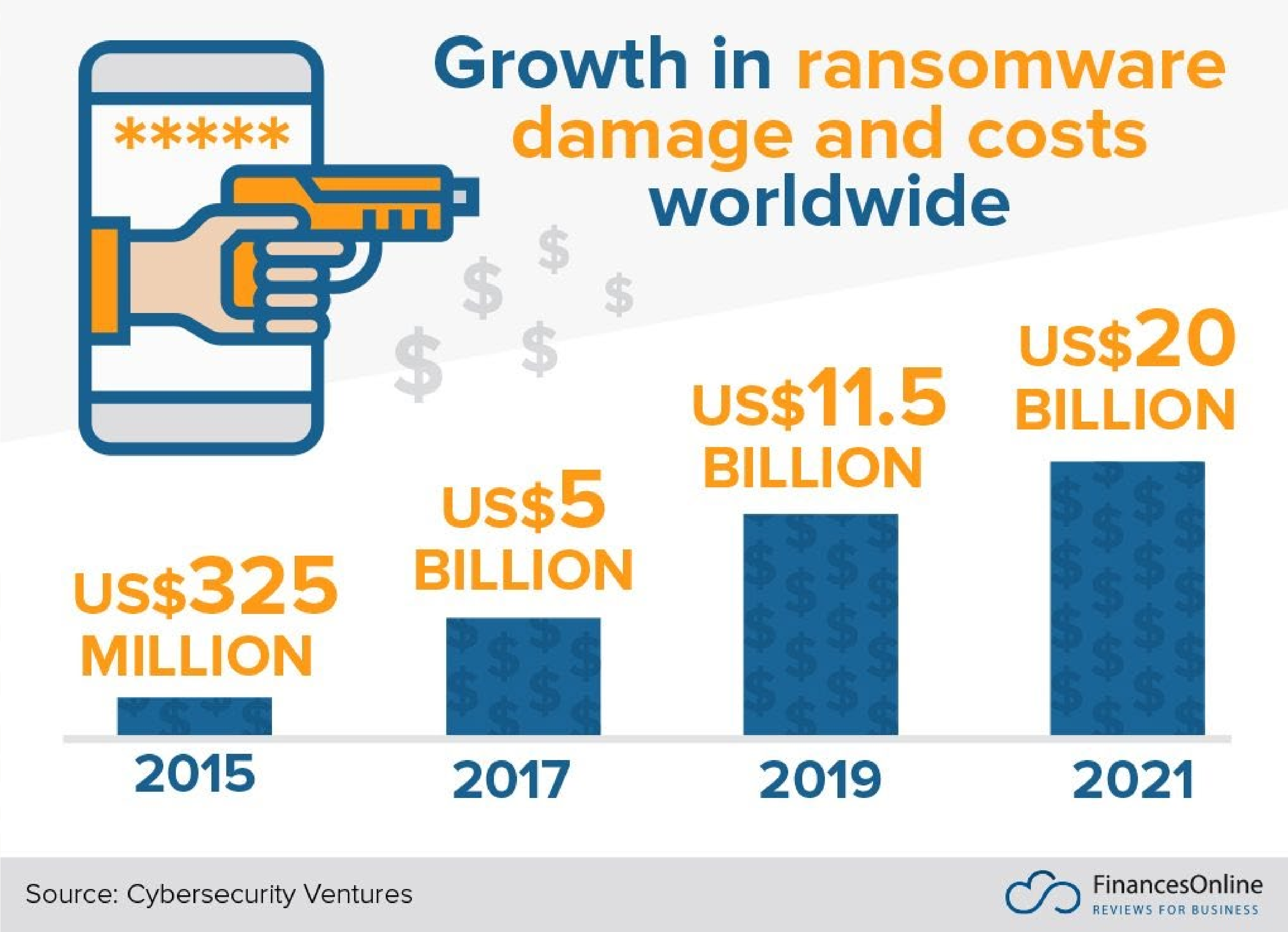


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Human Element

Breach Statistics: Ransomware



Breach Statistics: Ransomware

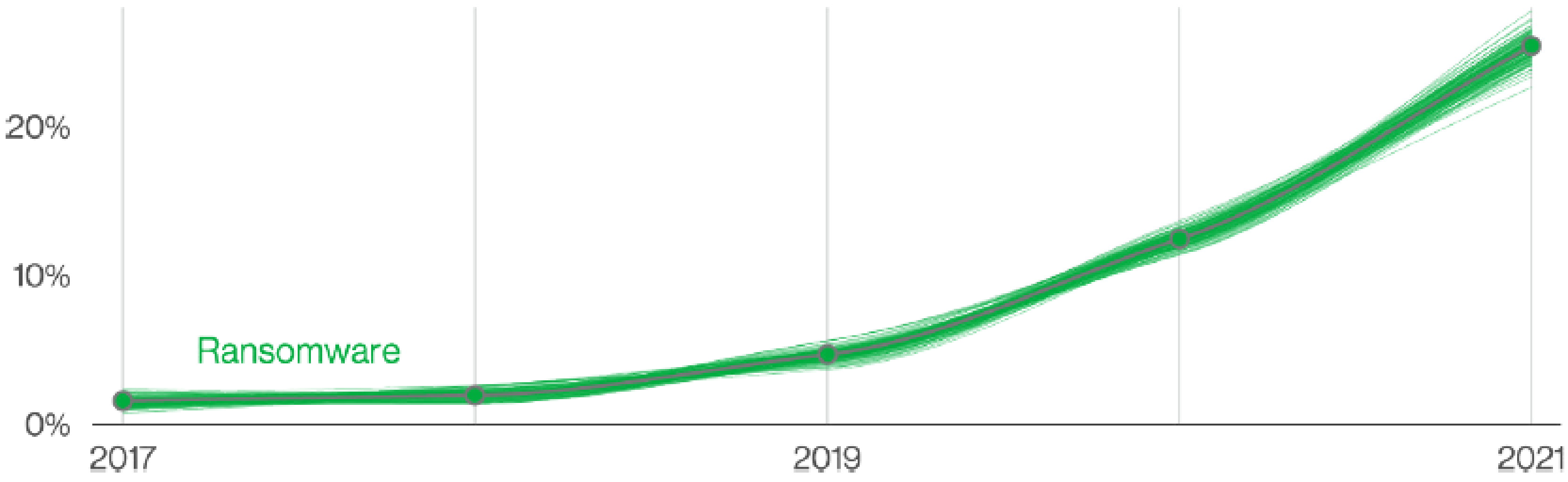


Figure 6. Ransomware over time in breaches

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Financial & Insurance

- 2,527 incidents with 690 confirmed data breaches
  - External actors – 73%
  - Internal actors – 27%

- Top patterns (the top three are present in 81% of breaches)
  - System intrusion
  - Basic web application attacks
  - Miscellaneous errors

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Breach Attack Patterns

Financial and Insurance Sectors Only

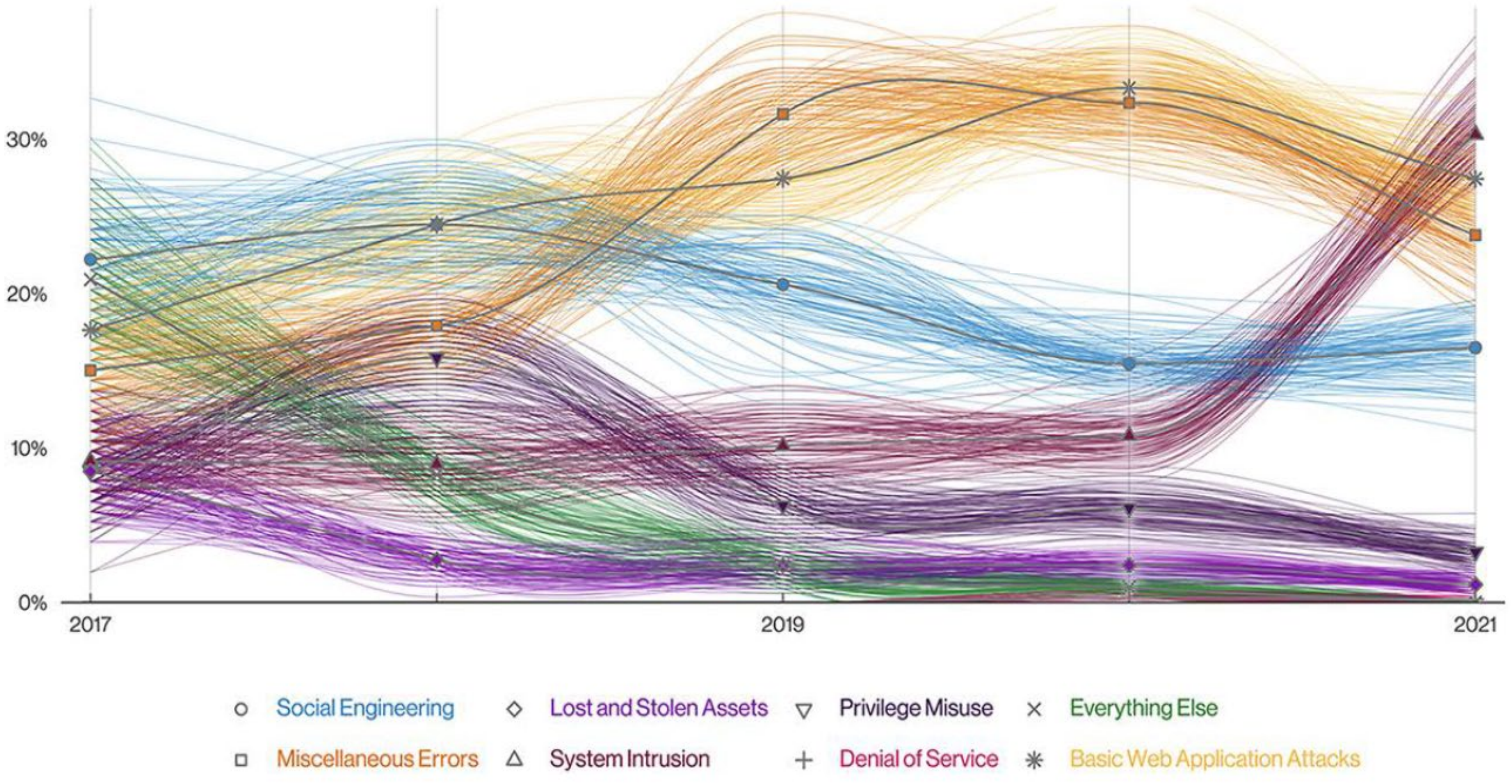


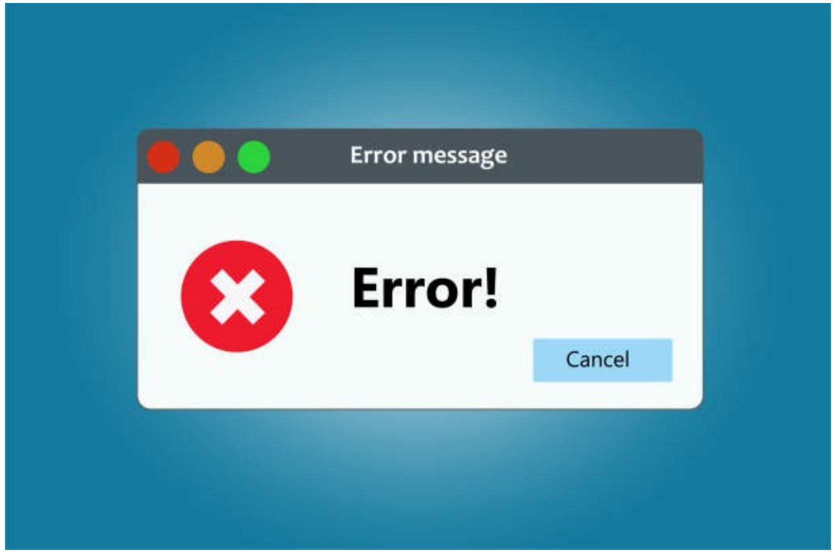
Figure 86. Patterns over time in Financial and Insurance industry breaches

Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Miscellaneous Errors

- Errors are unintentional actions

- Most common mistakes
  - Misconfiguration of database assets
  - Employees sending data to the wrong recipients (mis-delivery)



Source: 2022 Verizon Data Breach Investigation Report

Breach Statistics: Basic Web Application Attacks

- Basic web application attacks:
  - Small number of actions after the initial compromise
  - Attackers are very focused on direct objectives

- Web applications are most often compromised by:
  - Stolen credentials
  - Exploiting vulnerabilities
  - Brute force password attacks

Source: 2022 Verizon Data Breach Investigation Report

Cybersecurity Controls Banks can Implement

Cybersecurity Controls Banks can Implement

- Security awareness and training
- Secure configuration of enterprise assets and software
- Data protection

FFIEC

Cybersecurity Assessment Tool

Control Area: Security Awareness and Training

- Information security strategy that integrates technology, policies, procedures, and training
- Annual information security training provided
- Situational awareness materials available to staff
- Customer awareness materials readily available

Control Area: Secure Configuration

- Policies commensurate with risk and complexity
- Change management processes in place
- Systems configurations consistent with industry standards
- Access rights monitored and controlled

Control Area: Secure Configuration (continued)

- System sessions locked after inactivity
- Network perimeter defense tools in place
- Unnecessary services (e.g., ports, protocols) disabled
- Elevated privileges (e.g., administrator privileges) limited and tightly controlled

Control Area: Secure Configuration (continued)

- Default passwords and accounts changed before system implementation
- Threat information used to enhance controls
- Appropriate password rules and requirements in place

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Control Area: Data Protection

- Assets prioritized for protection based on data classification/ business value
- Appropriate data disposal rules in place
- Mobile devices encrypted if used to store confidential data
- Data flow diagrams document information flow to external parties

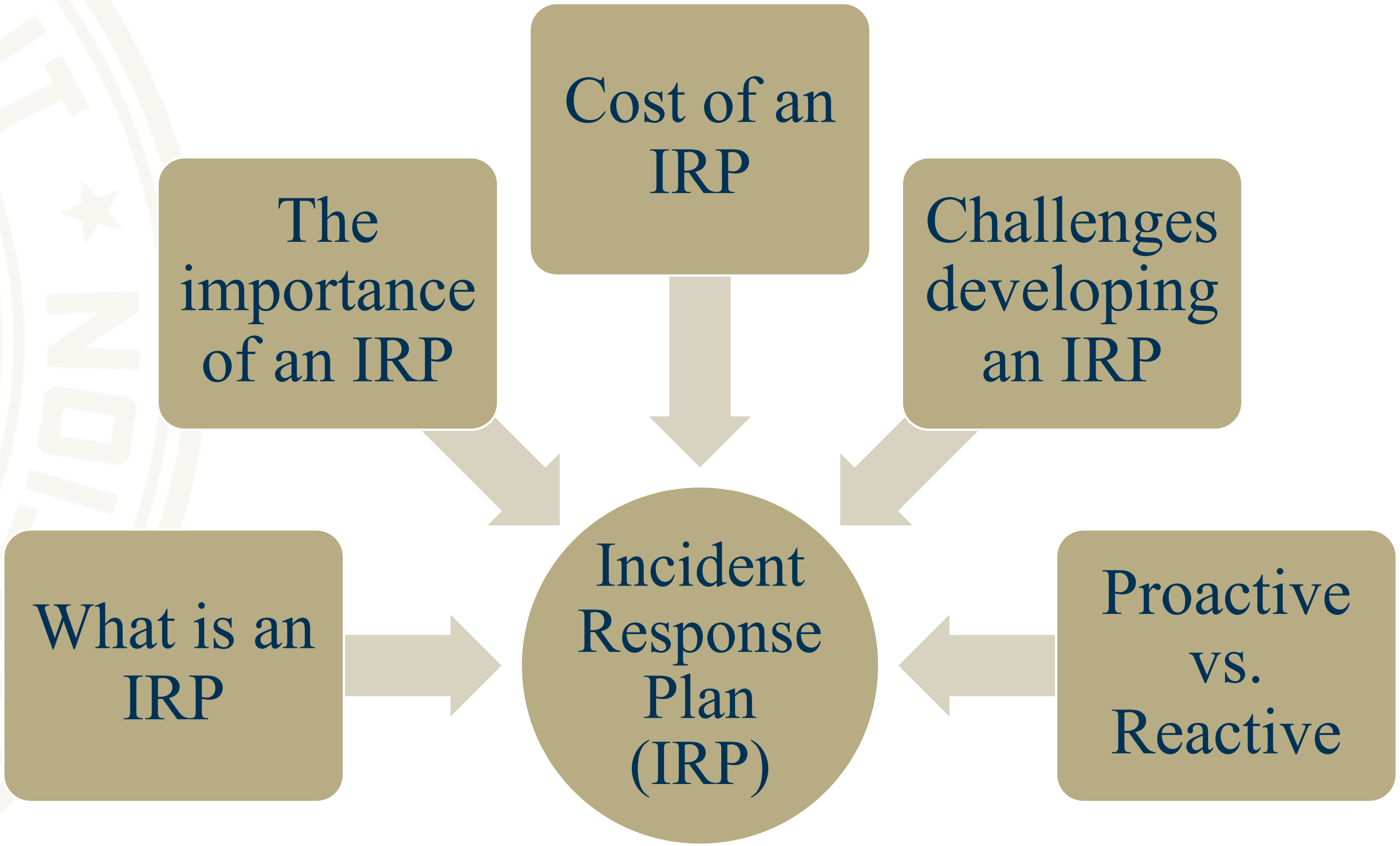
Control Area: Data Protection (continued)

- Use of removable media is restricted
- Data protection included in scope of independent audit
- Passwords encrypted in storage and transit
- Confidential data encrypted when transmitted across public or untrusted networks

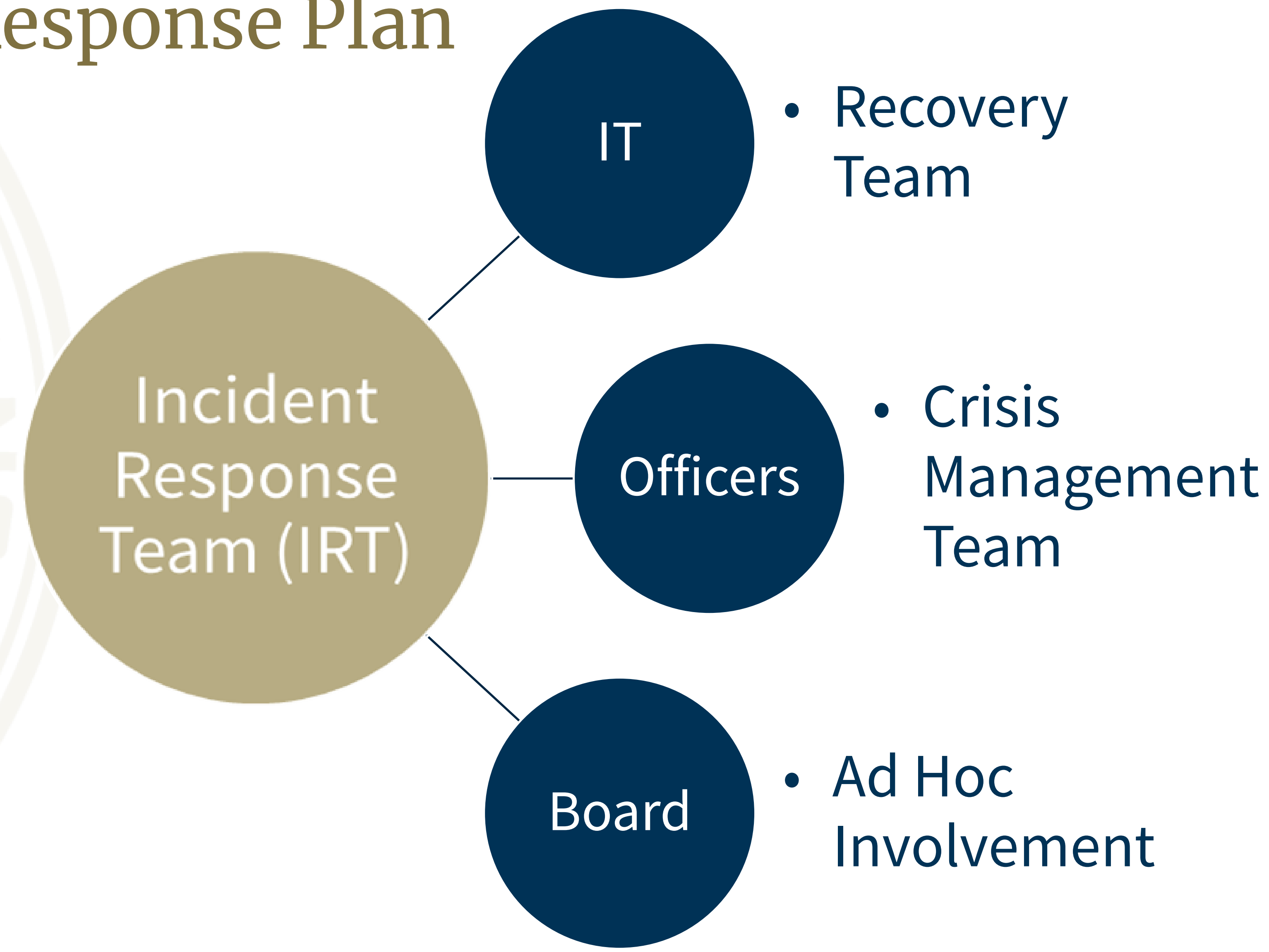
Incident Response Plan and Regulatory Notification

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Incident Response Plan



Incident Response Plan



Regulatory Notification

Banks are required to notify their primary federal regulator ***as soon as possible and no later than 36 hours*** when it is determined they have experienced a major disruptive computer security incident ("*notification incident*") that has, or is reasonably likely to materially disrupt or degrade banks:

- Ability to ***carry out banking operations***, or deliver banking products and services to a material portion of its customers;
- Resulted in a ***material loss*** of revenue, profit, or franchise value; or
- Operations that would pose a ***systemic threat*** to the financial stability of the United States.

Bank Service Provider Expectations

- Bank service providers are required to notify their bank clients **as soon as possible** if they experience a ***computer-security incident*** that has, or is reasonably likely to, materially ***disrupt or degrade*** services provided to a banking organization for ***four or more hours***.

- Computer-security incidents include any occurrence that *"results in **actual** harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."*

Regulatory Notification

Examples of Reportable Incidents

- Large-scale distributed denial of service attacks
- Bank service provider significantly disrupted
- Computer hacking incident
- Malware attack
- Ransomware attack

Cybersecurity Vignettes

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Vignette #7 Table Top Exercise

Vignette #9 Table Top Exercise

Cybersecurity Insurance

Cybersecurity Insurance

FFIEC Joint Statement on "Cyber Insurance and Its Potential Role in Risk Management Programs" (FIL-16-2018)

- Cyber insurance not required
- Insurance could offset financial losses from variety of exposures
- Traditional insurance may not provide effective coverage
- Cyber insurance does not replace sound risk management

Cybersecurity Insurance

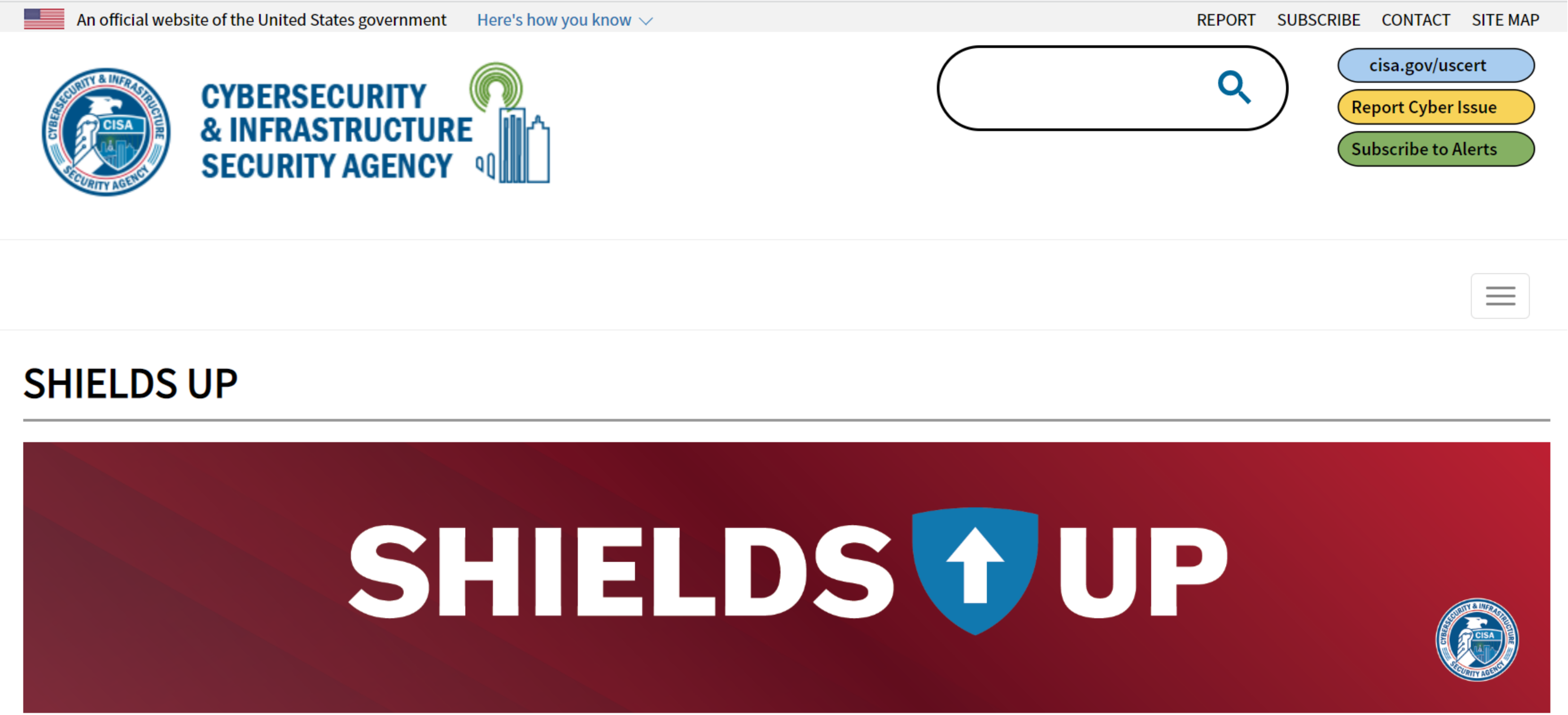
- What is cyber insurance?
- Who needs cyber insurance?
- What does cyber insurance cover?
- What does cyber insurance cost?
- How much cyber insurance is sufficient?

Conclusions and Resources

Conclusions

- Review cybersecurity assessment and threat intelligence process
- Develop a comprehensive IRP
- Test the IRP using various scenarios
- Incorporate a "lessons learned" process to continuously improve the IRP
- Involve directors, senior management, and IT managers

Resources



An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
SHIELDS UP
SHIELDS UP

Resources

Latest Updates

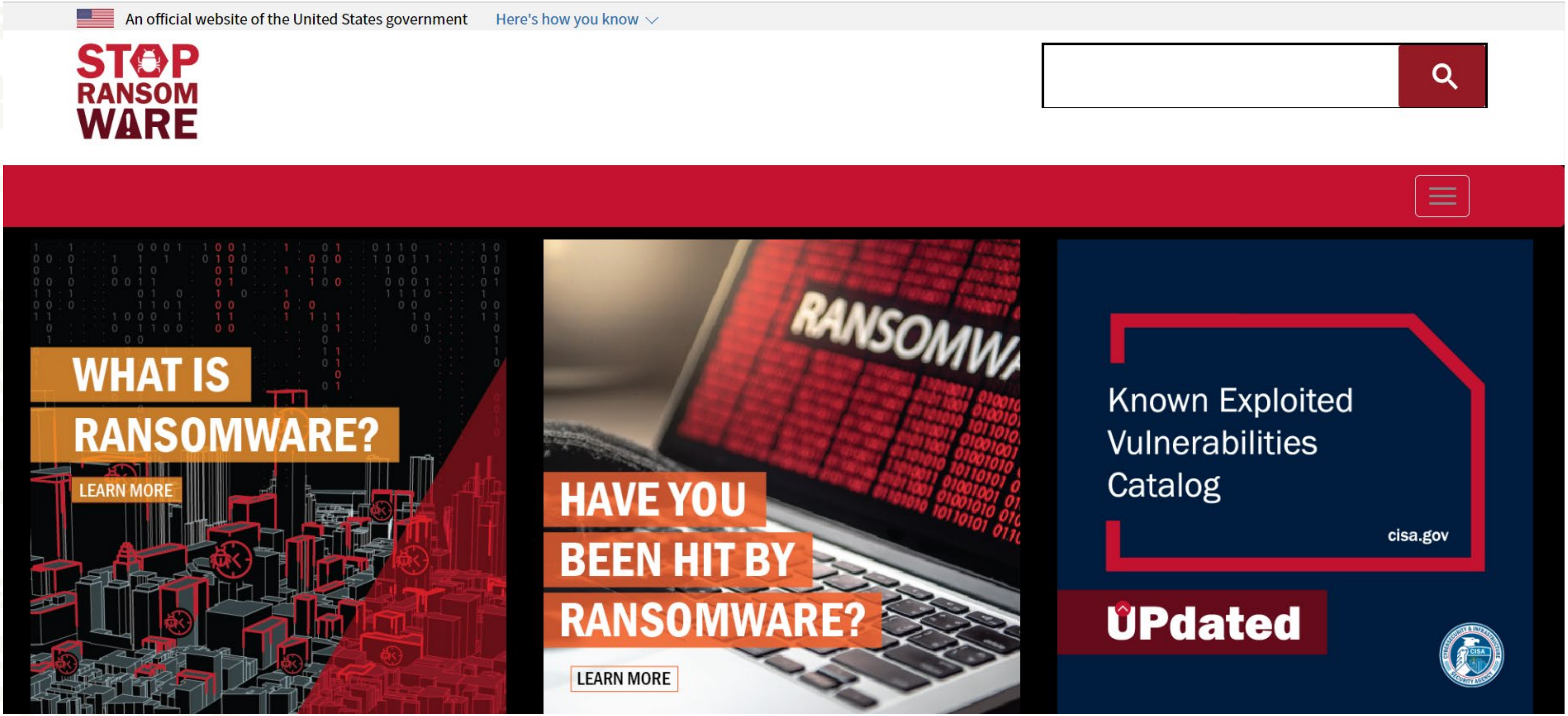
SHIELDS UP Guidance for All Organizations

Recommendations for Corporate Leaders and CEOs

Ransomware Response

Steps You Can Take To Protect Yourself & Your Family

Resources


An official website of the United States government
Here's how you know
STOP RANSOMWARE
WHAT IS RANSOMWARE?
LEARN MORE
RANSOMWA
HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE
Known Exploited Vulnerabilities Catalog
cisa.gov
UPdated

Resources

CISA Ransomware Guide

Part 1: Ransomware Prevention Best Practices

Part 2: Ransomware Response Checklist

Resources

- NIST 800-84 Comprehensive Guide for TTEs
- NIST Ransomware Risk Management: A Cybersecurity Framework Profile
- NIST Getting Started with Cybersecurity Risk Management: Ransomware
- CISA - TTE Packages
- CISA stopransomware.gov - TTE packages
- CSBS Ransomware Self-Assessment Tool
- iC3 FBI Website

FFIEC Cybersecurity Awareness

- https://www.ffiec.gov/cybersecurity.htm
- Includes:
  - Cybersecurity Assessment Tool (CAT)
  - Joint Statements and Guidance
  - Archive of Past Webinars
  - Links to Tabletop Exercises
  - Links to Other Resources (e.g., FBI, NIST, CERT, Secret Service)


Someone discovered my
PASSWORD.
Now I have to rename my dog.

Questions?