Cooley

Out of the Quagmire

Updating Your Privacy and Security Program for 2023

Presented for the
ACC National Capital Region
November 16, 2022

attorney advertisement

Copyright © Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

Cooley

Disclaimer

- The views expressed during today's session are those of the speakers and do not necessarily reflect the positions of any current or former clients or customers of the respective speakers…and nothing we discuss today constitutes legal advice. For any specific questions, seek the independent advice of your attorney, query the cloud, check the "Interwebs", or ask your social network. Furthermore, Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet…

Coverage and agenda

- “While many organizations may have a privacy and security program in place, a number of dynamics may cause those organizations to consider updates to their program (or cause organizations without a program to now put one in place).”
  - Governance
  - New Laws – including CPRA and SEC proposals
  - Information Sharing
  - VDPs and BBPs
  - Ransomware
  - Q&A

Governance

Cooley

Cyber and Privacy Governance

1. Create Governance Structure
2. Research Threats
3. Prioritize Personal Information and Other Information Assets
4. Perform a Risk Analysis
5. Create a Protection Plan Tied to a Technology Acquisition Strategy
6. Engage Third Parties Appropriately (legal, technical, procedural)
7. Request Regular Updates and Adjust Accordingly
8. Test the Response Plan
9. Maintain Appropriate Insurance Coverage
10. Provide Regular Cybersecurity and Privacy Training

Recent Governance Issues

- Whistleblower cases
  - Aerojet/Rocketdyne
    - Aerojet to pay $9M to settle alleged False Claims Act (FCA) violations by misrepresenting cyber compliance in government contracts.
    - Resolves lawsuit by former employee under qui tam (whistleblower) provisions of the FCA. Former employee will receive $2.61M as his share of the FCA recovery.
  - Twitter
    - From Congressional testimony by Mudge (former CISO): “[I] am here today because I believe that Twitter’s unsafe handling of the data of its users and its inability or unwillingness to truthfully represent issues to its board of directors and regulators have created real risk to tens of millions of Americans, the American democratic process, and America’s national security. Further, ***I believe that Twitter’s willingness to purposely mislead regulatory agencies violates Twitter’s legal obligations*** and cannot be ethically condoned.”
    - From a Verge article that spoke with an anonymous employee: “Twitter’s privacy and security teams are in turmoil after Elon Musk’s changes to the service ***bypassed its standard data governance processes***. Now, a company lawyer is encouraging employees to seek whistleblower protection ‘if you feel uncomfortable about anything you’re being asked to do.’”

Recent Governance Issues (cont'd)

- Uber CISO conviction
  - Joseph Sullivan guilty of obstructing FTC and Misprision of a Felony
  - Uber had disclosed to the FTC that a data breach occurred in 2014 involving unauthorized access of approximately 50,000 consumers' personal information
  - In responding to a CID, Sullivan supervised Uber's answers to the FTC's questions, participated in a presentation to the FTC in March 2016, and testified under oath, at length, to the FTC on November 4, 2016, regarding Uber's data security practices
  - Ten days later, Sullivan was contacted by threat actors regarding another Uber breach
  - Sullivan arranged a $100k payment to the threat actors, the FTC alleged, with the intent of hiding the activity and breach from the FTC (including a statement to employees that "this investigation does not exist")

New Privacy and Security Laws Going Into Effect in 2023

Cooley

New privacy and security laws in 2023

	California	Virginia	Colorado	Connecticut	Utah
Effective Date	January 1, 2023	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
Thresholds	• $25 million in gross annual revenue, *or* • 100,000 California residents, *or* • 50% revenue from sales	• 100,000 Virginia residents, *or* • 25,000 Virginia residents + 50% gross revenue from sales	• 100,000 Colorado residents, *or* • 25,000 Colorado residents + derives revenue from sales	• 100,000 CT residents, *or* • 25,000 CT residents + 25% of gross revenue from sales	• $25 million in gross annual revenue, and • 100,000 Utah residents, or • 25,000 Utah residents + 50% revenue from sales
Exemption	Activities subject to and compliant with GLBA	Financial institutions and data subject to GLBA	Financial institutions and data subject to GLBA	Financial institutions and data subject to GLBA	Financial institutions and data subject to GLBA

Common Requirements

- Consumer rights
  - Rights to know, access, correct, delete, opt-out (of sales, targeted ads), non-discrimination
  - Requirement to have privacy policy
- Sensitive personal information
  - But some are opt-in vs. opt-out
- Contractual requirements for service providers
  - CPRA also has contractual requirements for contractors and third parties
- Security requirements
- Requirements for de-identified data

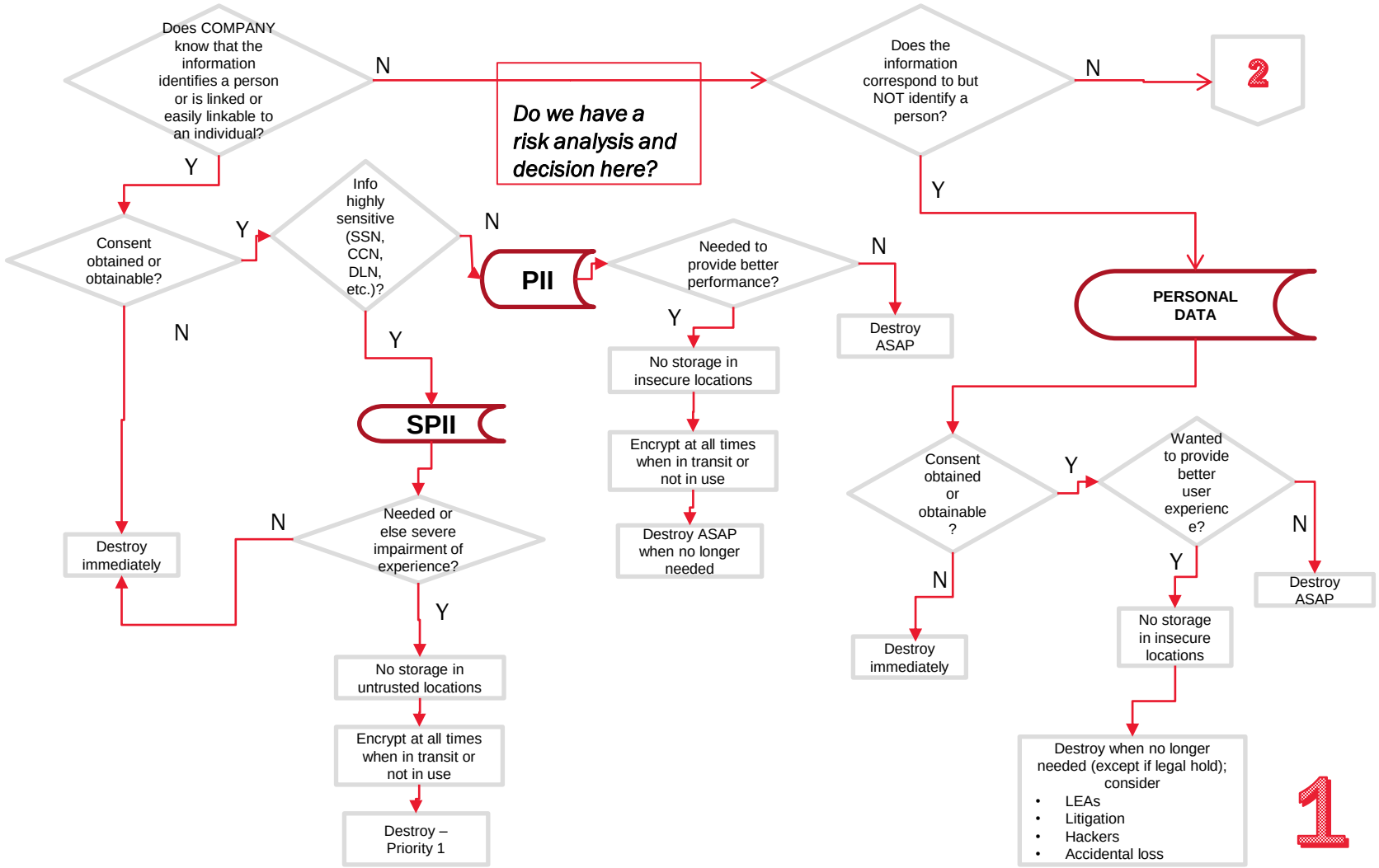
Material Differences

CCPA / CPRA	Newcomers (VA, CO, CT and UT)
Consumers = possibly include employees, B2B contacts	Consumers = true consumers (not employees or B2B contacts)
Sensitive personal information (SPI) definition	Differing definitions (some states do not include geolocation, email contents, financial information or SSN as sensitive; some include PI of known child)
Consent not needed to process SPI (but consumer has right to limit use/sharing)	Opt-in consent needed for processing SPI and children's PI (except UT)
Opt-out for selling and sharing of PI	All: Opt-out for selling PI for monetary consideration CO/CT: Opt-out of selling PI for other valuable consideration VA/CO/CT: Opt-out of sharing for targeted advertising and profiling UT opt-out of sharing for targeted advertising

Material Differences *(continued)*

CCPA / CPRA	Newcomers (VA, CO, CT and UT)
Data subject rights: no explicit right to appeal	Right to appeal (except UT)
Data subject rights: Right to correction	Right to correction (except UT)
“Dark pattern” consent prohibited	“Dark pattern” consent prohibited (except VA, UT)
Global privacy controls / signals: optional?	Required in CO (1/1/2024) and CT (1/1/2025)
Private right of action: Only for data breaches	No private right of action

Sidebar: Privacy and Security By Design



- Example of a simplified privacy and security by design decision tree
- Two other pages of similar content
- Collaboration between attorneys and design engineers

CPRA regulations

Cooley

Restrictions on collection and use of PI

- A business's collection, use, retention, and/or sharing of PI must be **reasonably necessary and proportionate** to achieve the purpose(s) for which the PI was collected or processed
  - i.e., consistent with what an average consumer would expect
- If the purpose is unrelated or incompatible with the purpose(s) for which the PI was collected or processed, a business must obtain **explicit consent**
- ***Arguably huge change:*** *switches CA from notice only regime to notice and consent regime for data processing that is common*

CPRA adds definition of ‘consent’

“ ‘Consent’ means any **freely given, specific, informed, and unambiguous** indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. **Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent**. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of **dark patterns** does not constitute consent.”

Other CPRA Considerations

- Privacy notice at collection – at or before collection; includes notice of sensitive PII collected, retention period, right to opt out
- Privacy policy – describe sharing and new rights available
- Right to opt out of sale and sharing (conspicuous link)
- New or modified rights: right to delete, right to know, right to limit use and disclosure of sensitive personal information (SPI), right to correct
- New category of “contractors” (as distinguished from service providers)
- New obligation on the business to establish contractual requirements for third parties

SEC Proposed Cybersecurity Rule and Insights from the Comment Period

Cooley

Cybersecurity enforcement landscape

- **Cybersecurity disclosures.** In June 2021, the SEC announced that it would focus on cybersecurity disclosures made by public companies as part of its regulatory agenda; the SEC had previously issued guidance in 2018 and 2011 regarding disclosures of cybersecurity risks and disclosure controls
- **Enforcement actions.** Shortly thereafter the SEC filed in quick succession two public company cybersecurity enforcement actions, signaling an increase in cybersecurity enforcement
  - Notably, neither case included any indication that the companies or their executives intended to deceive investors or that either cybersecurity incident was material to investors, indicating that no intent to deceive is needed and that materiality will be measured qualitatively
  - Both cases involved an alleged failure to maintain adequate disclosure controls and procedures, highlighting the importance of companies' policies and procedures around cybersecurity
- **New proposed cybersecurity disclosure rules.** In March 2022, the SEC proposed new rules for cybersecurity disclosure and incident reporting

Recent enforcement developments

- In June 2021, the SEC settled with First American for what the SEC found were inadequate disclosure controls and procedural violations revealed in connection with a cybersecurity vulnerability
  - **Key takeaway**: implementation of reporting procedures designed to inform senior management of vulnerabilities that may be material for financial reporting purposes
- In August 2021, the SEC settled with Pearson plc for what the SEC found to be negligence-based fraud and disclosure controls deficiencies. Three months after learning an incident, Pearson submitted a filing to the SEC containing a cybersecurity related risk factor but made no mention of the intrusion and instead phrased the risk as a hypothetical risk.
  - **Key takeaway**: consistent with their relevant guidance, the SEC expects public companies to tailor their cybersecurity-related risk factors

Proposed Disclosure Requirements

Disclosure Item	SEC Form(s)	Summary
Reporting of material cybersecurity incidents (Form 8-K Item 1.05)	8-K	• Disclosure required where registrant experiences a cybersecurity incident that is determined to be "material" • Current report on Form 8-K due within four business days of **date of determination of materiality**
Material updates to cybersecurity incidents (Reg. S-K Item 106(d))	10-K, 10-Q	• Requires registrant to disclose any material changes, additions or updates to cyber incident previously disclosed on a Form 8-K • Requires registrant to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate
Risk Management and Strategy (Reg. S-K Item 106(b))	10-K	• Requires registrant to describe its policies and procedures, if any, for the identification and management on cybersecurity risks
Governance (Reg. S-K Item 106(c))	10-K	• Requires registrant to describe the board's oversight of cybersecurity risk • Requires registrant to describe management's role in assessing and managing cybersecurity-related risks
Director cybersecurity expertise (Reg. S-K Item 407(j))	10-K, Proxy Statement	• Requires registrant to disclose the name of any director(s) and relevant details with respect to any directors with expertise in cybersecurity • Such determination does not impose on such director any additional duties, obligations or liability, nor does it affect the duties obligations or liability of any other director

Summary of Proposed Disclosure Requirements

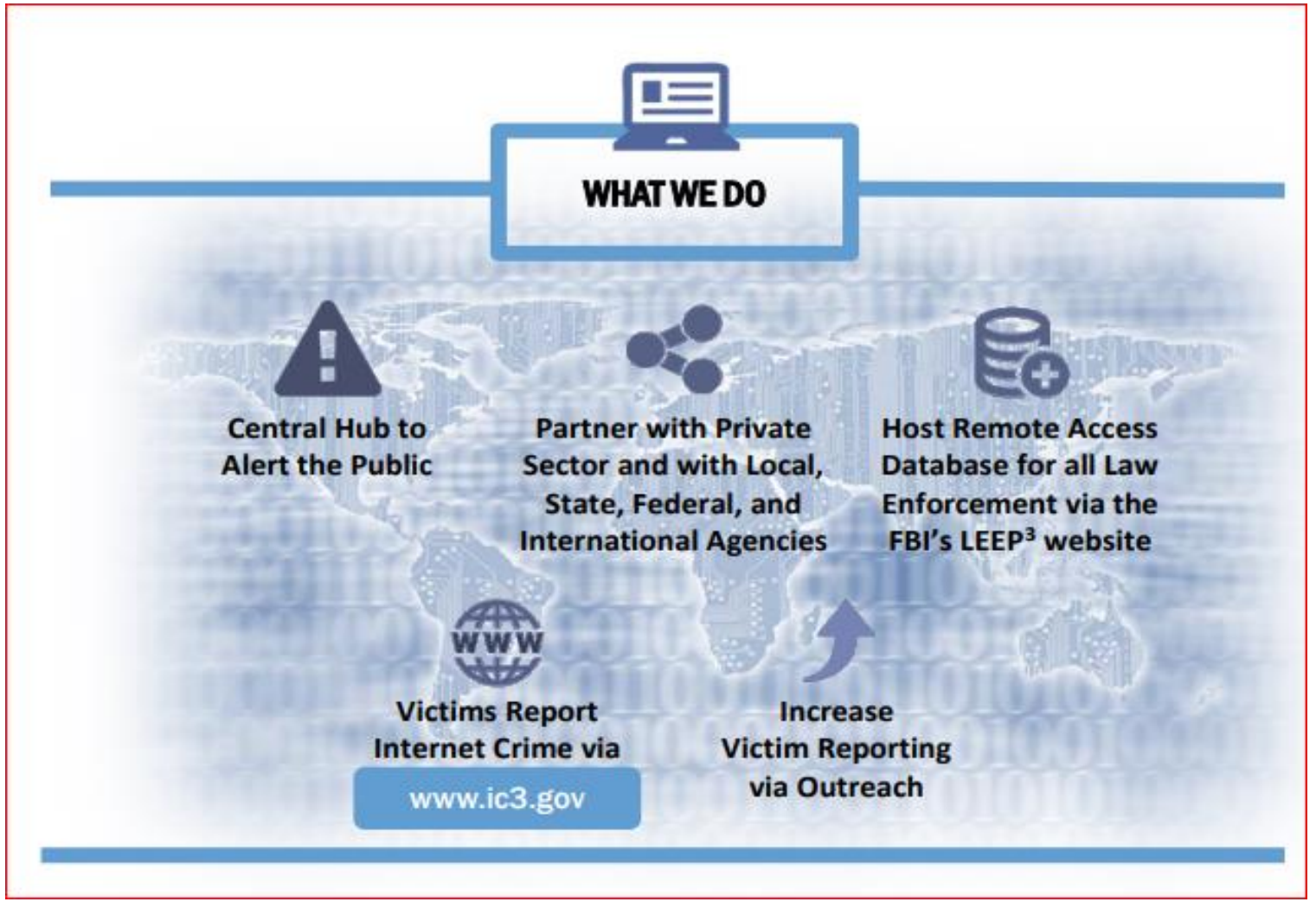
- Report “material cybersecurity incidents” to the SEC within 4 days
- Report non-material incidents that, when combined with other incidents, become material “in the aggregate”
- Provide updates on prior incidents in periodic SEC disclosures
- Describe company’s cybersecurity risk management system
- Describe the Board’s oversight of cybersecurity risk
- Disclose the cybersecurity expertise of the Board members

Information Sharing (including with government actors)

Cooley

Internet Crime Complaint Center (IC3)

- Established by the FBI in May 2000
- Centralized point for businesses and consumers to submit complaints pertaining to internet-related crime
- Since inception, more than 4 million complaints submitted with losses in excess of $5.52 billion



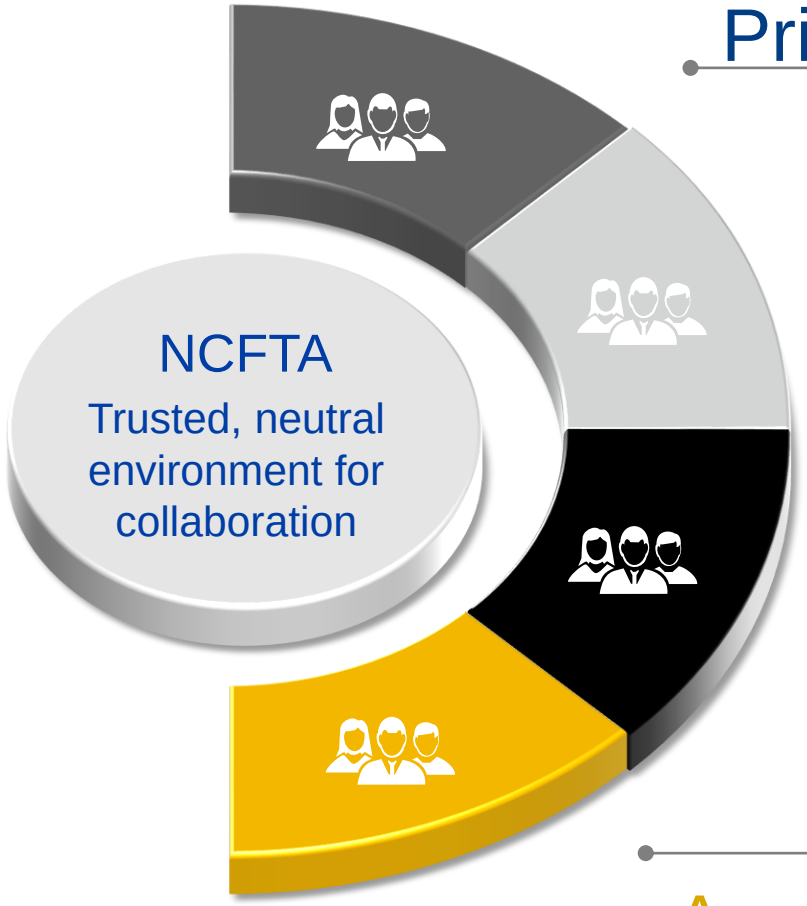
Internet Crime Complaint Center (IC3)

www.ic3.gov

Interacting with Law Enforcement

- The FBI maintains 56 field offices throughout the United States and more than 75 offices in strategic locations throughout the globe
- Contact local FBI field office and/or IC3 (www.ic3.gov)
- Law enforcement requests for information, what will you provide?
- Who will be law enforcement's point of contact?
- Who will handle notifications to stakeholders, if necessary?

NCFTA – the next generation of cyber intel sharing



Private Industry

NCFTA analysts

Law Enforcement

Academia & SMEs

NCFTA Analytical Teams – 3 Programs / Multiple inititatives

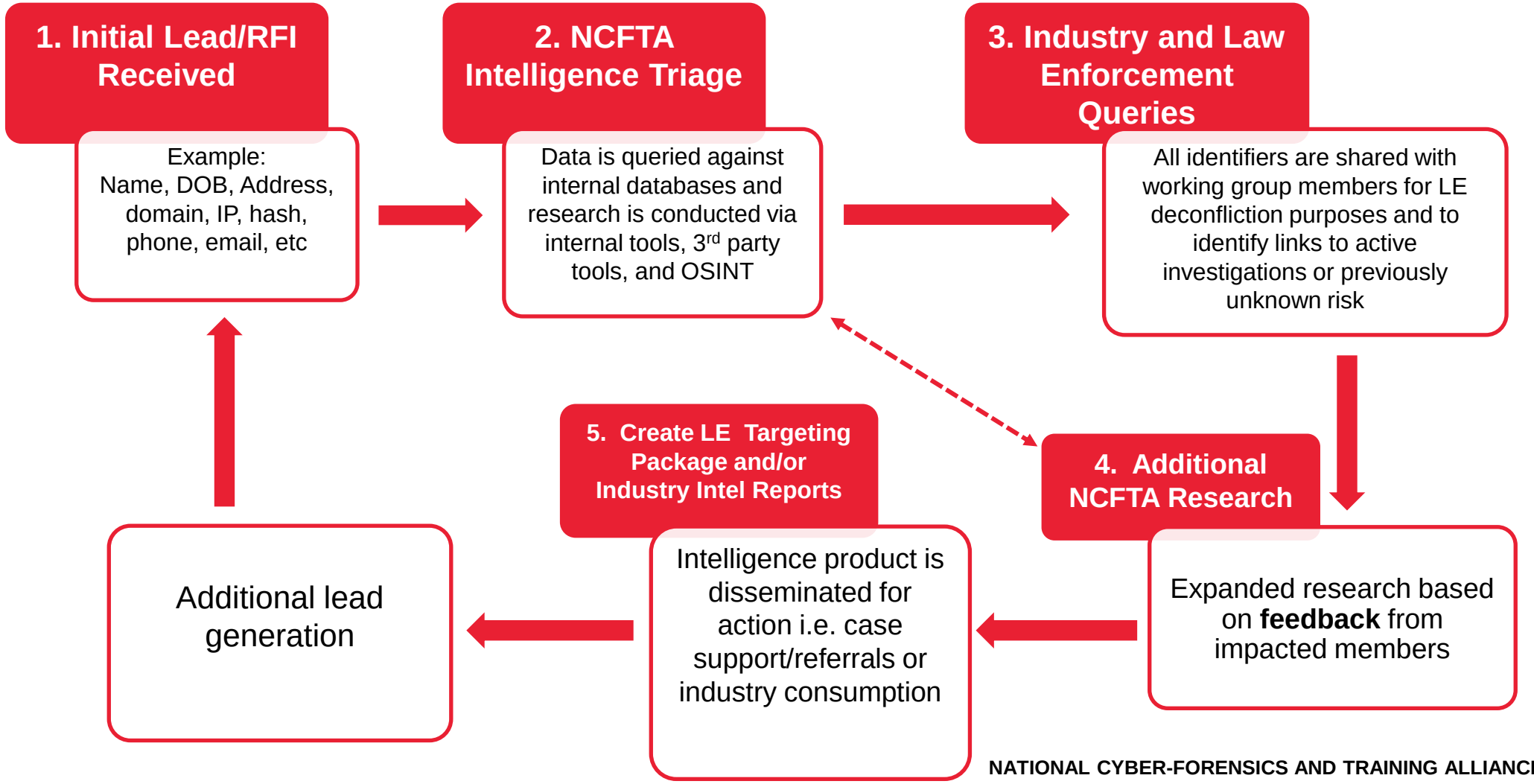
- Intellectual Property (IPR)
  - General Counterfeits
  - Automotive
  - Tobacco
- Pharmaceutical Fraud and Illicit Substances
- E-Commerce Fraud
- Internet Fraud Alert (IFA)

- Account Abuse and Intrusion
- Advanced Payments Abuse
- Transient Criminal Groups
- BEC Fraud & Money Mules
- Payment Card Fraud
- Cryptocurrency
- Human Trafficking
- Securities Fraud
- Synthetic Identity

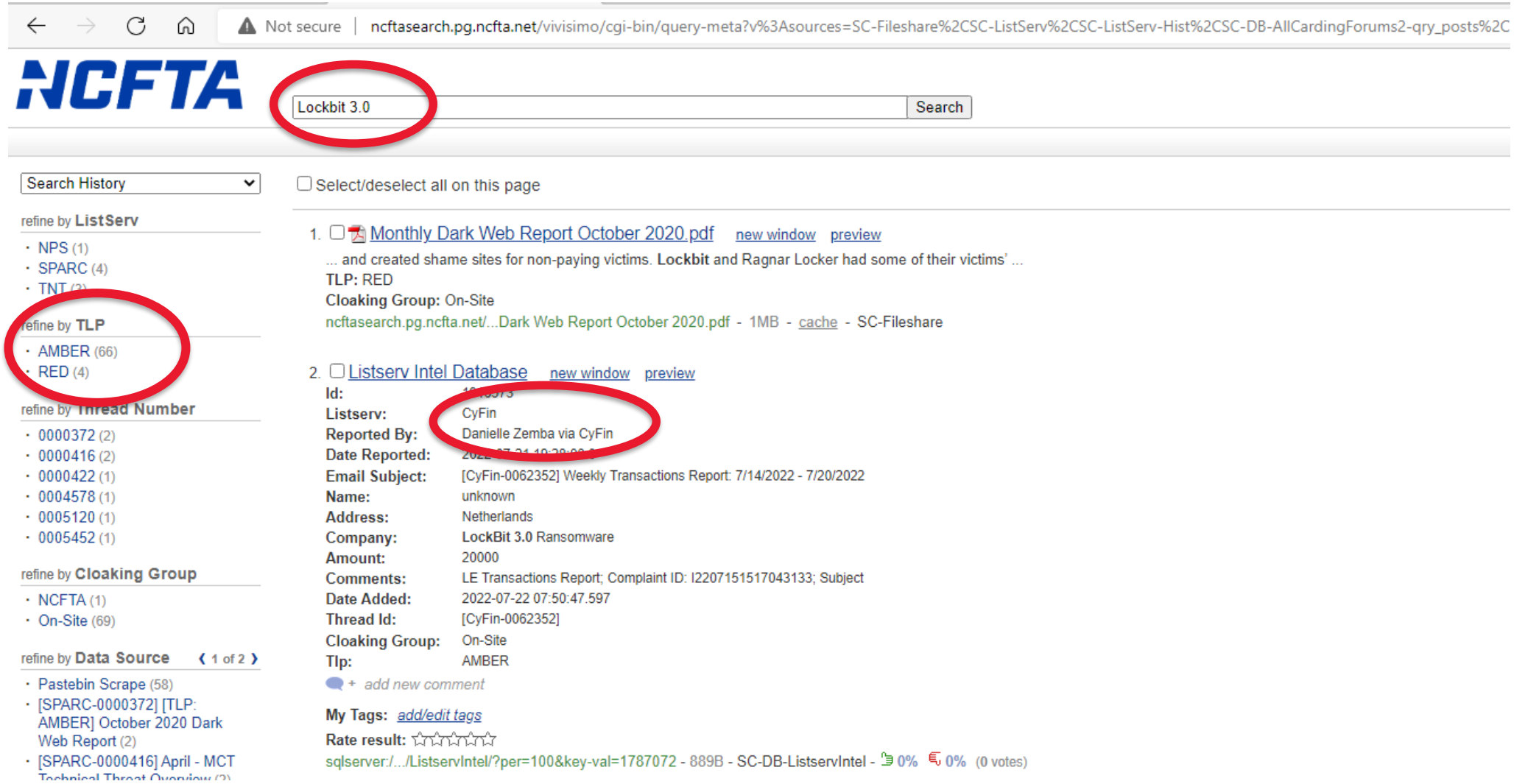
- Malware Analysis and Decryption
- Onsite Malware and Gaming Lab
- Honeypot/IoT Monitoring
- APTs and Other Threat Groups
- Dark Web Analysis
- Threat Actor Attribution/Engagement
- SIEM Support
- Controlled Purchases and Analysis

MULTI-LINGUAL INTEL ANALYSTS — RUSSIAN / UKRANIAN /CHINESE / ROMANIAN / SPANISH
Custom research & intelligence reports, incident support, law enforcement coordination

Information sharing at NCFTA: how does it work?



Up-to-date intelligence from government and the private sector



Information Sharing: CISA

- The Cybersecurity Information Sharing Act
  - Became law in December 2015
  - Encourages sharing of cybersecurity threat indicators and defensive measures
  - Shields companies from legal liability
    - Must not knowingly share PII unless directly associated with the attack/attacker
  - Provides protection from public disclosure when sharing w/USG (FOIA exemption)

Information Sharing: CISA

- Cybersecurity Threat Indicators (“CTI”) include information necessary to describe or identify a variety of things, including:
  - Malicious Recon
  - Methods of defeating security/exploiting a vulnerability
  - Tricking a user w/legit access to unwittingly defeat security
  - Malicious C&C
  - Harm caused by an incident, including description of exfil

Information Sharing: CISA

- Defensive Measures are:
  - actions, devices, procedures, signatures, techniques, or other measures applied to
    - an information system or
    - information that is stored on, processed by, or transiting an information system
  - that detect, prevent, or mitigate a known or suspected cybersecurity threat or security vulnerability

Vulnerability disclosure and bug bounty programs

Cooley

What is a Vulnerability Disclosure Program?

- Provides authorization to researchers to test systems and submit reports of vulnerabilities (‘safe harbor’)
- Usually unpaid/rewarded
- Can be as simple as providing an email alias where researchers can reach you and setting expectations
- Likely best option for small entities with limited resources
- There are multiple resources available (standards, government/agency recommendations, templates)

Bug Bounty Program

- More advanced approach - paying researchers for submissions
- Comes in many forms
  - Private Program - open only to selected researchers. Great way to start a program while trying to determine scale of submissions
  - Limited Public Program - open to all approved researchers - for instance, those that participate on platforms programs such as BugCrowd or HackerOne.
  - Public Program - open to all researchers.
  - Agreed Disclosure
  - Non-Disclosure

What about researchers disclosing to MITRE/CVE/CISA

Put Your Bug Bounty Program To Work!

- Now that you have a BBP, what happens when a bug is found?
- Keep in mind multiple types of BBPs – Company/internal, third party, hybrid; also, responsible disclosure program
- Not a black/white situation when dealing with researchers; keep this in mind when researchers become an issue
- Realize the importance of balancing a safe harbor provision in your terms with a limitation on how far researches can go (e.g., “We give you permission to test our systems for vulns, but you aren't permitted to touch user data or confidential business data. If you do by accident, you must immediately stop and tell us about it. We won't sue you or refer you to LE if you made a good faith effort to comply with these terms.”)

Your BBP at Work – Legal Concerns of Researchers

- “The vast majority of researchers (92%) generally engage in some form of coordinated vulnerability disclosure. When they have gone a different route (e.g., public disclosure) **it has generally been because of frustrated expectations, mostly around communication**.” (NTIA Survey, 2015)
- “[T]he results indicate that **rules with more content** (e.g., more detailed list of included / excluded areas and issues) and explicit statements on duplication, disclosure, etc., **are associated with more bugs resolved**.” (Laszka et al., 2018)
- The most common reasons for leaving a bug-bounty program are all related to **communication issues** (Omer Akgul et al. 2020)

Ransomware

Cooley

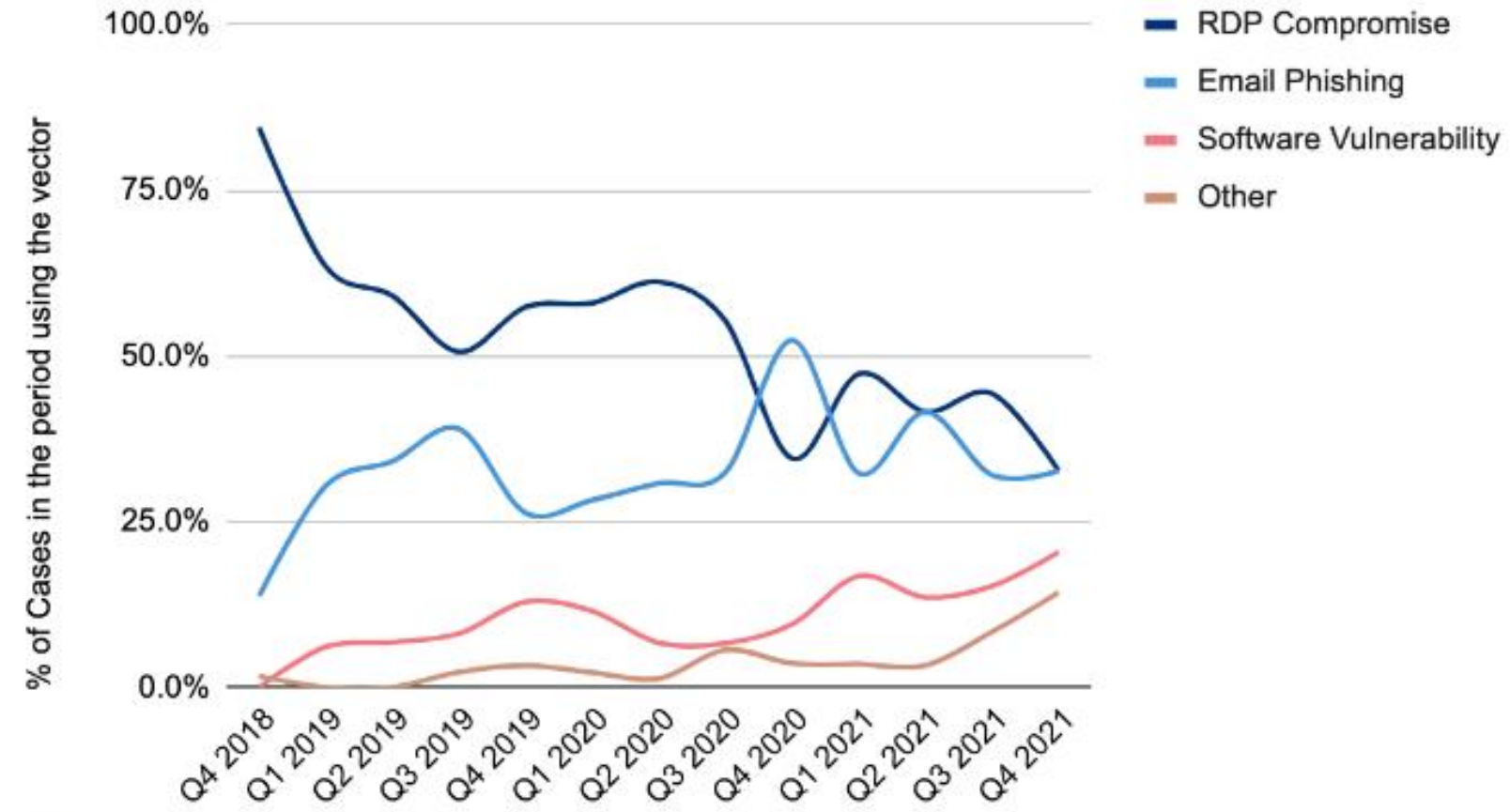
Shift from PII Breaches to Ransomware Attacks

- PII breaches versus ransomware attacks
- Ease of monetization
- Why not both?
  - Double extortion (data release)
  - Triple extortion (disclosure to customers)

“Big Game” Ransomware Attacks/Impacts: Business interruption and data asset loss

- **Characteristics**
  - **Not drive-by attacks:** intelligence gathering, planning, use of multiple tools and lateral movement (often through admin access)
  - **Bad timing:** attackers maximize pressure by timing attacks at bad times
  - **Encryption of back-ups**
  - **Entire system disabled** (e.g., email, manufacturing, order fulfillment, invoicing, delivery)
  - **Need to wipe and rebuild in real-time:** cannot simply restore or decrypt because of high risk of secondary attack
  - **Data exfiltration investigation is necessary after initial triage**
  - **Phishing is often root or contributing cause**

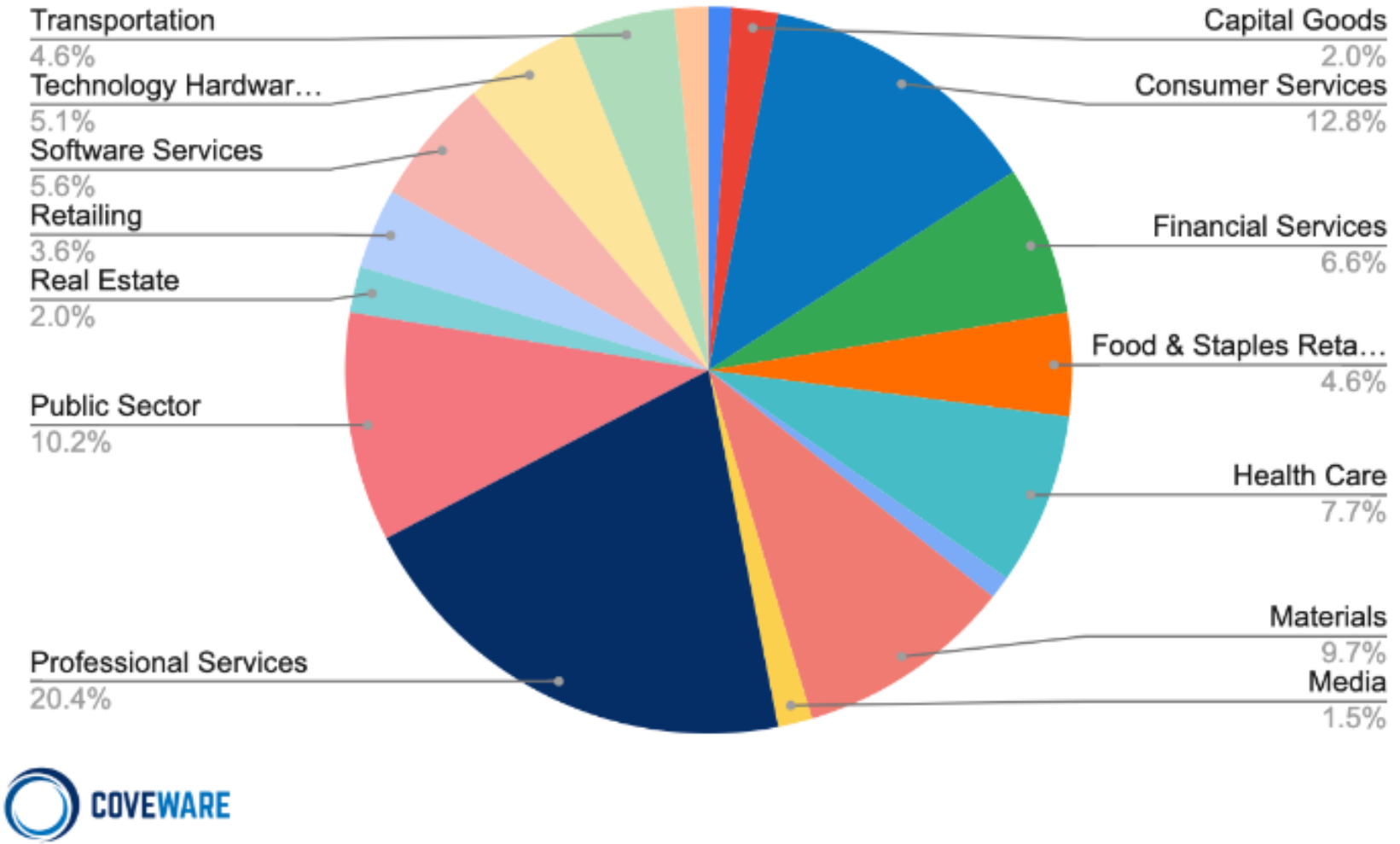
Ransomware Attack Vectors



COVEWARE

Source: *https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021*

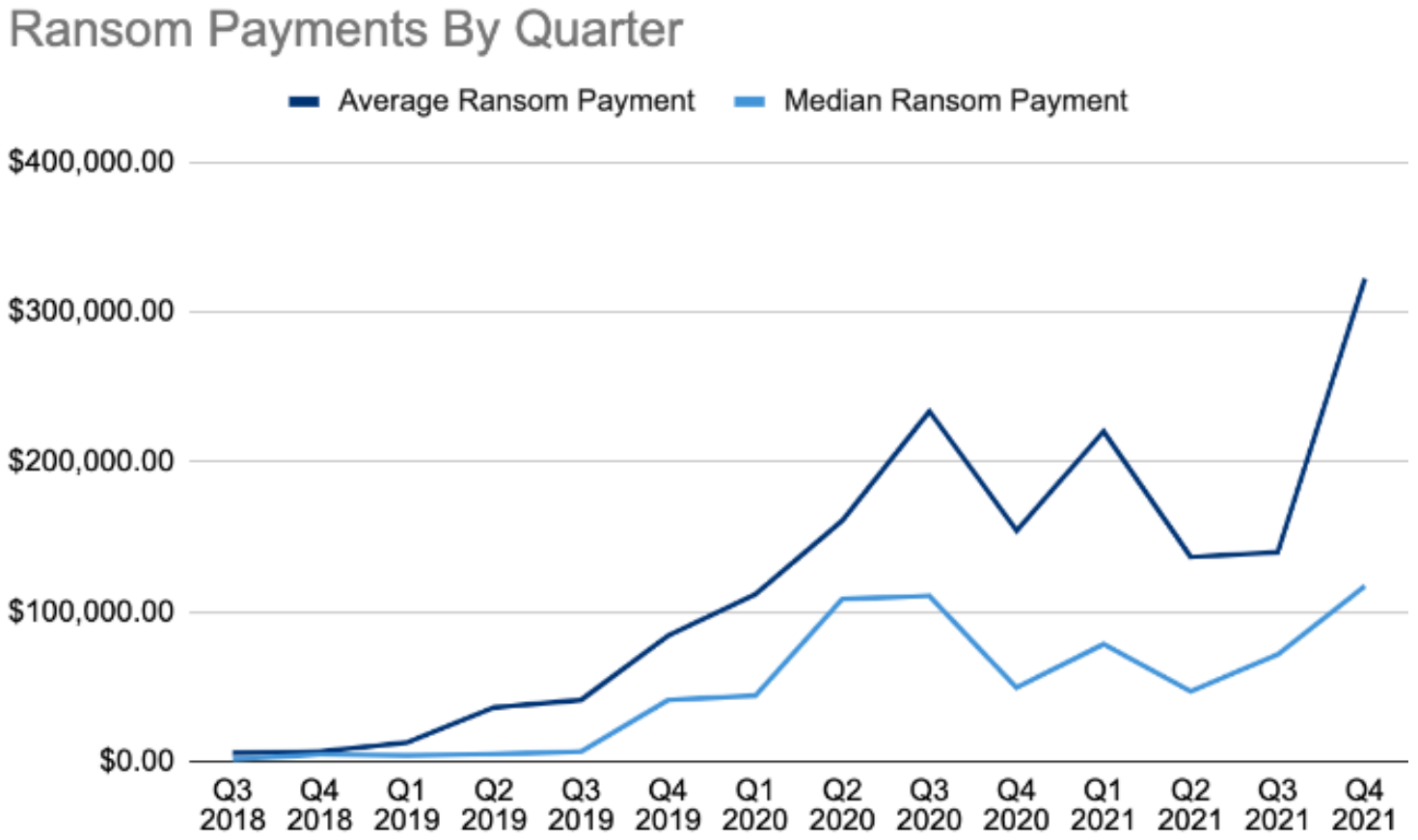
Targeted Industries



COVEWARE

Source: *https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021*

Ransomware Payment Statistics



Average Ransom Payment

$322,168

+130% from Q3 2021

Median Ransom Payment

$117,116

+63% from Q3 2021

COVEWARE

Source: *https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021*

Ransomware Response

- Identifying the threat actor – negotiation strategy and risk
- Tying into business continuity/disaster recovery
- Understanding the operational and financial impact of the incident
- Recovery challenges – time and risk
- Data exfiltration leverage
- Need for broader investigation: data exfiltration and root cause
- OFAC issues (and insurance coverage)
- Immediate communication challenges

Negotiating with Threat Actors

- Specialists with dark web personas – prior experience / dossiers
- Obtain “proof of life”
- Leverage depends on “facts on the ground”
  - Is the company down?
  - Do backups exist?
  - Did they take valuable data?
  - Do they want to walk away?

Negotiating with Threat Actors

- Setting a budget
- Establishing a narrative
- Strategic bidding
  - Based on budget
  - Decreasing increments create a sense of scarcity / diminishing returns

OFAC Compliance

- September 2021 Updated Guidance: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
  - "Actors and others who materially assist, sponsor, or provide financial, material, or technological support"
    - Individuals, groups, bitcoin wallets, crypto exchanges
  - Any transaction that causes a violation is also prohibited (e.g. banks, insurers who reimburse)
- OFAC Enforcement Guidelines
  - Existence, nature, and adequacy of a sanctions compliance program
  - Security measures to reduce risk of extortion (see CISA September 2020 Ransomware Guide)
  - Reporting to law enforcement
- OFAC Licensing: "case-by-case basis with a presumption of denial"

Q&A and wrap up

Cooley

Cooley

Out of the Quagmire

Updating Your Privacy and Security Program for 2023

Presented for the
ACC National Capital Region
November 16, 2022

attorney advertisement

Copyright © Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.