SEPT.
18TH

EDUCATION SECURITY SUMMIT

Critical Threats & Solutions For Education Organizations

Agenda

- Welcome
- Legal Response to Emerging Cyber Threats During COVID-10
- A Day in the Life of a Security Analyst
- Stretch Break
- School Security
- Top Security Challenges
- Endnotes

Maggie Collins

Maggie Collins has a Masters Degree in Learning Design and Technology from Purdue University. Her experience spans from classroom teaching, Marketing, Relations Director, to Instructional Designer and project manager for eLearning in higher education at Indiana Wesleyan University. She is currently Lead Instructional Designer at HighPoint Global creating training products for government partners currently, CMS (Center for Medicare/Medicaid Services). With Indiana Infragard she has held several positions over the years, Scholarship Director, Sector Security and Resiliency Program Coordinator, and now **President**.

Legal Response to Emerging Cyber Threats During Covid-19

Stephen Reynolds, CIPP/US, CISSP
Partner, Ice Miller LLP
Stephen.Reynolds@icemiller.com

Tiffany Kim, CIPP/US
Associate, Ice Miller LLP
Tiffany.Kim@icemiller.com

Stephen Reynolds is a partner in Ice Miller's Litigation Group, member of the Data Security and Privacy Practice and of the Firm's Board of Directors. Stephen frequently advises clients on complex matters involving data security and privacy laws and serves on the board of directors of the International Association of Privacy Professionals (IAPP).

Stephen has assisted companies of all sizes—ranging from Fortune 50 to small businesses—in responding to cybersecurity incidents, including ransomware attacks, fund transfer fraud, data breaches, and business email compromise matters. Additionally, he actively represents companies in data security and privacy matters and has litigated through trial multiple other matters—such as products liability cases, construction litigation, trade secrets litigation, and general commercial litigation.

He is a Certified Information Privacy Professional (CIPP/US). In addition to being a Certified Information Systems Security Professional (CISSP), Stephen teaches CISSP classes as a Direct Instructor with the (ISC)².

Tiffany Kim is an attorney in Ice Miller's Litigation and Data Security and Privacy Practice Groups. Her background as a former homeland security planner and tactical communications operator with the U.S. Marine Corps give her a unique perspective when advising clients on cybersecurity matters.

Tiffany advises clients on compliance with state, federal and international data protection laws including data breach notification laws, the California Consumer Privacy Act (CCPA), HIPAA and the European Union General Data Protection Regulation (GDPR). She is a member of the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional U.S. Private-Sector (CIPP/US) from that organization. Tiffany also assists clients with significant security incidents during the response, investigation and remediation phases.

Prior to law school, Tiffany served as a Homeland Security Planner with the Kent County Sheriff's Office. Additionally, Tiffany served as co-chair of the West Michigan Cyber Security Consortium. Tiffany served active duty with the United States Marine Corps, where she specialized in tactical communications as a field radio operator.

Today's Agenda

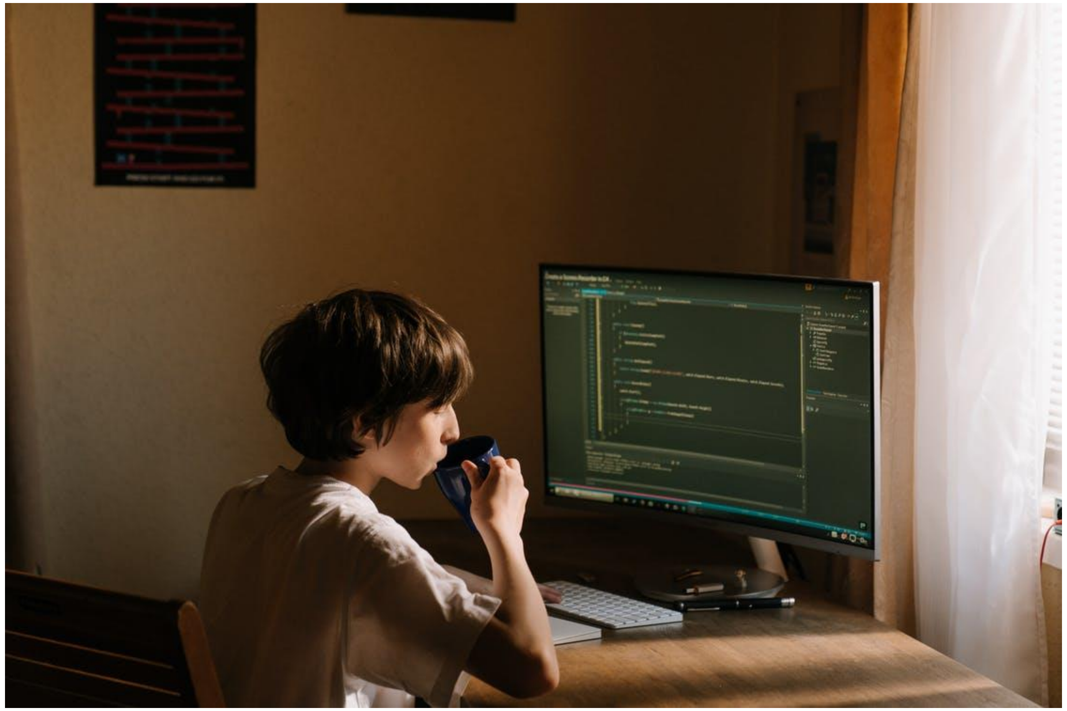
1. Understand trend in emerging threats during Covid-19

2. Discuss mitigation tactics and strategies

3. Discuss Incident Response and collaborating with government agencies and third parties

Overview of Emerging Threats

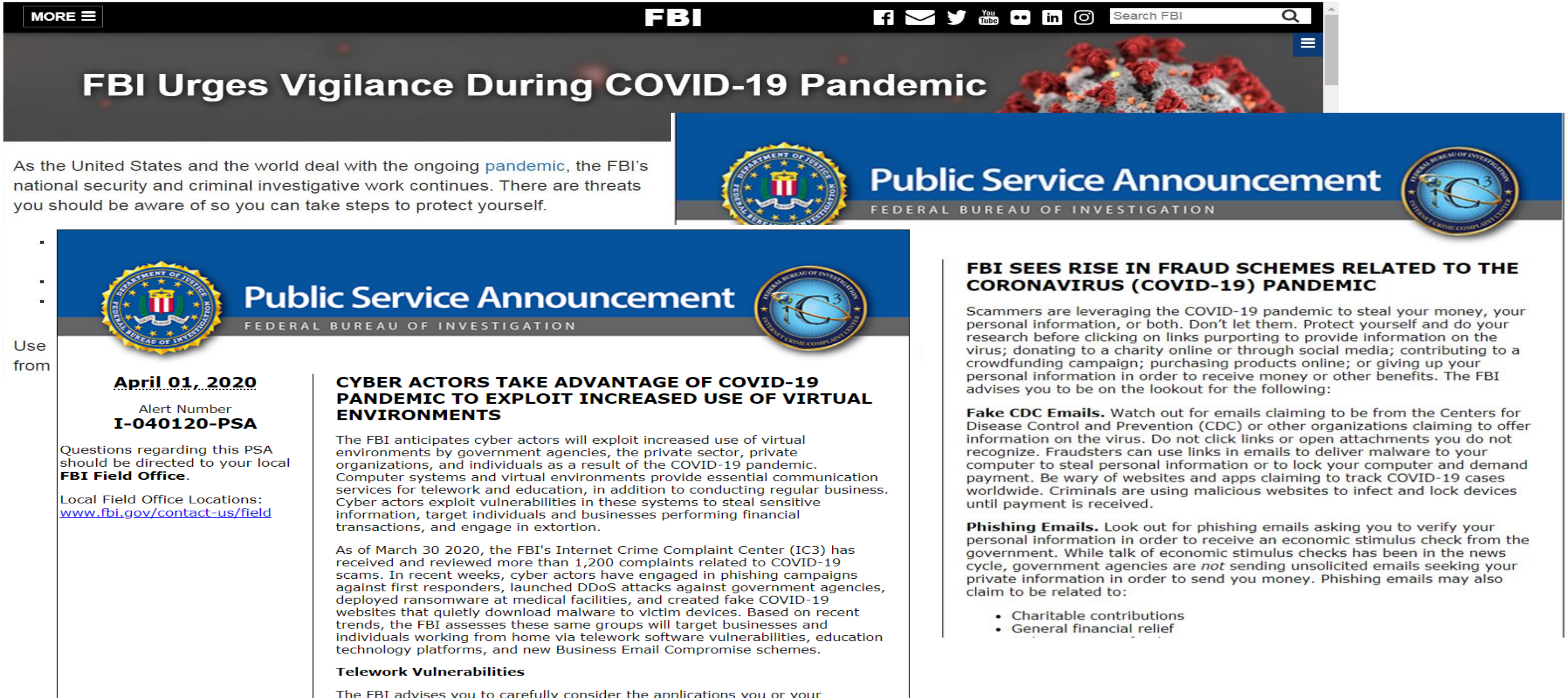
- Covid-19 scams
- Unprotected networks
- Online learning applications and platforms
- Remotely conducting school board/administrator business



Emerging Threats

Cyberattack shuts down e-learning

Covid-19 Related Threats



FBI Urges Vigilance During COVID-19 Pandemic

As the United States and the world deal with the ongoing pandemic, the FBI's national security and criminal investigative work continues. There are threats you should be aware of so you can take steps to protect yourself.

Use
from

April 01, 2020

Alert Number
I-040120-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

CYBER ACTORS TAKE ADVANTAGE OF COVID-19 PANDEMIC TO EXPLOIT INCREASED USE OF VIRTUAL ENVIRONMENTS

The FBI anticipates cyber actors will exploit increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic. Computer systems and virtual environments provide essential communication services for telework and education, in addition to conducting regular business. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion.

As of March 30 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 1,200 complaints related to COVID-19 scams. In recent weeks, cyber actors have engaged in phishing campaigns against first responders, launched DDoS attacks against government agencies, deployed ransomware at medical facilities, and created fake COVID-19 websites that quietly download malware to victim devices. Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new Business Email Compromise schemes.

Telework Vulnerabilities

The FBI advises you to carefully consider the applications you or your

FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

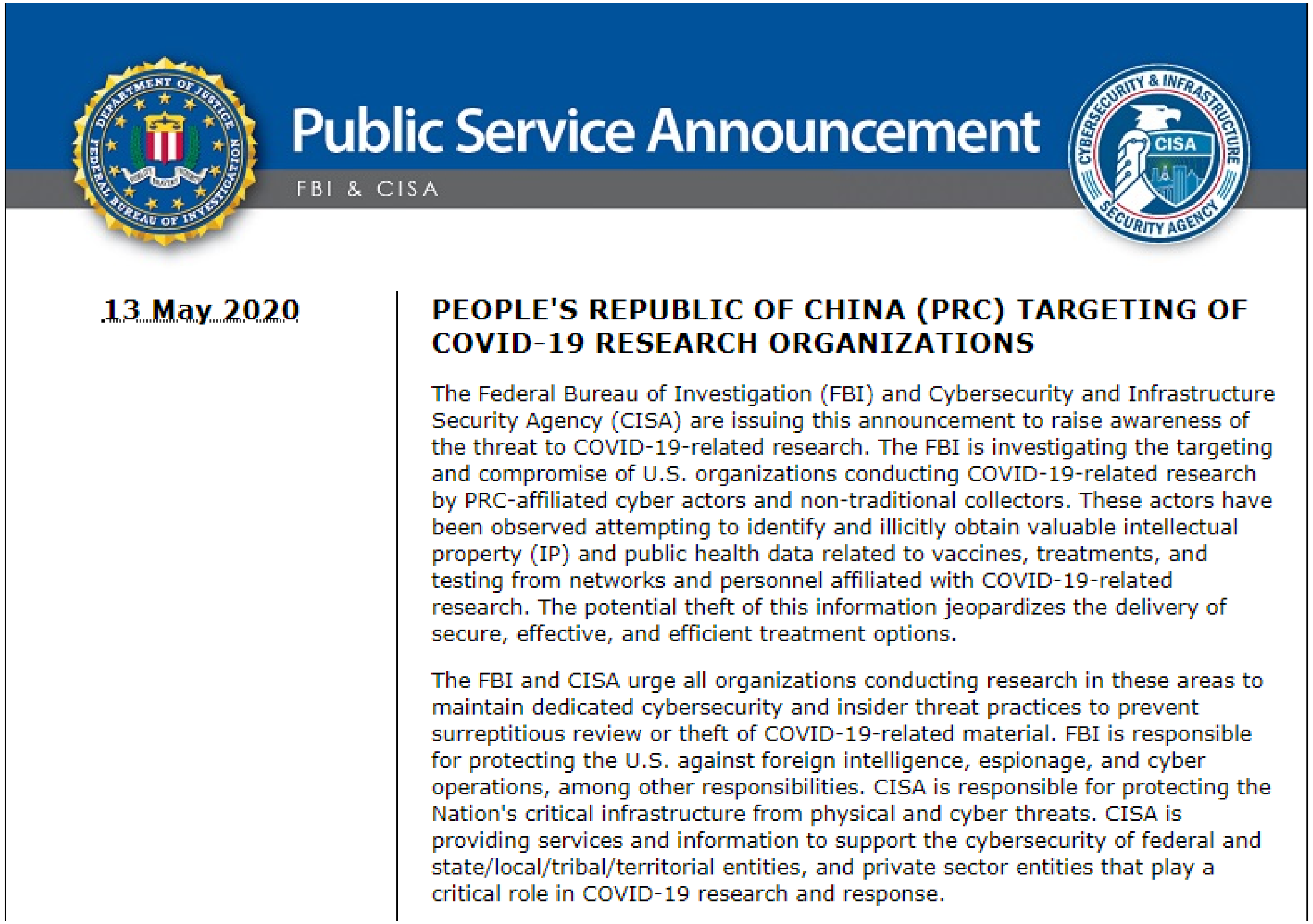
Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

Phishing Emails. Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

- Charitable contributions
- General financial relief

Covid-19 Related Threats



Public Service Announcement

FBI & CISA

13 May 2020

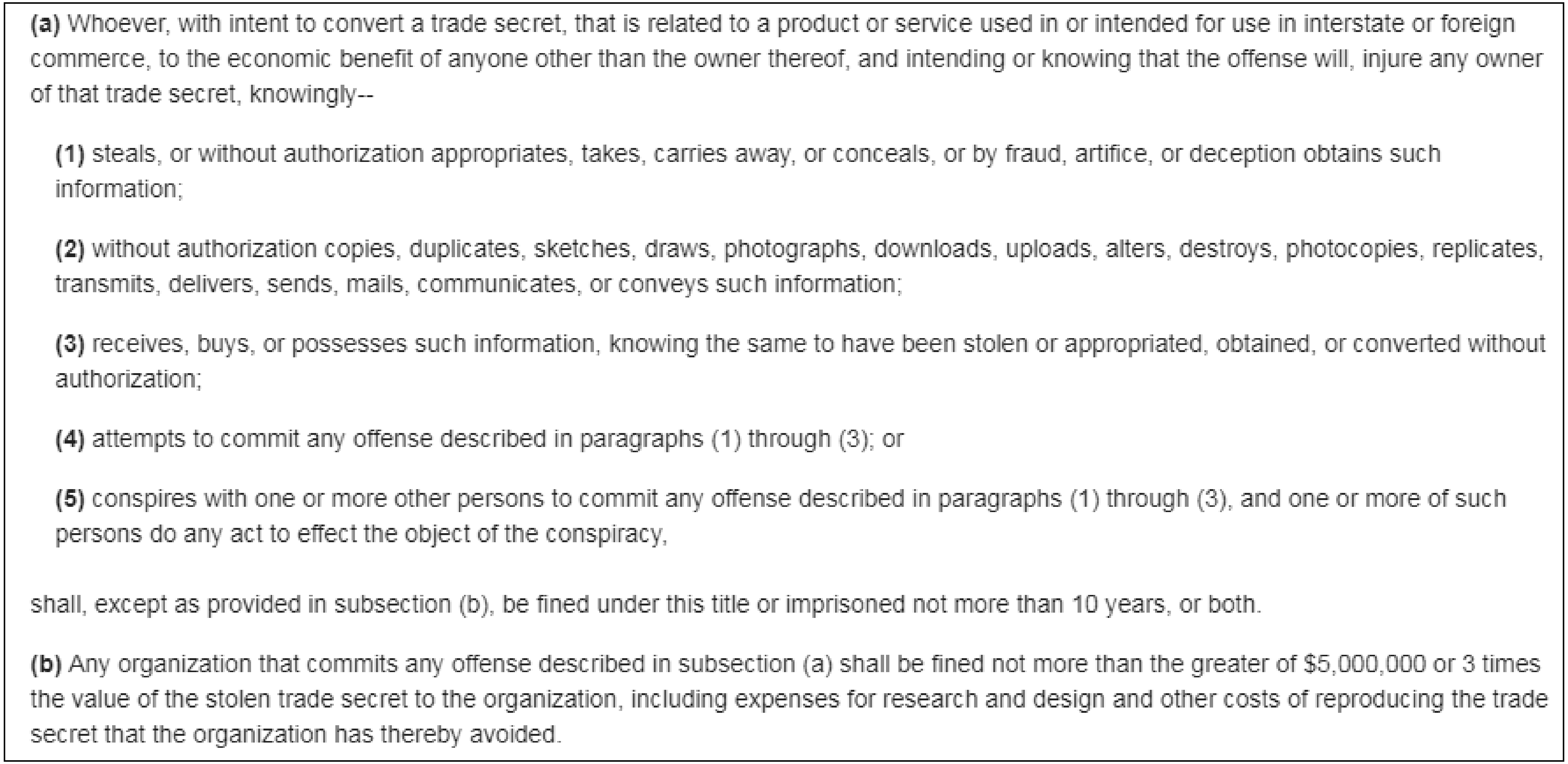
PEOPLE'S REPUBLIC OF CHINA (PRC) TARGETING OF COVID-19 RESEARCH ORGANIZATIONS

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the threat to COVID-19-related research. The FBI is investigating the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors. These actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. The potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options.

The FBI and CISA urge all organizations conducting research in these areas to maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material. FBI is responsible for protecting the U.S. against foreign intelligence, espionage, and cyber operations, among other responsibilities. CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. CISA is providing services and information to support the cybersecurity of federal and state/local/tribal/territorial entities, and private sector entities that play a critical role in COVID-19 research and response.

Source: https://www.ic3.gov/media/2020/200513.aspx

18 U.S.C. § 1832 Theft of Trade Secrets



(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

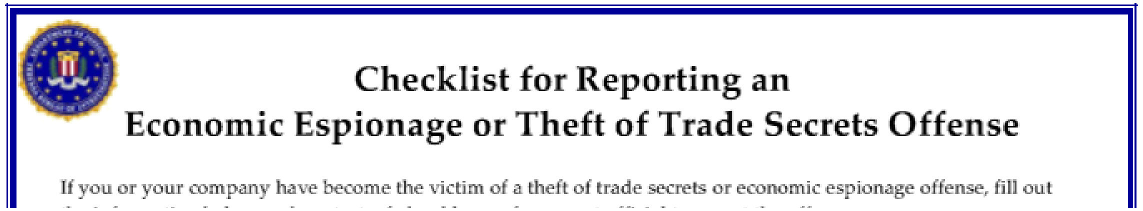
(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

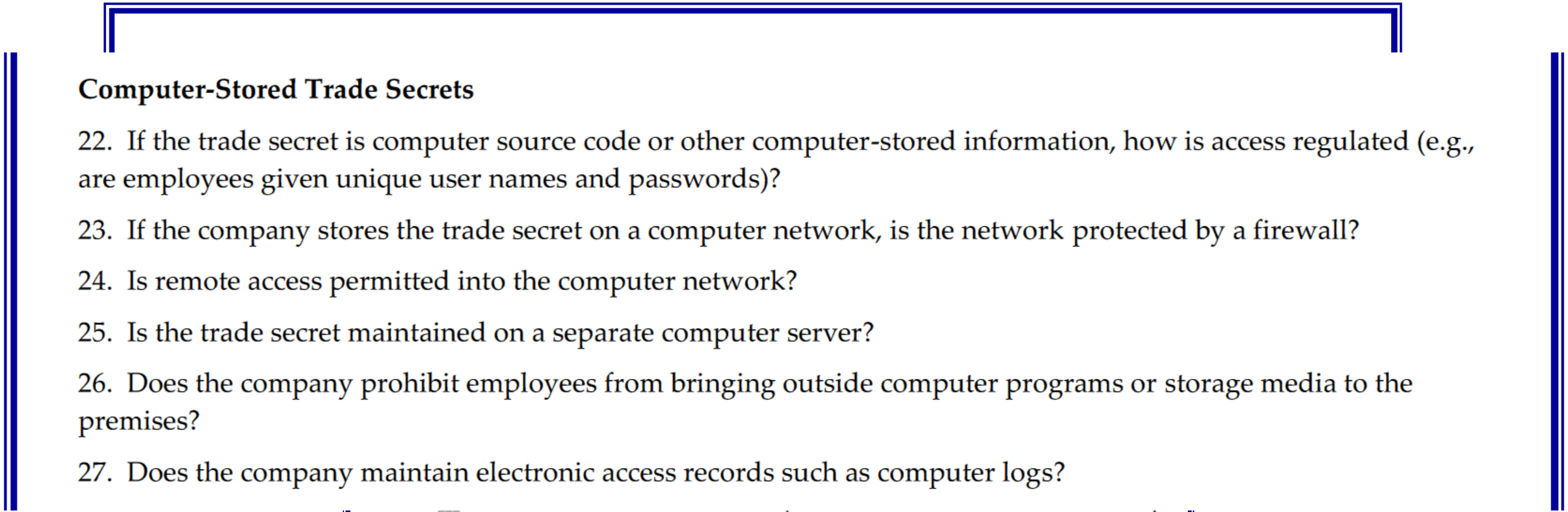
(b) Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

Legal Response



Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense

If you or your company have become the victim of a theft of trade secrets or economic espionage offense, fill out



Computer-Stored Trade Secrets

22. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names and passwords)?

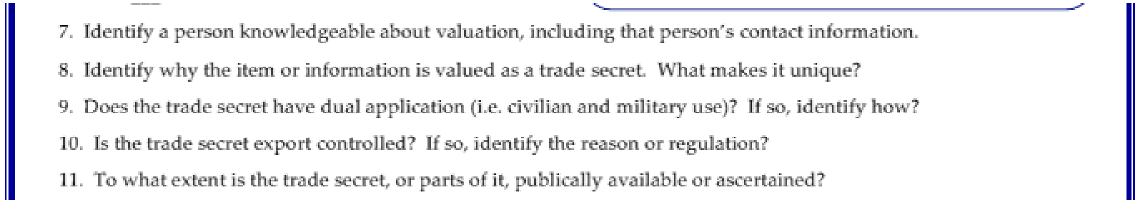
23. If the company stores the trade secret on a computer network, is the network protected by a firewall?

24. Is remote access permitted into the computer network?

25. Is the trade secret maintained on a separate computer server?

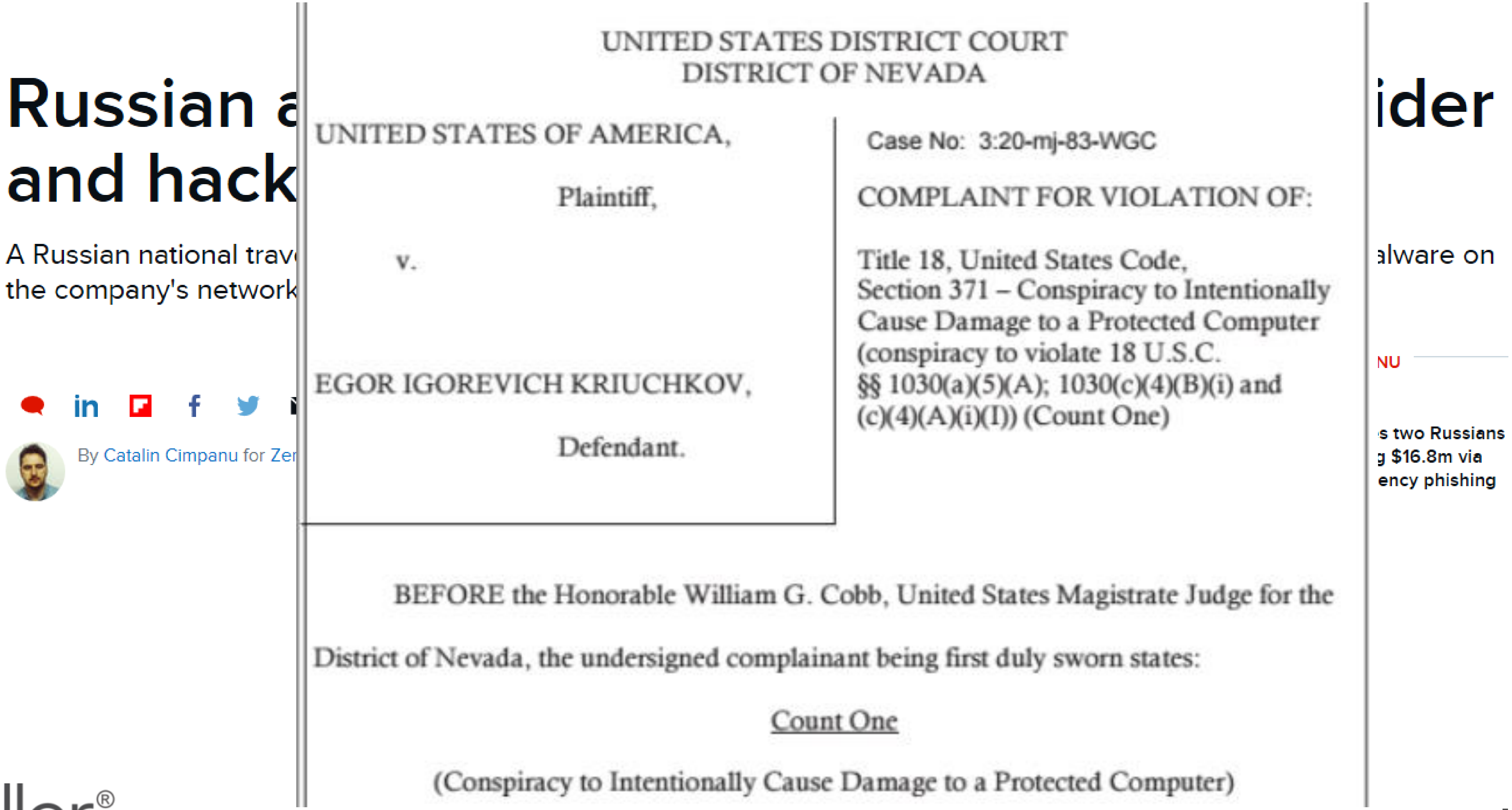
26. Does the company prohibit employees from bringing outside computer programs or storage media to the premises?

27. Does the company maintain electronic access records such as computer logs?



7. Identify a person knowledgeable about valuation, including that person's contact information.
8. Identify why the item or information is valued as a trade secret. What makes it unique?
9. Does the trade secret have dual application (i.e. civilian and military use)? If so, identify how?
10. Is the trade secret export controlled? If so, identify the reason or regulation?
11. To what extent is the trade secret, or parts of it, publically available or ascertained?

Legal Response



Russian a

and hack

ider

A Russian national trav

the company's network

alware on

By Catalin Cimpanu for Zer

NU

s two Russians

g $16.8m via

ency phishing

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA,

Plaintiff,

v.

EGOR IGOREVICH KRIUCHKOV,

Defendant.

Case No: 3:20-mj-83-WGC

COMPLAINT FOR VIOLATION OF:

Title 18, United States Code, Section 371 – Conspiracy to Intentionally Cause Damage to a Protected Computer (conspiracy to violate 18 U.S.C. §§ 1030(a)(5)(A); 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I)) (Count One)

BEFORE the Honorable William G. Cobb, United States Magistrate Judge for the District of Nevada, the undersigned complainant being first duly sworn states:

Count One

(Conspiracy to Intentionally Cause Damage to a Protected Computer)

Fund Transfer Fraud

Town of Erie scammed out of more than $1 million in bridge project

Just over $1.01 million was sent to an unknown person for Erie Parkway Bridge construction

Unintended Disclosures

Mitigation: Working Remotely

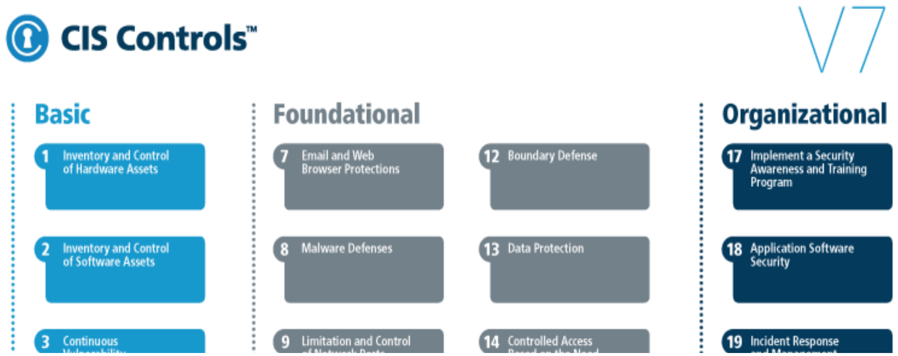
- Use a Virtual Private Network (VPN) to the extent possible
- Improve personal network security
- Use antivirus software
- Install home firewall
- Install mufti-factor authentication

Mitigation: Phishing and BEC Attacks

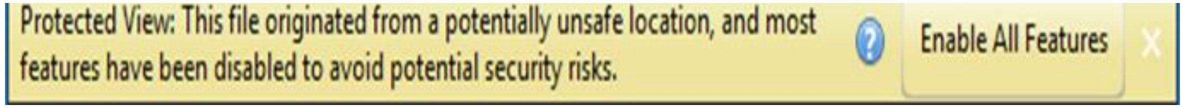
- People, Policies, and Processes
- Table Top Exercises, Penetration Testing
- Education and Training

Mitigation: Ransomware

- Implement technical safeguards:


CIS Controls™
V7
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control
12 Boundary Defense
13 Data Protection
14 Controlled Access
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response

EXTERNAL EMAIL WARNING! Use caution with links, attachments, or responses. DO Not provide your credentials!

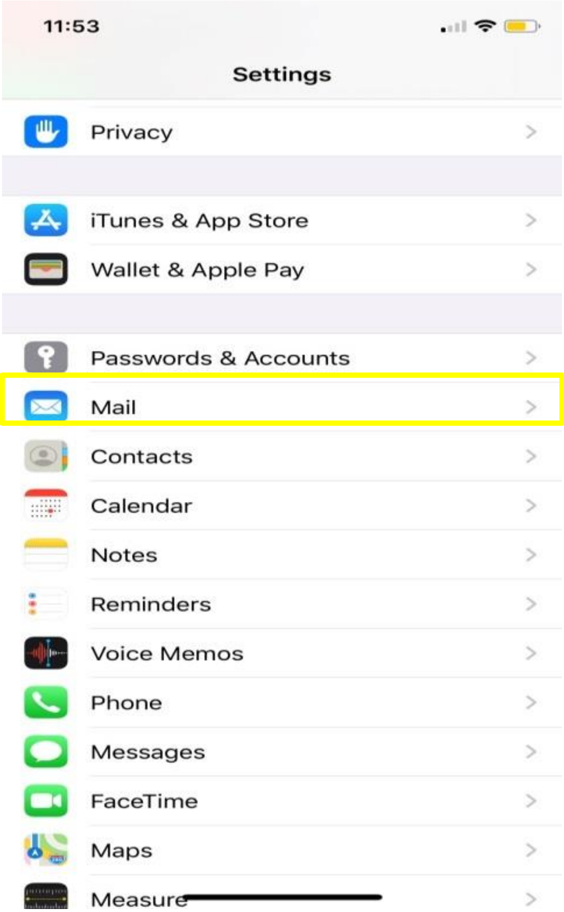


Protected View: This file originated from a potentially unsafe location, and most features have been disabled to avoid potential security risks.

Mitigation: Fund Transfer Fraud

Assess vendor agreements for liability

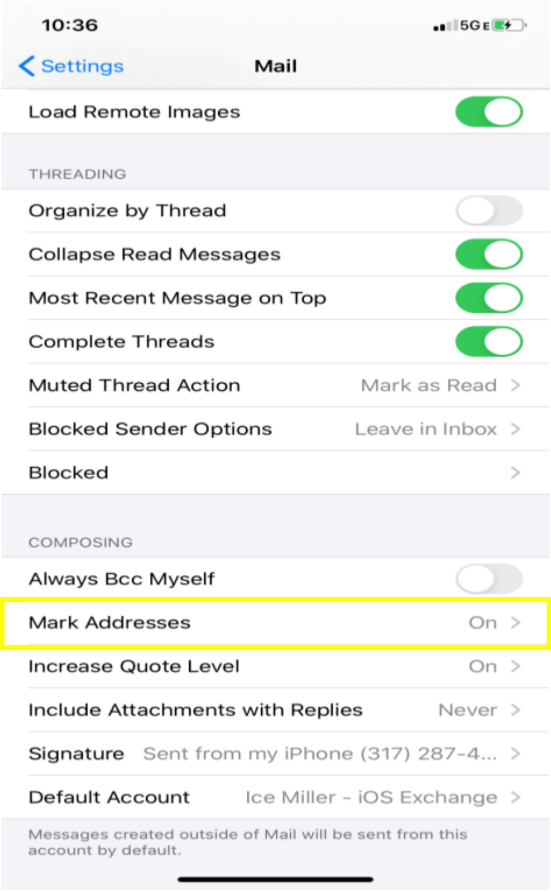
Mitigation: Inadvertent Disclosure on iPhone



11:53

Settings

- Privacy
- iTunes & App Store
- Wallet & Apple Pay
- Passwords & Accounts
- Mail
- Contacts
- Calendar
- Notes
- Reminders
- Voice Memos
- Phone
- Messages
- FaceTime
- Maps
- Measure



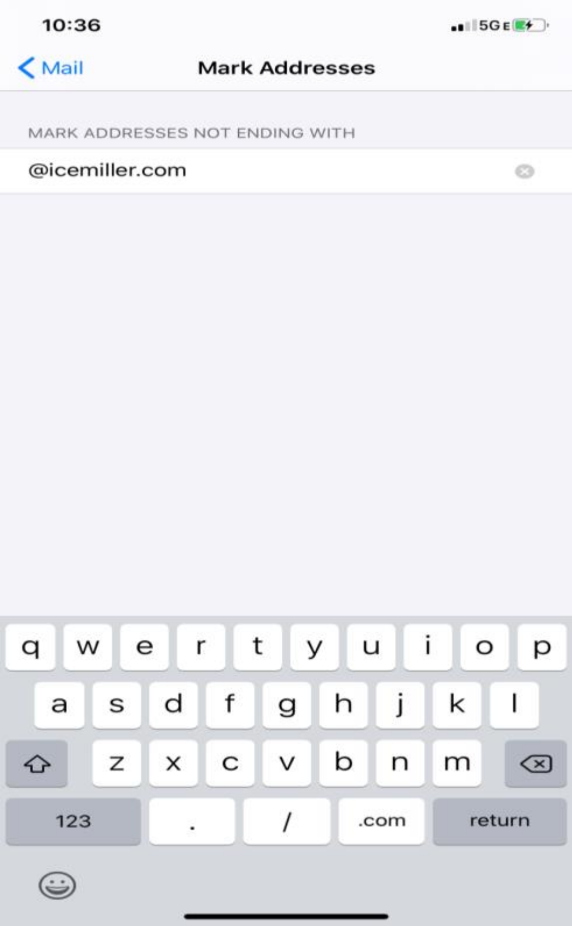
10:36

< Settings Mail

Load Remote Images	●
THREADING	
Organize by Thread	○
Collapse Read Messages	●
Most Recent Message on Top	●
Complete Threads	●
Muted Thread Action	Mark as Read >
Blocked Sender Options	Leave in Inbox >
Blocked	>
COMPOSING	
Always Bcc Myself	○
Mark Addresses	On >
Increase Quote Level	On >
Include Attachments with Replies	Never >
Signature	Sent from my iPhone (317) 287-4... >
Default Account	Ice Miller - iOS Exchange >

Messages created outside of Mail will be sent from this account by default.

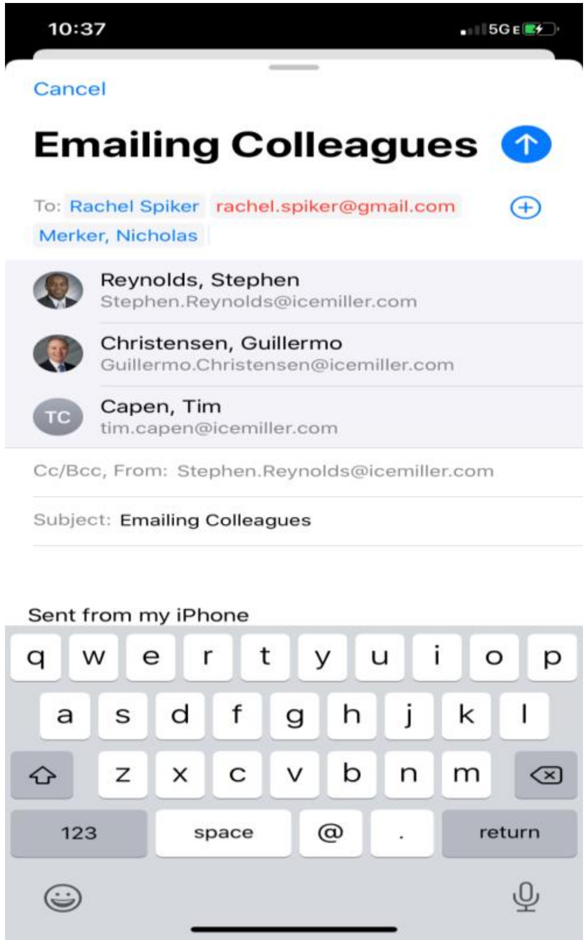
Mitigation: Inadvertent Disclosure on iPhone



Mark Addresses

MARK ADDRESSES NOT ENDING WITH

@icemiller.com



Emailing Colleagues

To: Rachel Spiker rachel.spiker@gmail.com

Merker, Nicholas

Reynolds, Stephen
Stephen.Reynolds@icemiller.com

Christensen, Guillermo
Guillermo.Christensen@icemiller.com

TC Capen, Tim
tim.capen@icemiller.com

Cc/Bcc, From: Stephen.Reynolds@icemiller.com

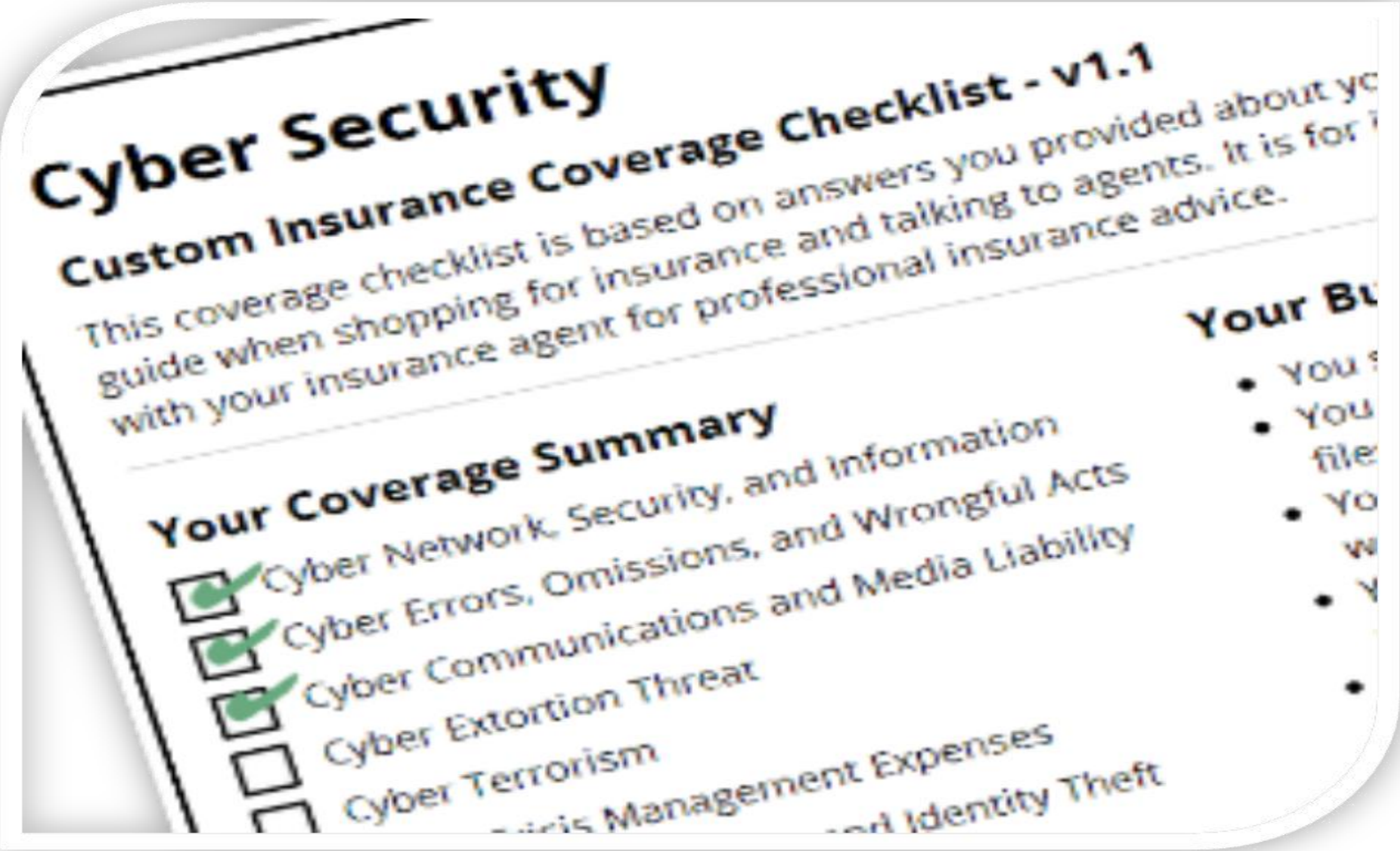
Subject: Emailing Colleagues

Sent from my iPhone

IceMiller®
LEGAL COUNSEL

Mitigation: Cyber-risk Insurance

Obtain cyber liability insurance



Cyber Security

Custom Insurance Coverage Checklist - v1.1

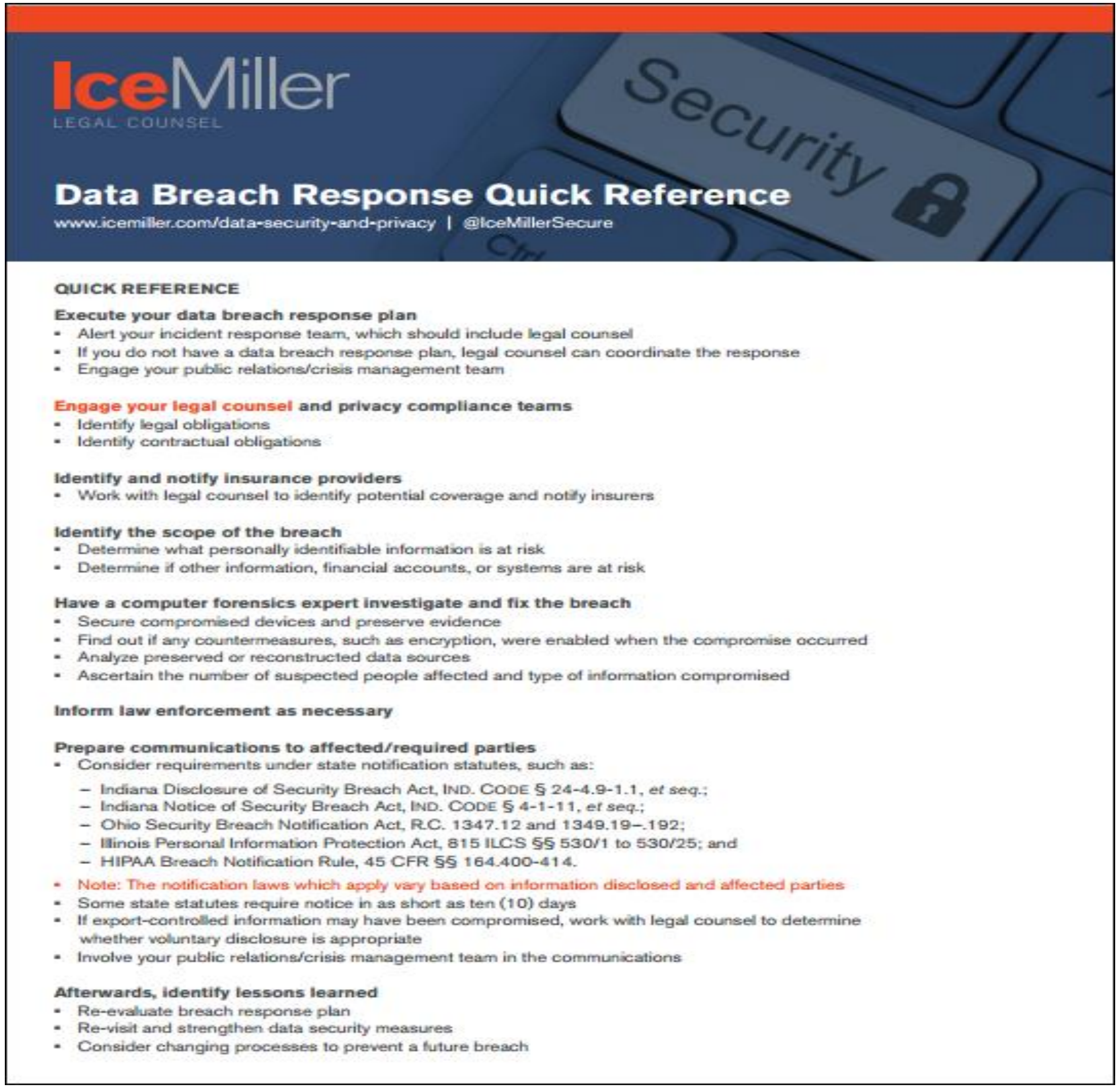
This coverage checklist is based on answers you provided about yo
guide when shopping for insurance and talking to agents. It is for i
with your insurance agent for professional insurance advice.

Your Coverage Summary

☑ Cyber Network, Security, and Information
☑ Cyber Errors, Omissions, and Wrongful Acts
☑ Cyber Communications and Media Liability
□ Cyber Extortion Threat
□ Cyber Terrorism
□ risis Management Expenses
nd Identity Theft

Your Bu
- You
- You file
- Yo w
- Y
-

Mitigation: Incident Response Plan


Security
Ctrl

IceMiller
LEGAL COUNSEL

Data Breach Response Quick Reference

www.icemiller.com/data-security-and-privacy | @IceMillerSecure

QUICK REFERENCE

Execute your data breach response plan

- Alert your incident response team, which should include legal counsel
- If you do not have a data breach response plan, legal counsel can coordinate the response
- Engage your public relations/crisis management team

Engage your legal counsel and privacy compliance teams

- Identify legal obligations
- Identify contractual obligations

Identify and notify insurance providers

- Work with legal counsel to identify potential coverage and notify insurers

Identify the scope of the breach

- Determine what personally identifiable information is at risk
- Determine if other information, financial accounts, or systems are at risk

Have a computer forensics expert investigate and fix the breach

- Secure compromised devices and preserve evidence
- Find out if any countermeasures, such as encryption, were enabled when the compromise occurred
- Analyze preserved or reconstructed data sources
- Ascertain the number of suspected people affected and type of information compromised

Inform law enforcement as necessary

Prepare communications to affected/required parties

- Consider requirements under state notification statutes, such as:
  - Indiana Disclosure of Security Breach Act, IND. CODE § 24-4.9-1.1, *et seq.*;
  - Indiana Notice of Security Breach Act, IND. CODE § 4-1-11, *et seq.*;
  - Ohio Security Breach Notification Act, R.C. 1347.12 and 1349.19–.192;
  - Illinois Personal Information Protection Act, 815 ILCS §§ 530/1 to 530/25; and
  - HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.
- Note: The notification laws which apply vary based on information disclosed and affected parties
- Some state statutes require notice in as short as ten (10) days
- If export-controlled information may have been compromised, work with legal counsel to determine whether voluntary disclosure is appropriate
- Involve your public relations/crisis management team in the communications

Afterwards, identify lessons learned

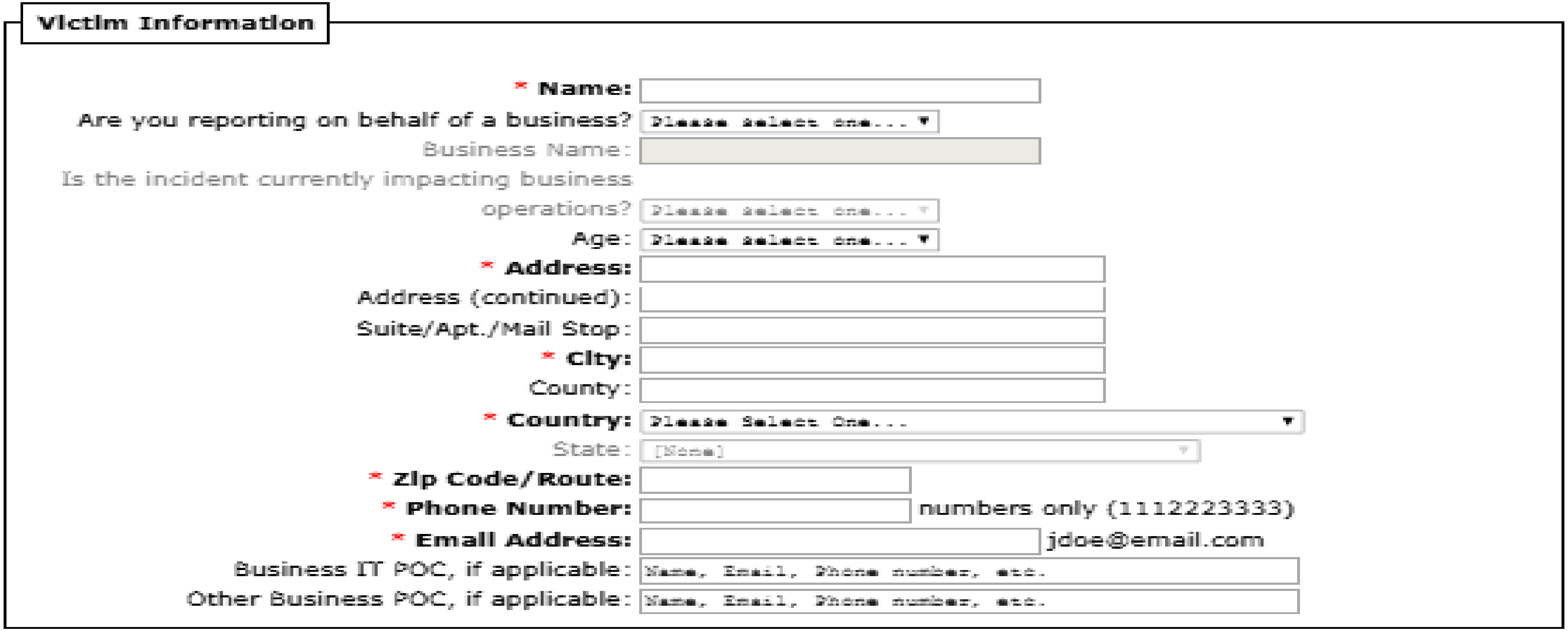
- Re-evaluate breach response plan
- Re-visit and strengthen data security measures
- Consider changing processes to prevent a future breach

Develop and implement an Incident Response Plan

Incident Response: Lawyers

- Assist with execution of breach response plan
- Identify legal and contractual obligations
- Identify potential insurance coverage and notify insurers
- Identify scope of the breach
- Oversee forensic investigation into incident
- Work with law enforcement
- Prepare required notifications under applicable state, federal, and international laws

Incident Response: Law Enforcement



Victim Information

* **Name:**

Are you reporting on behalf of a business? Please select one... ▼

Business Name:

Is the incident currently impacting business operations? Please select one... ▼

Age: Please select one... ▼

* **Address:**

Address (continued):

Suite/Apt./Mail Stop:

* **City:**

County:

* **Country:** Please Select One... ▼

State: [None] ▼

* **Zip Code/Route:**

* **Phone Number:** numbers only (1112223333)

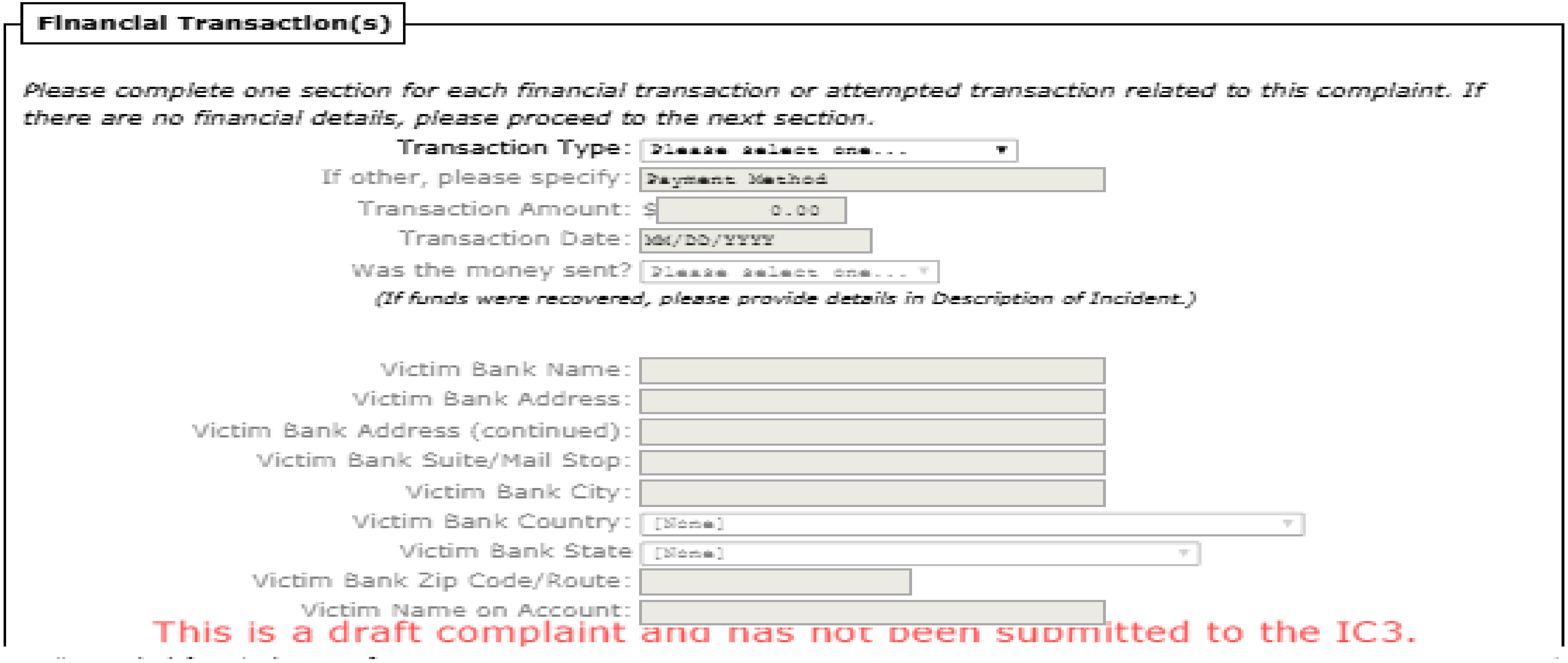
* **Email Address:** jdoe@email.com

Business IT POC, if applicable: Name, Email, Phone number, etc.

Other Business POC, if applicable: Name, Email, Phone number, etc.

Report
Internet Crime
to the FBI
www.ic3.gov
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
FEDERAL BUREAU OF INVESTIGATION
INTERNET CRIME COMPLAINT CENTER
IC3

Incident Response: Law Enforcement



Financial Transaction(s)

Please complete one section for each financial transaction or attempted transaction related to this complaint. If there are no financial details, please proceed to the next section.

Transaction Type: Please select one... ▾

If other, please specify: Payment Method

Transaction Amount: $ 0.00

Transaction Date: MM/DD/YYYY

Was the money sent? Please select one... ▾

(If funds were recovered, please provide details in Description of Incident.)

Victim Bank Name:

Victim Bank Address:

Victim Bank Address (continued):

Victim Bank Suite/Mail Stop:

Victim Bank City:

Victim Bank Country: [None] ▾

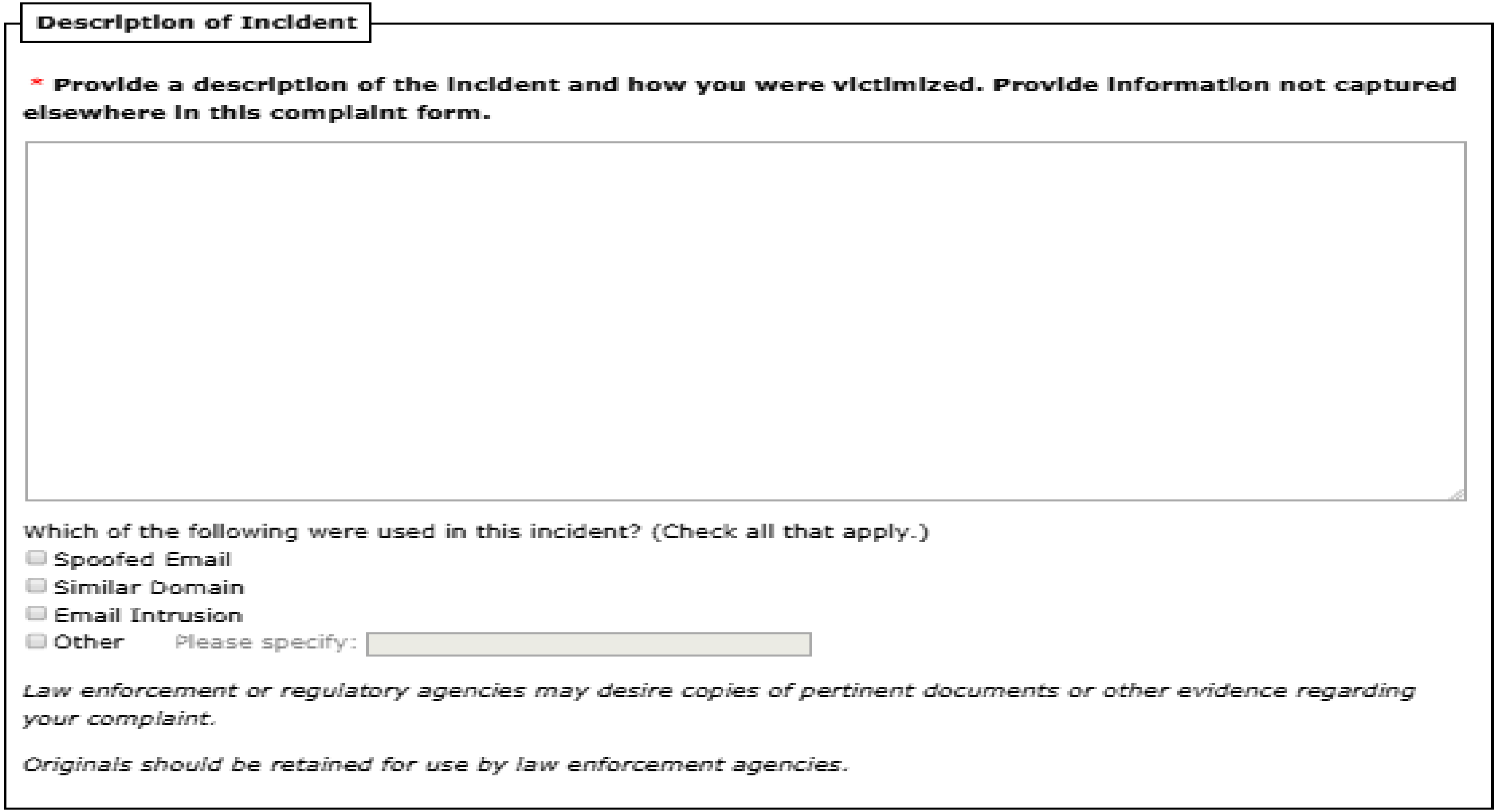
Victim Bank State: [None] ▾

Victim Bank Zip Code/Route:

Victim Name on Account:

This is a draft complaint and has not been submitted to the IC3.

Incident Response: Law Enforcement



Description of Incident

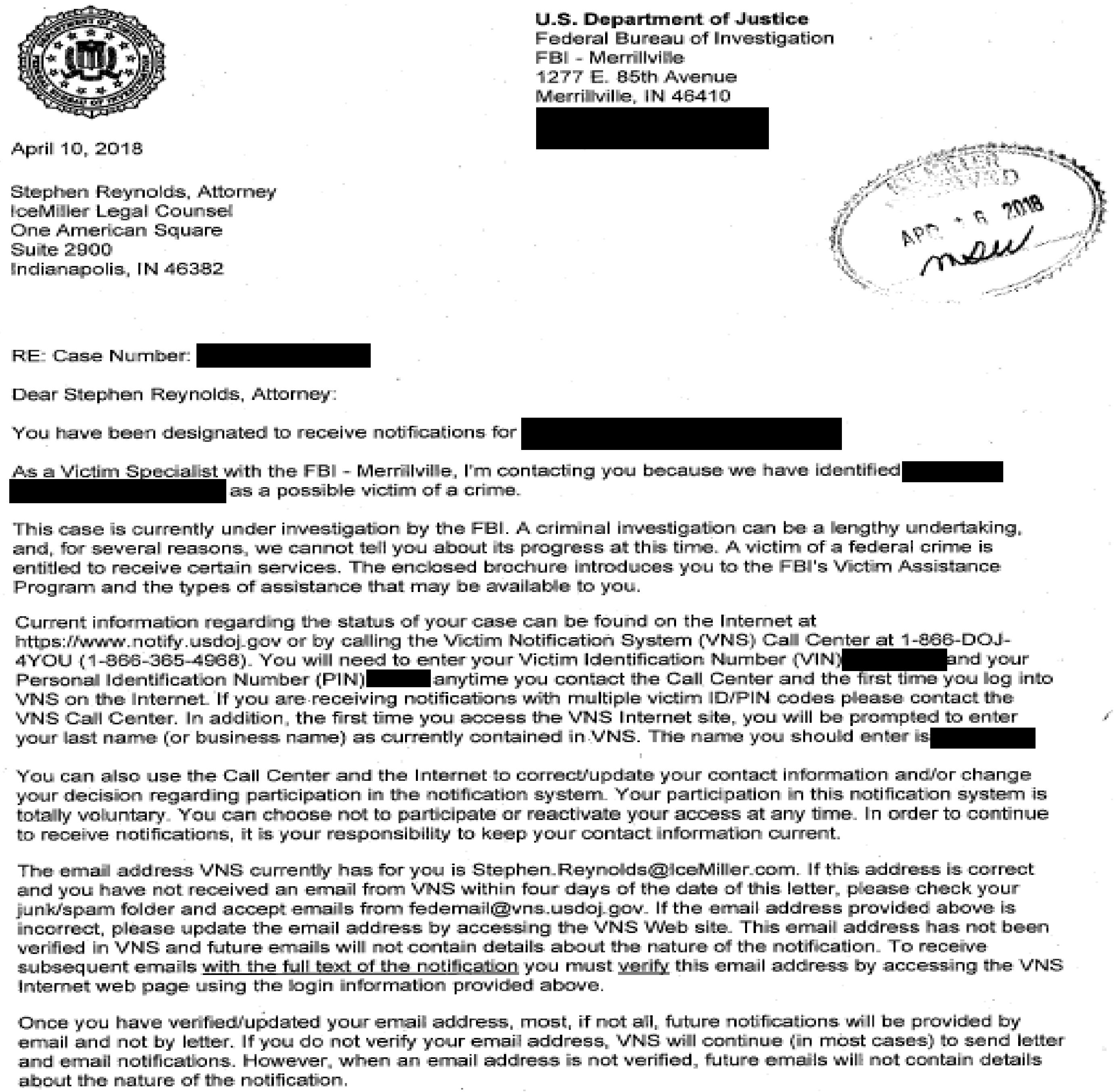
*** Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.**

Which of the following were used in this incident? (Check all that apply.)

□ Spoofed Email
□ Similar Domain
□ Email Intrusion
□ Other   Please specify:

Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.

Originals should be retained for use by law enforcement agencies.



U.S. Department of Justice
Federal Bureau of Investigation
FBI - Merrillville
1277 E. 85th Avenue
Merrillville, IN 46410
[redacted]

April 10, 2018

Stephen Reynolds, Attorney
IceMiller Legal Counsel
One American Square
Suite 2900
Indianapolis, IN 46382

RE: Case Number: [redacted]

Dear Stephen Reynolds, Attorney:

You have been designated to receive notifications for [redacted]

As a Victim Specialist with the FBI - Merrillville, I'm contacting you because we have identified [redacted] [redacted] as a possible victim of a crime.

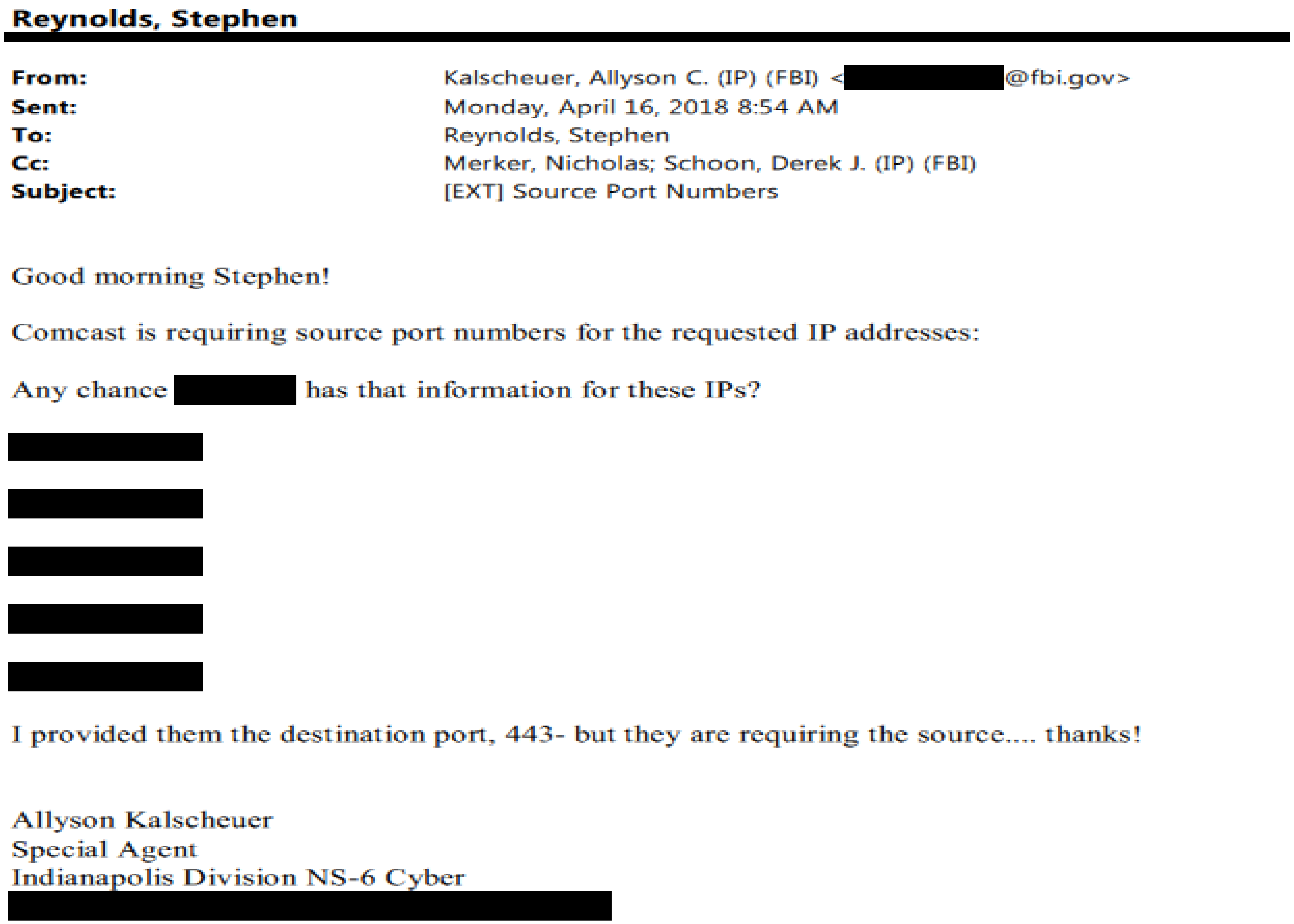
This case is currently under investigation by the FBI. A criminal investigation can be a lengthy undertaking, and, for several reasons, we cannot tell you about its progress at this time. A victim of a federal crime is entitled to receive certain services. The enclosed brochure introduces you to the FBI's Victim Assistance Program and the types of assistance that may be available to you.

Current information regarding the status of your case can be found on the Internet at https://www.notify.usdoj.gov or by calling the Victim Notification System (VNS) Call Center at 1-866-DOJ-4YOU (1-866-365-4968). You will need to enter your Victim Identification Number (VIN) [redacted] and your Personal Identification Number (PIN) [redacted] anytime you contact the Call Center and the first time you log into VNS on the Internet. If you are receiving notifications with multiple victim ID/PIN codes please contact the VNS Call Center. In addition, the first time you access the VNS Internet site, you will be prompted to enter your last name (or business name) as currently contained in VNS. The name you should enter is [redacted]

You can also use the Call Center and the Internet to correct/update your contact information and/or change your decision regarding participation in the notification system. Your participation in this notification system is totally voluntary. You can choose not to participate or reactivate your access at any time. In order to continue to receive notifications, it is your responsibility to keep your contact information current.

The email address VNS currently has for you is Stephen.Reynolds@IceMiller.com. If this address is correct and you have not received an email from VNS within four days of the date of this letter, please check your junk/spam folder and accept emails from fedemail@vns.usdoj.gov. If the email address provided above is incorrect, please update the email address by accessing the VNS Web site. This email address has not been verified in VNS and future emails will not contain details about the nature of the notification. To receive subsequent emails with the full text of the notification you must verify this email address by accessing the VNS Internet web page using the login information provided above.

Once you have verified/updated your email address, most, if not all, future notifications will be provided by email and not by letter. If you do not verify your email address, VNS will continue (in most cases) to send letter and email notifications. However, when an email address is not verified, future emails will not contain details about the nature of the notification.



Reynolds, Stephen

From: Kalscheuer, Allyson C. (IP) (FBI) <[redacted]@fbi.gov>
Sent: Monday, April 16, 2018 8:54 AM
To: Reynolds, Stephen
Cc: Merker, Nicholas; Schoon, Derek J. (IP) (FBI)
Subject: [EXT] Source Port Numbers

Good morning Stephen!

Comcast is requiring source port numbers for the requested IP addresses:

Any chance [redacted] has that information for these IPs?

[redacted]

I provided them the destination port, 443- but they are requiring the source.... thanks!

Allyson Kalscheuer
Special Agent
Indianapolis Division NS-6 Cyber
[redacted]

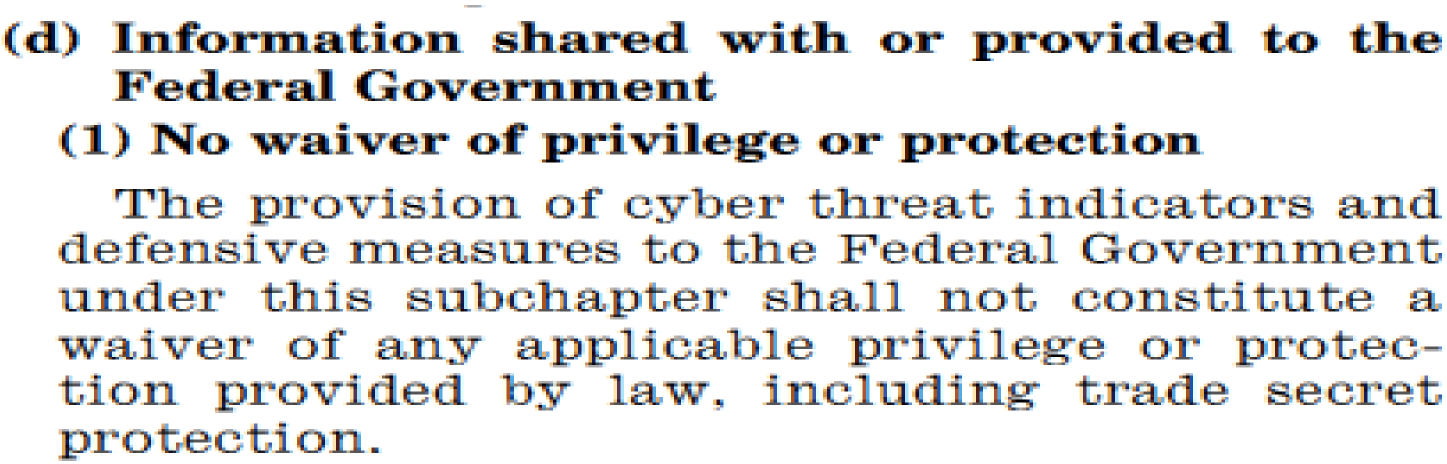
How do we all work together?

Lawyers
Regulators
Law Enforcement

Achieving Goals,
Preserving Privilege,
Assisting Investigation

Preserving Attorney-Client Privilege: Law Enforcement Collaboration

Cybersecurity Information Sharing Act of 2015 (CISA)



(d) Information shared with or provided to the Federal Government

(1) No waiver of privilege or protection

The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

Protections Conferred for Sharing Under CISA

No waiver of privilege for shared material
Liability protection for sharing of cyber threat indicators
Exemption from state & federal disclosure laws
Exemption from state & federal regulatory use
Treatment of commercial, financial, and proprietary information

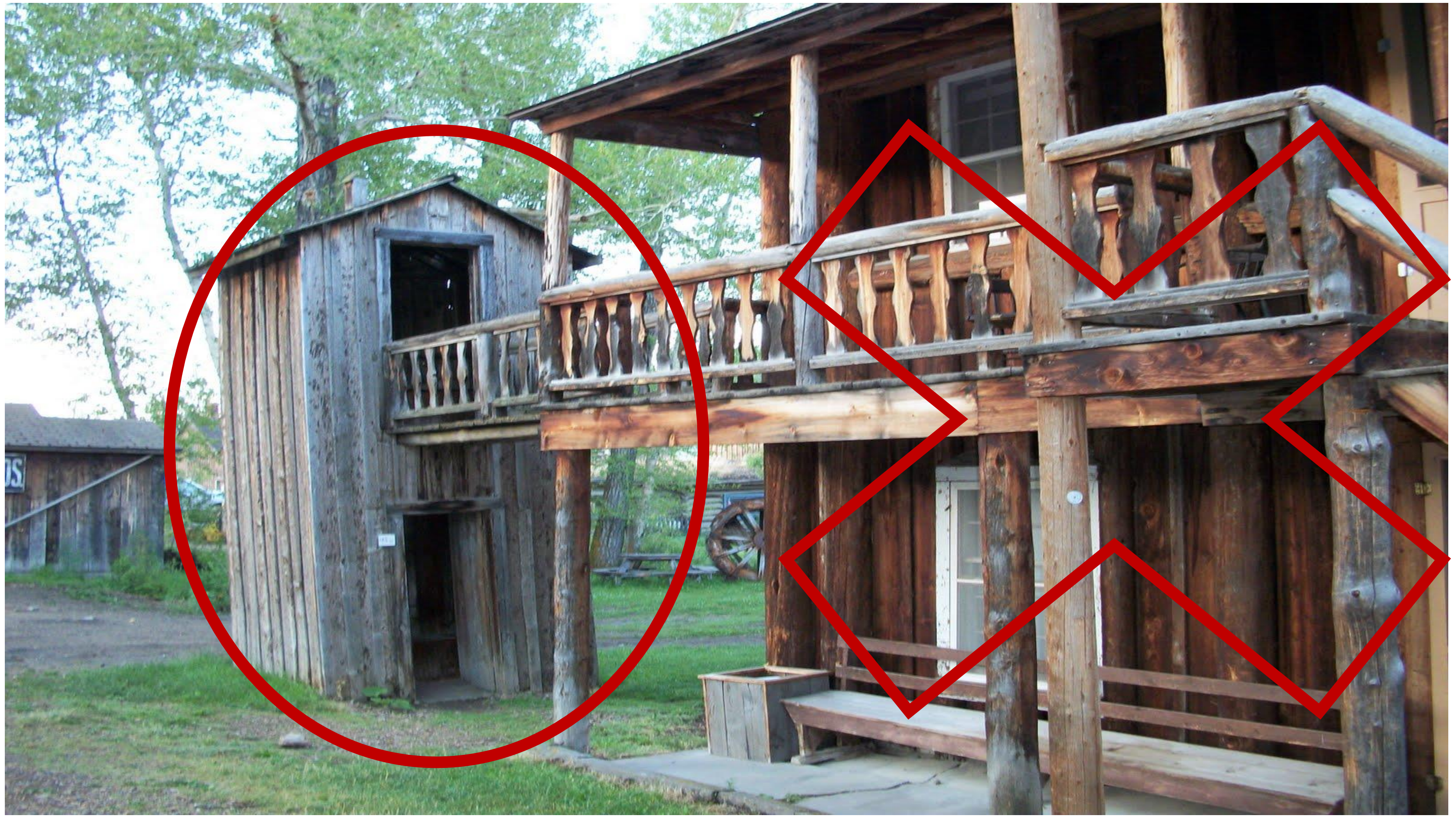
Retain Outside Counsel

Clearly distinguishes a legal purpose

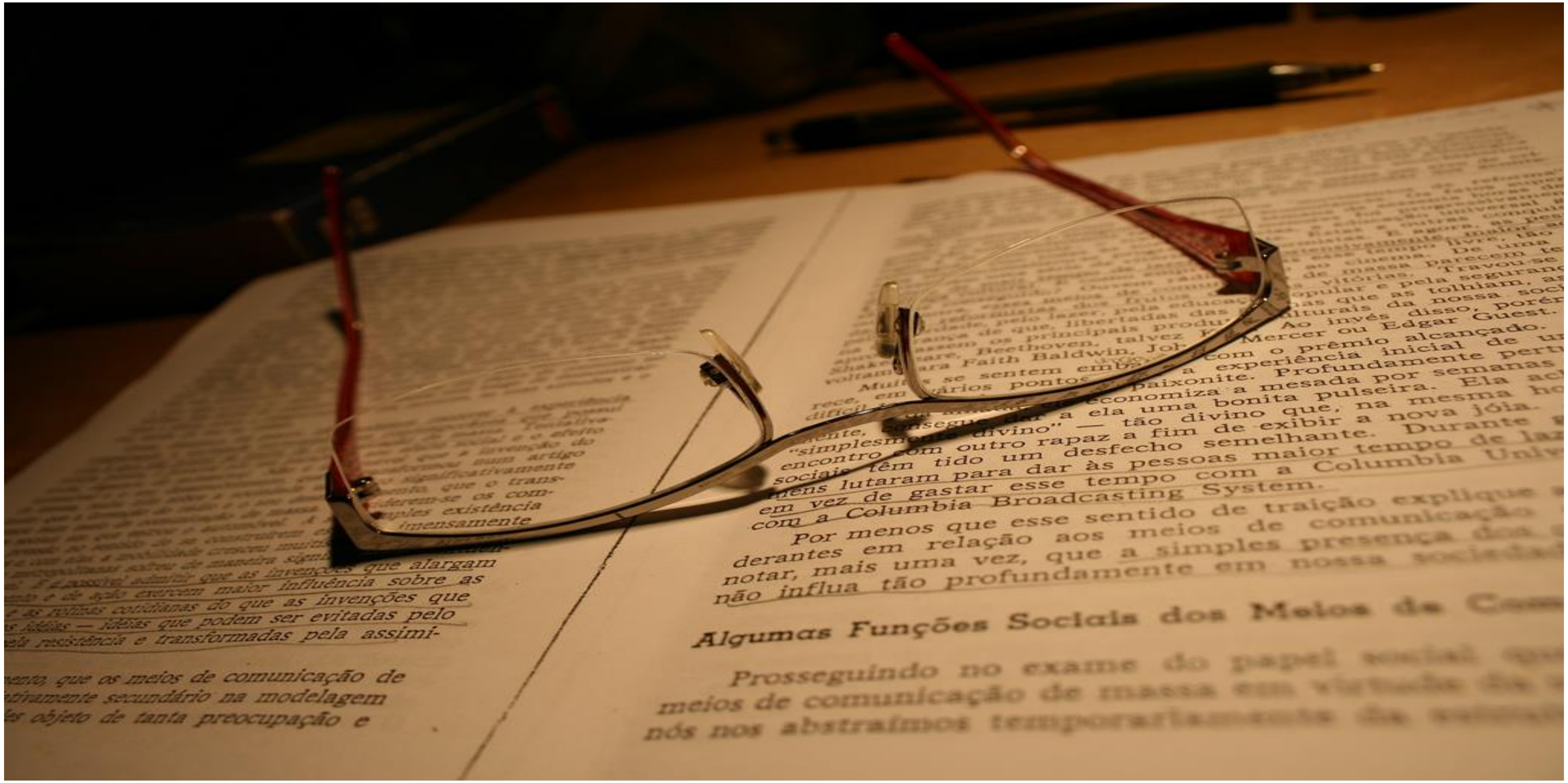
Supports the argument that documents were produced in anticipation of litigation

Engage Third Parties

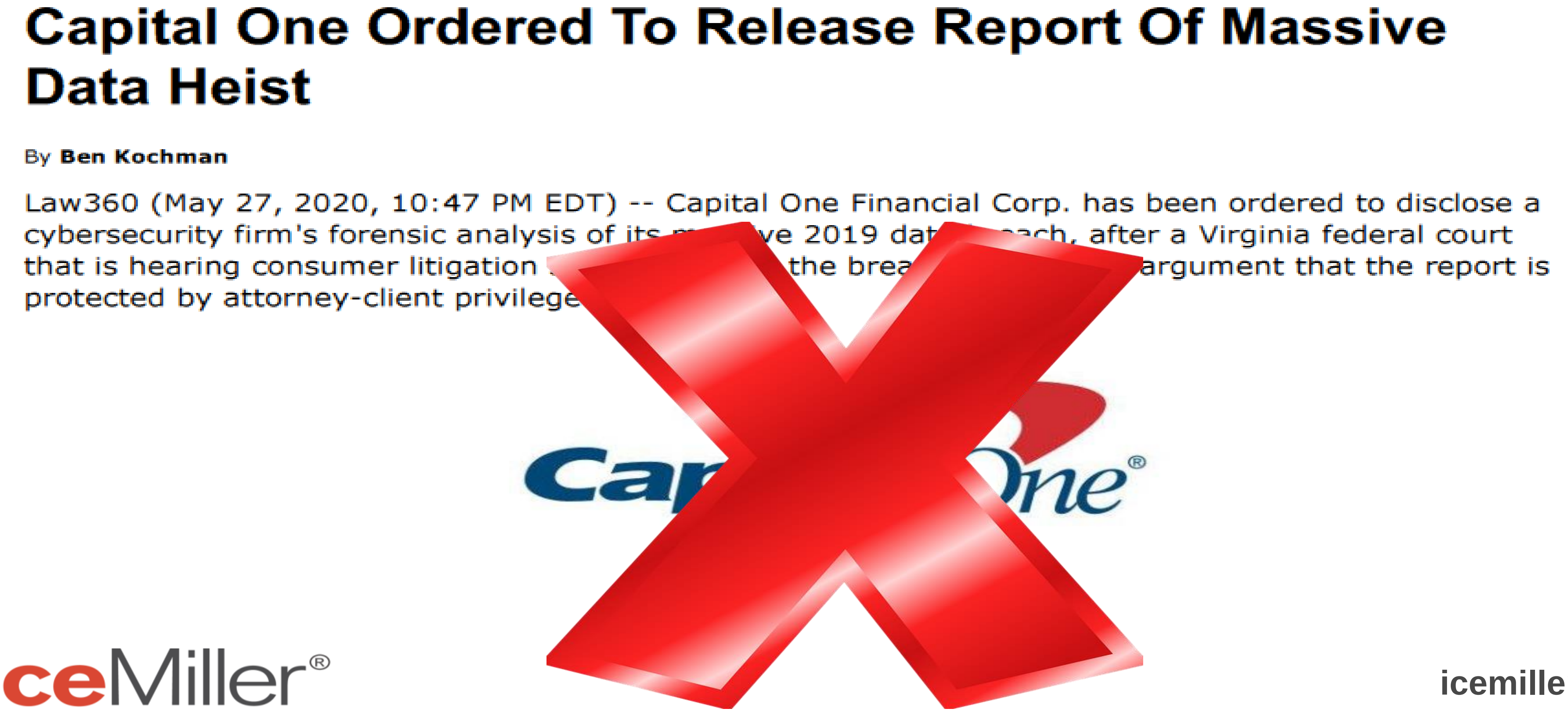
Outside counsel should engage cyber forensic company from the beginning



Case Studies



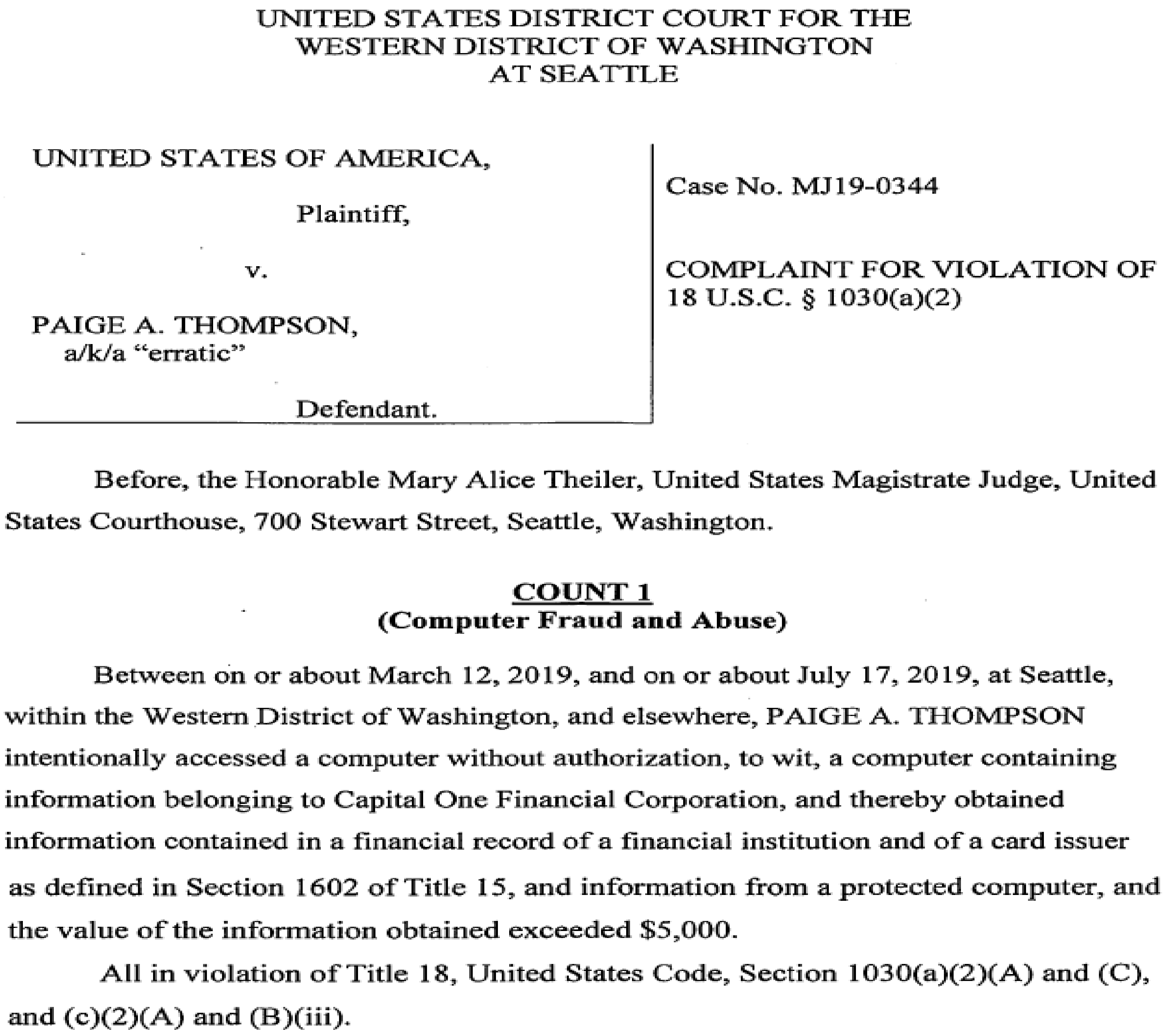
IN RE CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION



Capital One Ordered To Release Report Of Massive Data Heist

By **Ben Kochman**

Law360 (May 27, 2020, 10:47 PM EDT) -- Capital One Financial Corp. has been ordered to disclose a cybersecurity firm's forensic analysis of its m ve 2019 dat each, after a Virginia federal court that is hearing consumer litigation the brea argument that the report is protected by attorney-client privilege



UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

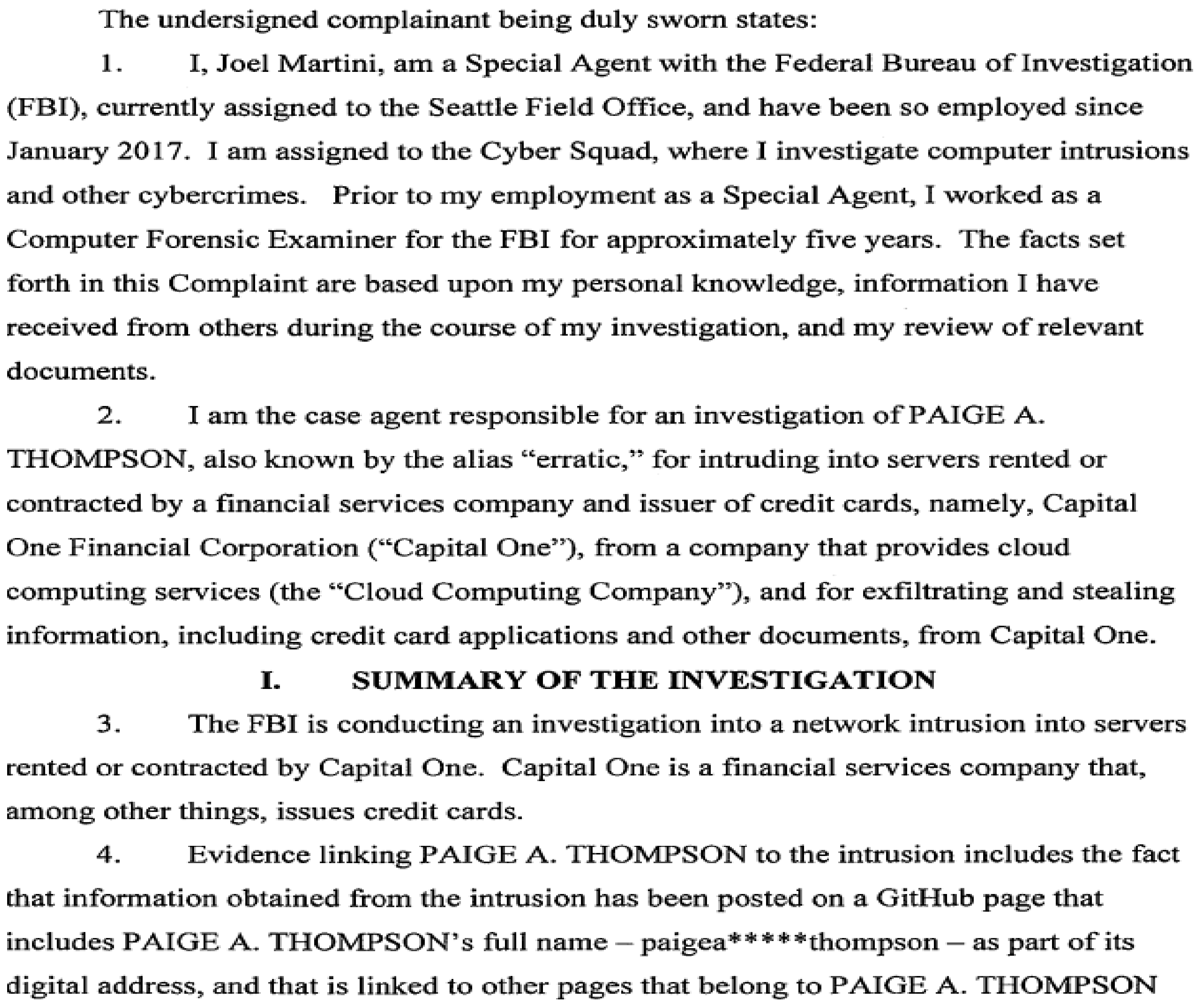
UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, a/k/a "erratic" Defendant.	Case No. MJ19-0344 COMPLAINT FOR VIOLATION OF 18 U.S.C. § 1030(a)(2)

Before, the Honorable Mary Alice Theiler, United States Magistrate Judge, United States Courthouse, 700 Stewart Street, Seattle, Washington.

COUNT 1
(Computer Fraud and Abuse)

Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer as defined in Section 1602 of Title 15, and information from a protected computer, and the value of the information obtained exceeded $5,000.

All in violation of Title 18, United States Code, Section 1030(a)(2)(A) and (C), and (c)(2)(A) and (B)(iii).



The undersigned complainant being duly sworn states:

1. I, Joel Martini, am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber Squad, where I investigate computer intrusions and other cybercrimes. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately five years. The facts set forth in this Complaint are based upon my personal knowledge, information I have received from others during the course of my investigation, and my review of relevant documents.

2. I am the case agent responsible for an investigation of PAIGE A. THOMPSON, also known by the alias "erratic," for intruding into servers rented or contracted by a financial services company and issuer of credit cards, namely, Capital One Financial Corporation ("Capital One"), from a company that provides cloud computing services (the "Cloud Computing Company"), and for exfiltrating and stealing information, including credit card applications and other documents, from Capital One.

I. SUMMARY OF THE INVESTIGATION

3. The FBI is conducting an investigation into a network intrusion into servers rented or contracted by Capital One. Capital One is a financial services company that, among other things, issues credit cards.

4. Evidence linking PAIGE A. THOMPSON to the intrusion includes the fact that information obtained from the intrusion has been posted on a GitHub page that includes PAIGE A. THOMPSON's full name – paigea*****thompson – as part of its digital address, and that is linked to other pages that belong to PAIGE A. THOMPSON

Genesco, Inc. v. Visa U.S.A., Inc.

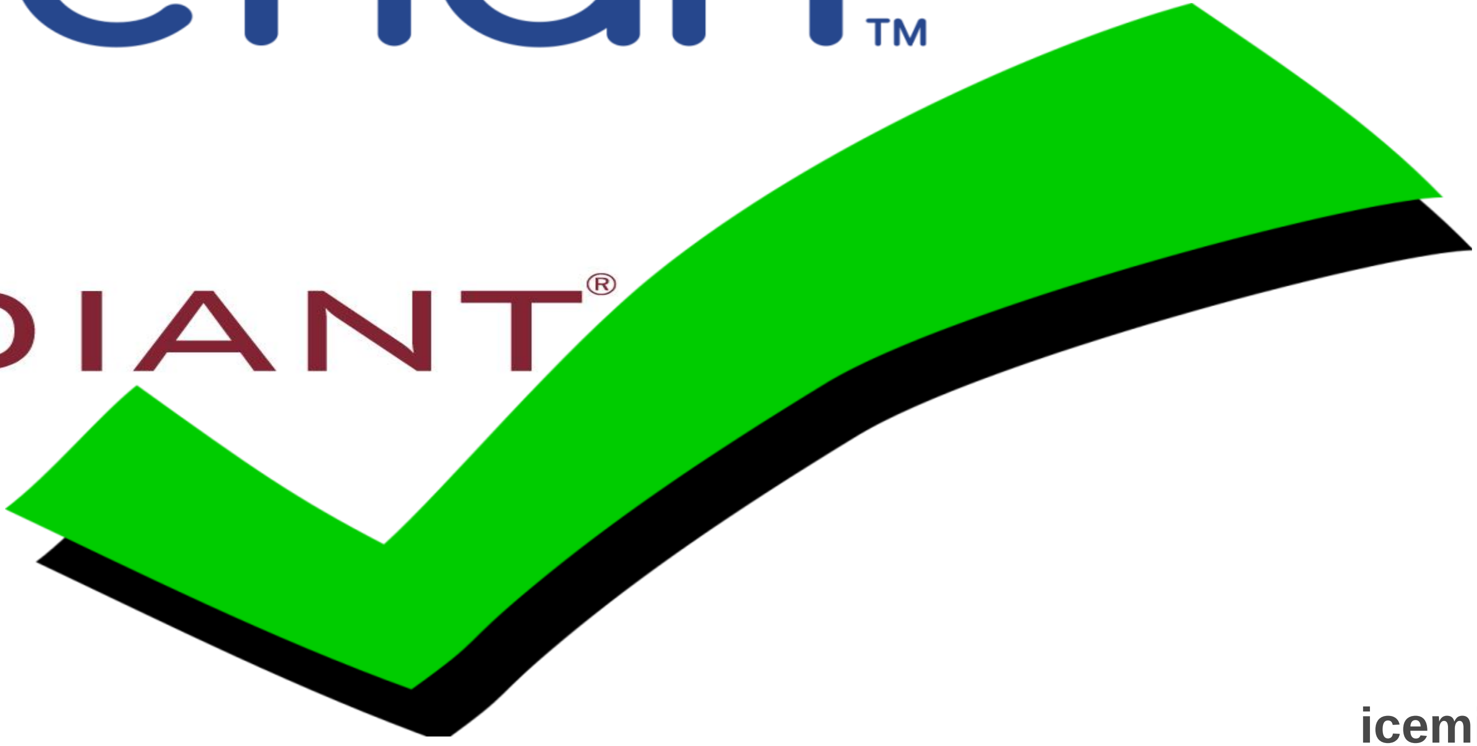
In Re Target Corp. Customer Data Security Breach Litigation

Banneker Ventures, LLC v. Graham (Washington Metropolitan Area Transit Authority)

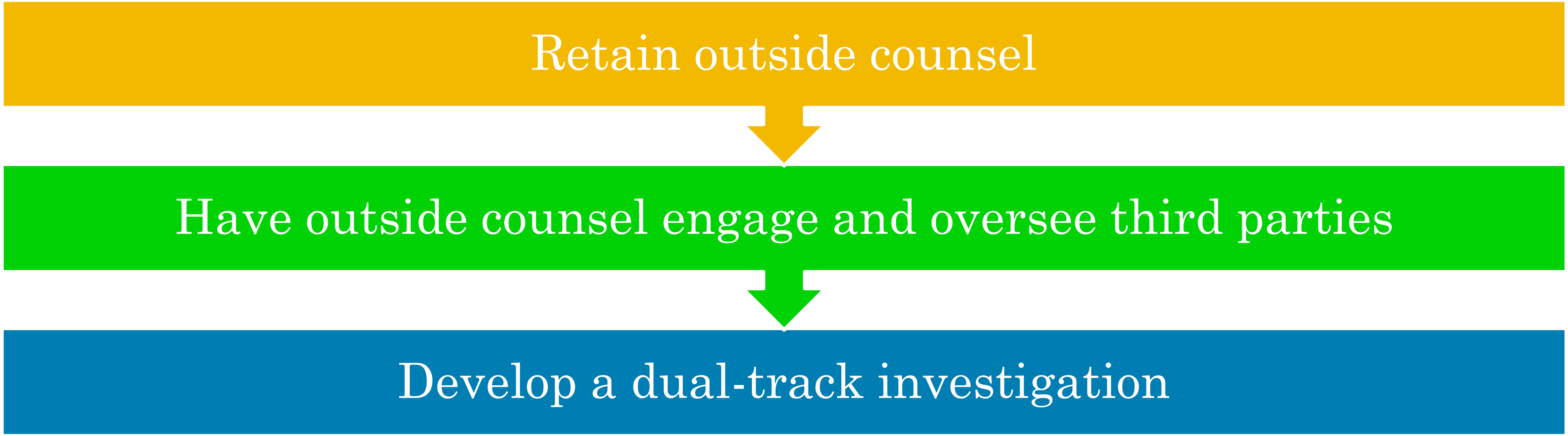
IN RE EXPERIAN DATA BREACH LITIGATION

experian™

MANDIANT®



Preserving Attorney-Client Privilege: Strategy for Data Breach Response



Retain outside counsel

Have outside counsel engage and oversee third parties

Develop a dual-track investigation

Questions?

Stephen Reynolds, CIPP/US, CISSP
Partner, Ice Miller LLP
Stephen.Reynolds@icemiller.com

Tiffany Kim, CIPP/US
Associate, Ice Miller LLP
Tiffany.Kim@icemiller.com

A Day in the Life

- Tyler Uffelman is a threat hunter at Allegion PLC in Carmel, Indiana. Previously, Tyler worked for an MSSP as a security analyst and as a contractor for the Department of Homeland Security. While working as a contractor at DHS, Tyler completed a Master's degree in Cyber Security.
- Tyler's accomplishments include earning Comptia CySA+ certification and published research by the IEEE related to IoT security.

A Day in the Life of a SOC Analyst

Tyler Uffelman – Threat Hunter

Target Audience

- New/aspiring security analysts – particularly blue teamers
- People interested in security team operations

Bio – Tyler Uffelman

- Threat hunter
- Comptia CySA+ Certified
- M.S. Cyber Security, published IoT researcher

What is an average day for a SOC analyst?

- Fun fact: no such thing exists

  Every day is different and provides new challenges

Examples of SOC analyst tasks

- Investigate traffic from a source (network, endpoint protection, alert, etc)
- Research threat intelligence and other modern security news
- Create reports on trends, current activity, etc
- Remediate a compromised entity post-investigation
- Configure/fortify infrastructure (settings, rules, blocks, whitelists, etc)

Examples of SOC Tools

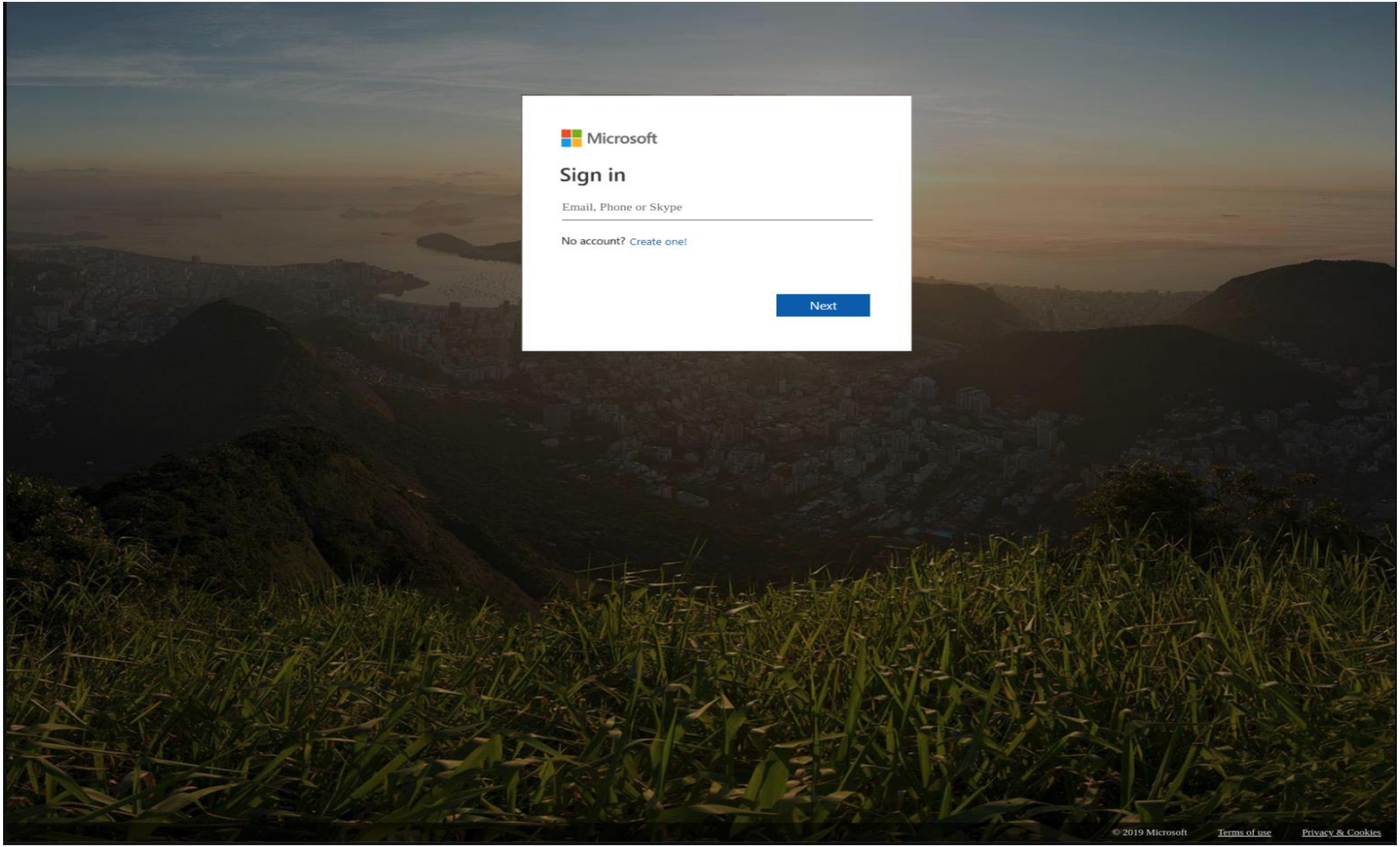
Examples of security tools

- SIEM
- Endpoint Protection
- Firewall
- DNS Filtering
- Alerting Platforms
- Threat Intelligence Platforms
- Vulnerability Management Platform
- Other (nmap, pcap analysis, malware analysis tools, etc)

Blue Team Mentality

- Desire to work in evidence-based practices
- Strategizing *reasonable* defensive measures
- Life learner

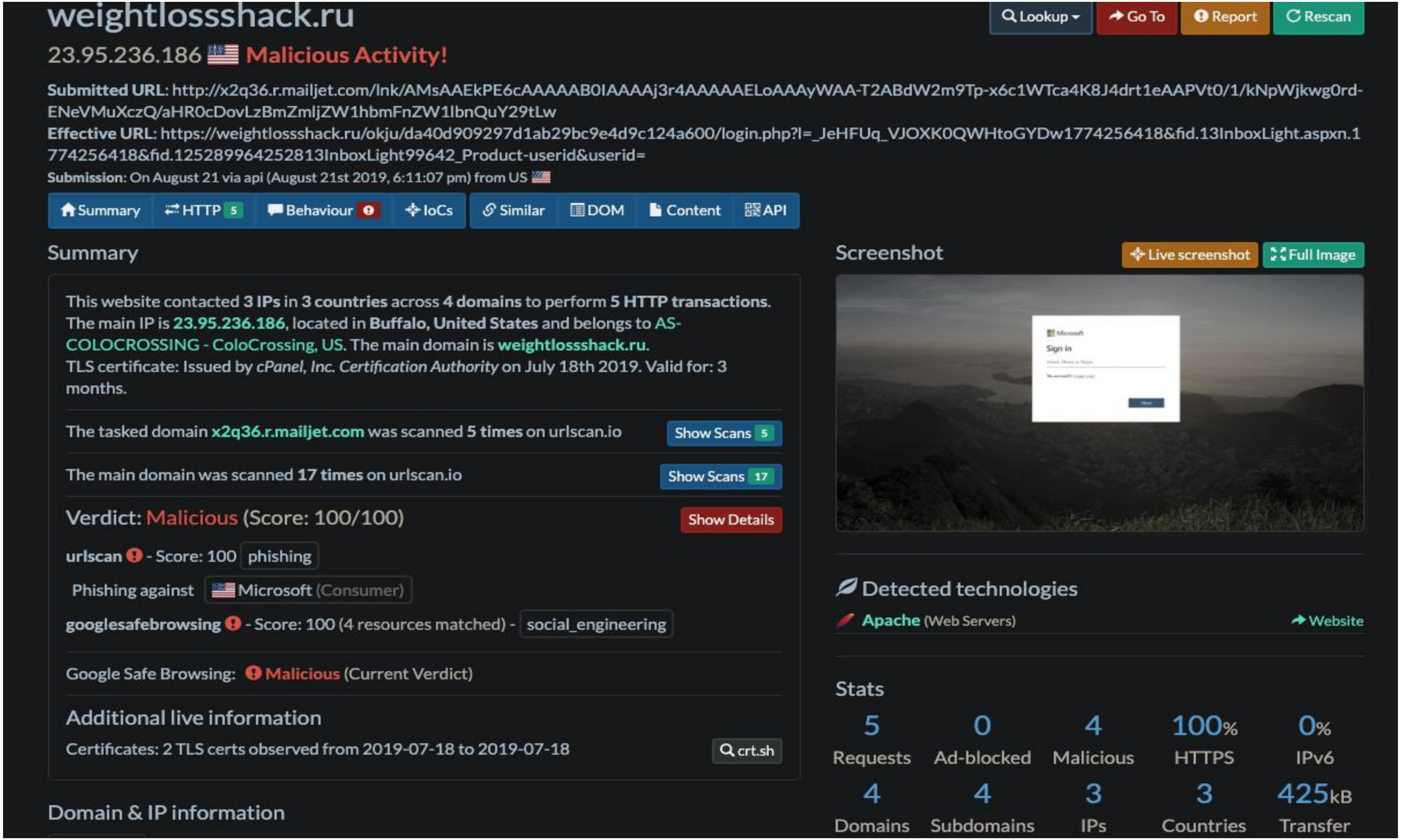
Examples of Threat Detection



Sign in

Email, Phone or Skype

No account? Create one!



weightlossshack.ru

23.95.236.186 Malicious Activity!

Submitted URL: http://x2q36.r.mailjet.com/lnk/AMsAAEkPE6cAAAAAB0IAAAAj3r4AAAAAELoAAAyWAA-T2ABdW2m9Tp-x6c1WTca4K8J4drt1eAAPVt0/1/kNpWjkwg0rd-ENeVMuXczQ/aHR0cDovLzBmZmljZW1hbmFnZW1lbnQuY29tLw

Effective URL: https://weightlossshack.ru/okju/da40d909297d1ab29bc9e4d9c124a600/login.php?l=_JeHFUq_VJOXK0QWHtoGYDw1774256418&fid.13InboxLight.aspxn.1774256418&fid.125289964252813InboxLight99642_Product-userid&userid=

Submission: On August 21 via api (August 21st 2019, 6:11:07 pm) from US

Summary

This website contacted **3 IPs** in **3 countries** across **4 domains** to perform **5 HTTP transactions**. The main IP is **23.95.236.186**, located in **Buffalo, United States** and belongs to AS-COLOCROSSING - ColoCrossing, US. The main domain is **weightlossshack.ru**.
TLS certificate: Issued by *cPanel, Inc. Certification Authority* on July 18th 2019. Valid for: 3 months.

The tasked domain **x2q36.r.mailjet.com** was scanned **5 times** on urlscan.io

The main domain was scanned **17 times** on urlscan.io

Verdict: Malicious (Score: 100/100)

urlscan - Score: 100 phishing

Phishing against Microsoft (Consumer)

googlesafebrowsing - Score: 100 (4 resources matched) - social_engineering

Google Safe Browsing: Malicious (Current Verdict)

Additional live information

Certificates: 2 TLS certs observed from 2019-07-18 to 2019-07-18

Domain & IP information

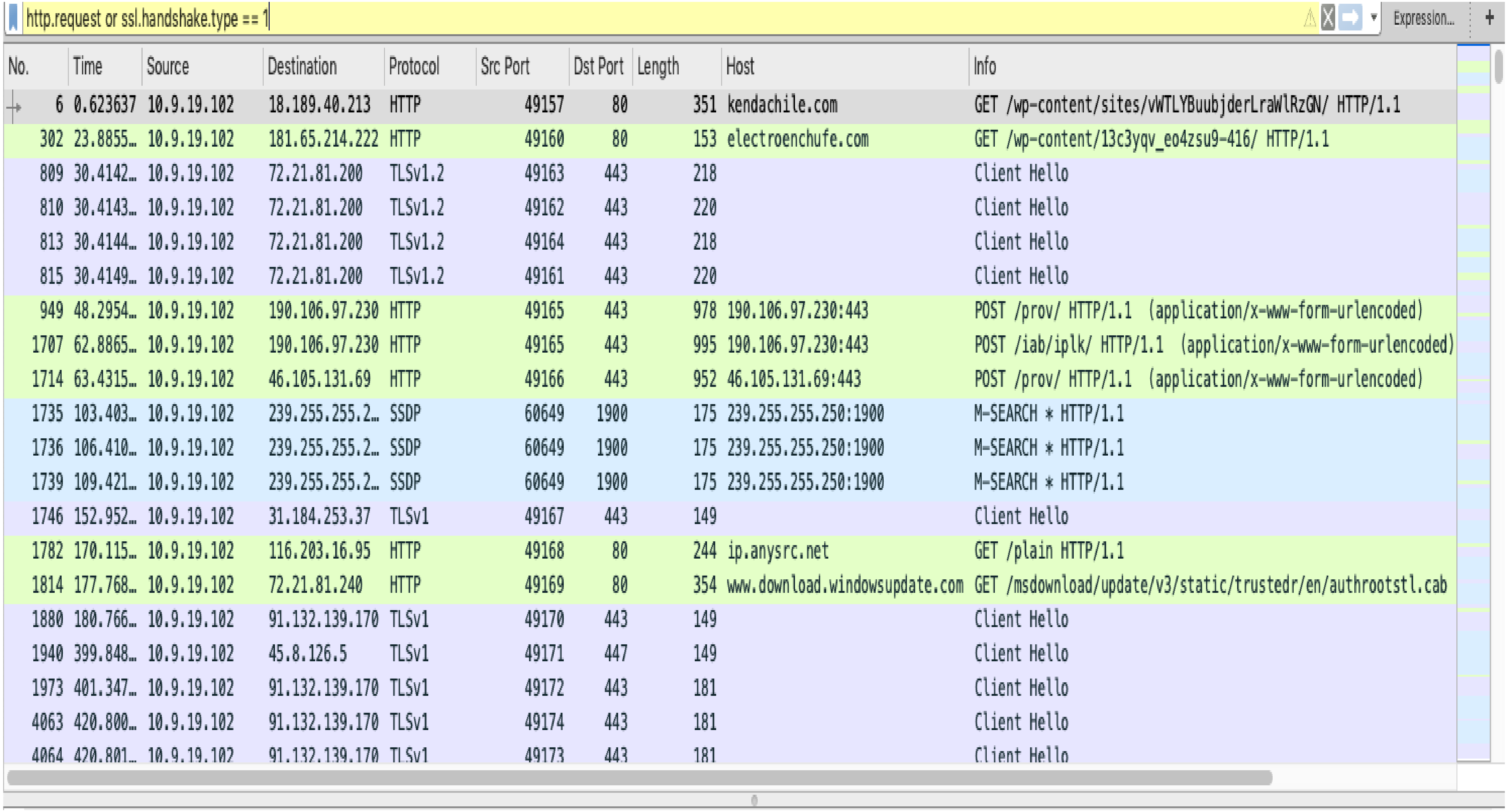
Screenshot

Detected technologies

Apache (Web Servers)

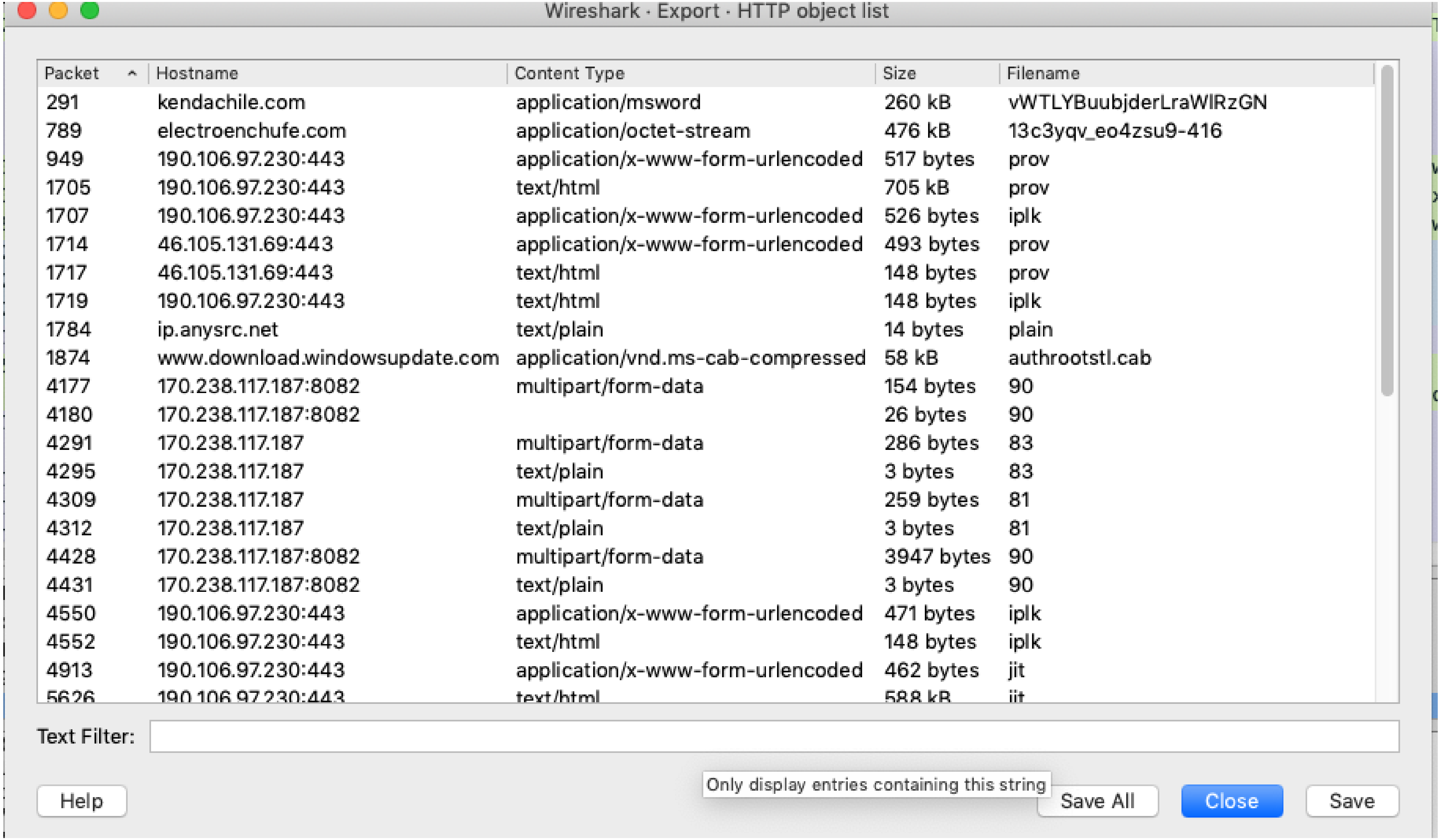
Stats

5	0	4	100%	0%
Requests	Ad-blocked	Malicious	HTTPS	IPv6
4	4	3	3	425kB
Domains	Subdomains	IPs	Countries	Transfer



http.request or ssl.handshake.type == 1

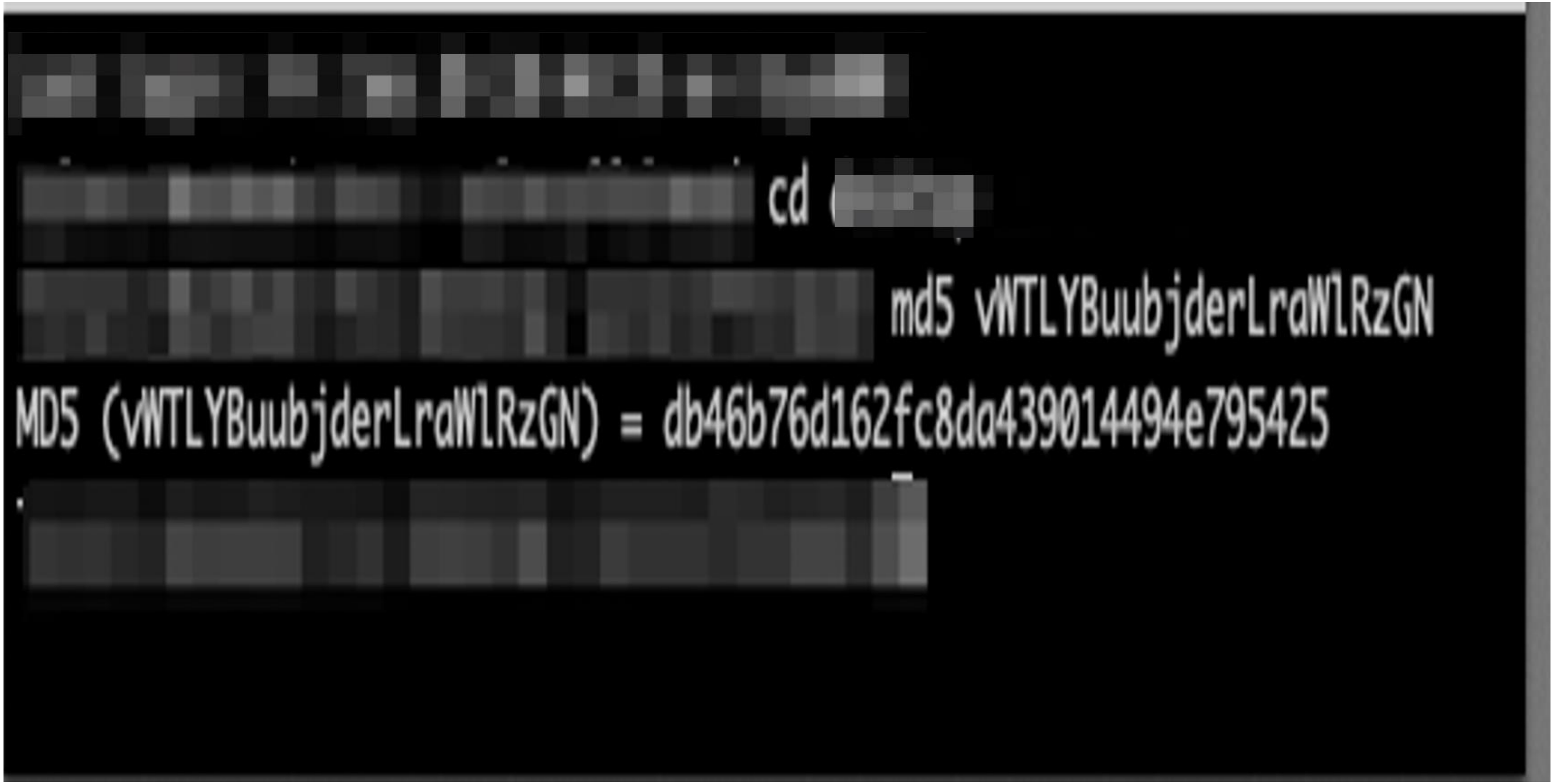
No.	Time	Source	Destination	Protocol	Src Port	Dst Port	Length	Host	Info
6	0.623637	10.9.19.102	18.189.40.213	HTTP	49157	80	351	kendachile.com	GET /wp-content/sites/vWTLYBuubjderLraWlRzGN/ HTTP/1.1
302	23.8855…	10.9.19.102	181.65.214.222	HTTP	49160	80	153	electroenchufe.com	GET /wp-content/13c3yqv_eo4zsu9-416/ HTTP/1.1
809	30.4142…	10.9.19.102	72.21.81.200	TLSv1.2	49163	443	218		Client Hello
810	30.4143…	10.9.19.102	72.21.81.200	TLSv1.2	49162	443	220		Client Hello
813	30.4144…	10.9.19.102	72.21.81.200	TLSv1.2	49164	443	218		Client Hello
815	30.4149…	10.9.19.102	72.21.81.200	TLSv1.2	49161	443	220		Client Hello
949	48.2954…	10.9.19.102	190.106.97.230	HTTP	49165	443	978	190.106.97.230:443	POST /prov/ HTTP/1.1 (application/x-www-form-urlencoded)
1707	62.8865…	10.9.19.102	190.106.97.230	HTTP	49165	443	995	190.106.97.230:443	POST /iab/iplk/ HTTP/1.1 (application/x-www-form-urlencoded)
1714	63.4315…	10.9.19.102	46.105.131.69	HTTP	49166	443	952	46.105.131.69:443	POST /prov/ HTTP/1.1 (application/x-www-form-urlencoded)
1735	103.403…	10.9.19.102	239.255.255.2…	SSDP	60649	1900	175	239.255.255.250:1900	M-SEARCH * HTTP/1.1
1736	106.410…	10.9.19.102	239.255.255.2…	SSDP	60649	1900	175	239.255.255.250:1900	M-SEARCH * HTTP/1.1
1739	109.421…	10.9.19.102	239.255.255.2…	SSDP	60649	1900	175	239.255.255.250:1900	M-SEARCH * HTTP/1.1
1746	152.952…	10.9.19.102	31.184.253.37	TLSv1	49167	443	149		Client Hello
1782	170.115…	10.9.19.102	116.203.16.95	HTTP	49168	80	244	ip.anysrc.net	GET /plain HTTP/1.1
1814	177.768…	10.9.19.102	72.21.81.240	HTTP	49169	80	354	www.download.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab
1880	180.766…	10.9.19.102	91.132.139.170	TLSv1	49170	443	149		Client Hello
1940	399.848…	10.9.19.102	45.8.126.5	TLSv1	49171	447	149		Client Hello
1973	401.347…	10.9.19.102	91.132.139.170	TLSv1	49172	443	181		Client Hello
4063	420.800…	10.9.19.102	91.132.139.170	TLSv1	49174	443	181		Client Hello
4064	420.801…	10.9.19.102	91.132.139.170	TLSv1	49173	443	181		Client Hello



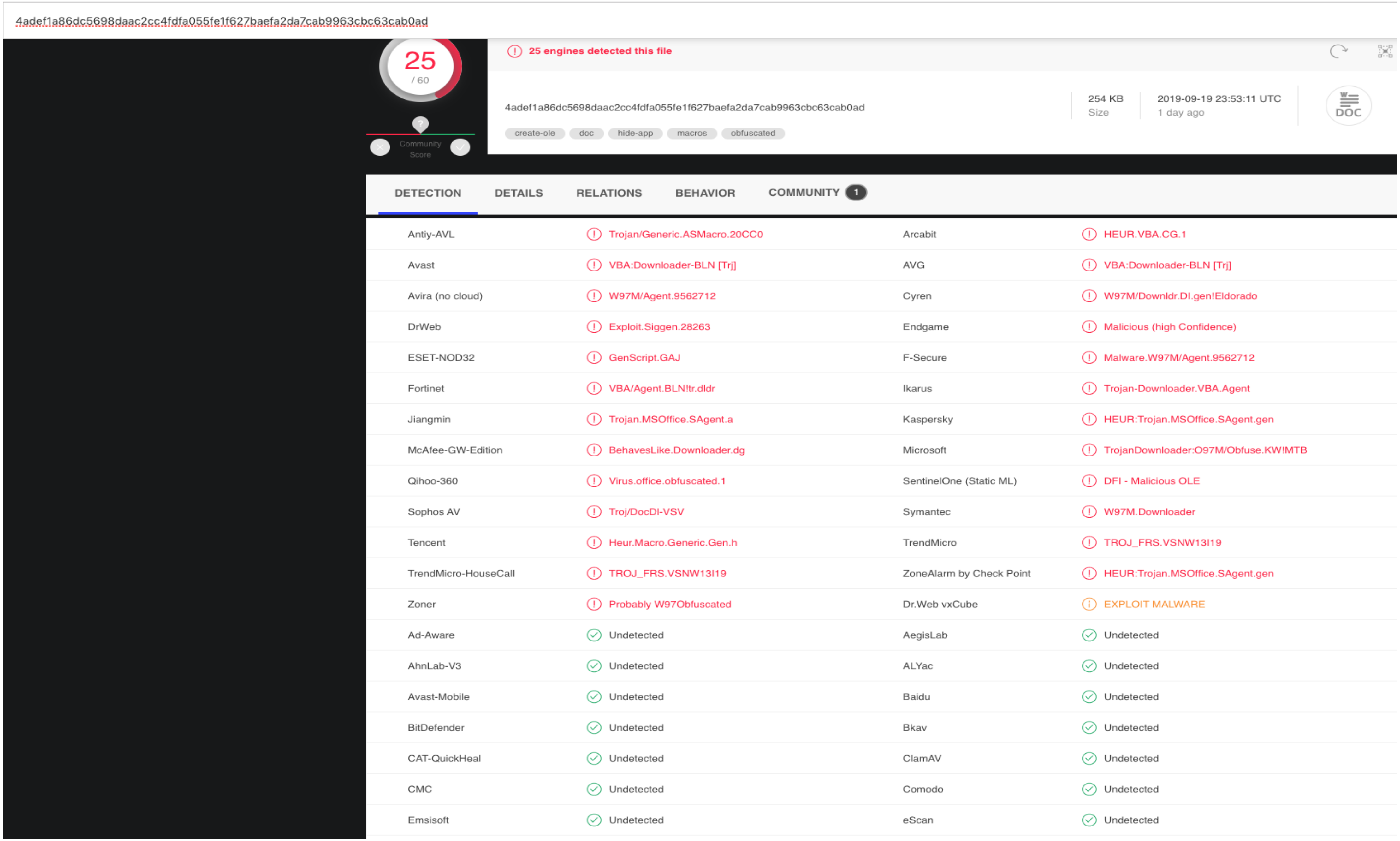
Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
291	kendachile.com	application/msword	260 kB	vWTLYBuubjderLraWIRzGN
789	electroenchufe.com	application/octet-stream	476 kB	13c3yqv_eo4zsu9-416
949	190.106.97.230:443	application/x-www-form-urlencoded	517 bytes	prov
1705	190.106.97.230:443	text/html	705 kB	prov
1707	190.106.97.230:443	application/x-www-form-urlencoded	526 bytes	iplk
1714	46.105.131.69:443	application/x-www-form-urlencoded	493 bytes	prov
1717	46.105.131.69:443	text/html	148 bytes	prov
1719	190.106.97.230:443	text/html	148 bytes	iplk
1784	ip.anysrc.net	text/plain	14 bytes	plain
1874	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	58 kB	authrootstl.cab
4177	170.238.117.187:8082	multipart/form-data	154 bytes	90
4180	170.238.117.187:8082		26 bytes	90
4291	170.238.117.187	multipart/form-data	286 bytes	83
4295	170.238.117.187	text/plain	3 bytes	83
4309	170.238.117.187	multipart/form-data	259 bytes	81
4312	170.238.117.187	text/plain	3 bytes	81
4428	170.238.117.187:8082	multipart/form-data	3947 bytes	90
4431	170.238.117.187:8082	text/plain	3 bytes	90
4550	190.106.97.230:443	application/x-www-form-urlencoded	471 bytes	iplk
4552	190.106.97.230:443	text/html	148 bytes	iplk
4913	190.106.97.230:443	application/x-www-form-urlencoded	462 bytes	jit
5626	190.106.97.230:443	text/html	588 kB	jit

Text Filter:



```
[redacted]
[redacted] cd [redacted]
[redacted] md5 vWTLYBuubjderLraWlRzGN
MD5 (vWTLYBuubjderLraWlRzGN) = db46b76d162fc8da439014494e795425
[redacted]
```



4adef1a86dc5698daac2cc4fdfa055fe1f627baefa2da7cab9963cbc63cab0ad

25
/ 60

25 engines detected this file

4adef1a86dc5698daac2cc4fdfa055fe1f627baefa2da7cab9963cbc63cab0ad

create-ole doc hide-app macros obfuscated

254 KB
Size

2019-09-19 23:53:11 UTC
1 day ago

Antiy-AVL	Trojan/Generic.ASMacro.20CC0	Arcabit	HEUR.VBA.CG.1
Avast	VBA:Downloader-BLN [Trj]	AVG	VBA:Downloader-BLN [Trj]
Avira (no cloud)	W97M/Agent.9562712	Cyren	W97M/Downldr.DI.gen!Eldorado
DrWeb	Exploit.Siggen.28263	Endgame	Malicious (high Confidence)
ESET-NOD32	GenScript.GAJ	F-Secure	Malware.W97M/Agent.9562712
Fortinet	VBA/Agent.BLN!tr.dldr	Ikarus	Trojan-Downloader.VBA.Agent
Jiangmin	Trojan.MSOffice.SAgent.a	Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
McAfee-GW-Edition	BehavesLike.Downloader.dg	Microsoft	TrojanDownloader:O97M/Obfuse.KW!MTB
Qihoo-360	Virus.office.obfuscated.1	SentinelOne (Static ML)	DFI - Malicious OLE
Sophos AV	Troj/DocDl-VSV	Symantec	W97M.Downloader
Tencent	Heur.Macro.Generic.Gen.h	TrendMicro	TROJ_FRS.VSNW13I19
TrendMicro-HouseCall	TROJ_FRS.VSNW13I19	ZoneAlarm by Check Point	HEUR:Trojan.MSOffice.SAgent.gen
Zoner	Probably W97Obfuscated	Dr.Web vxCube	EXPLOIT MALWARE
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Avast-Mobile	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	Bkav	✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Comodo	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected

Thank you for attending!

Thoughts, questions, concerns?

INFRAGARD

PARTNERSHIP FOR PROTECTION

Safe Schools/School Security

Evan Francen, CEO

SECURITYSTUDIO®

Safe Schools/School Security

IMPORTANT! First things first…

- The World Health Organization states that **over 800,000 people die every year due to suicide, and that suicide is the second leading cause of death in 15-29-year-olds**.
- **5 percent** of adults (18 or older) experience a mental illness in any one year
- In the United States, almost half of adults (**46.4 percent**) will experience a mental illness during their lifetime.
- In the United States, **only 41 percent** of the people who had a mental disorder in the past year received professional health care or other services.
- https://www.mentalhealthhackers.org/resources-and-links/

IN MEMORY OF
Robert
Andrew Wallenberg
"Robby"
Bragg

Safe Schools/School Security

A simple CTF challenge in Robby’s Memory.

qr fbir ygdblcg yafr erodkganc hbd oneqrde oe yb ygr zrcannanc bh ygr kbefbe.

oe qr kgoncrj pwonre qoayanc hbd yafr yb kbfr onj cby bhh ygae powr zwlr jby hbd o kbefak zwans bh on rmr,

qr kolcgy o cwafper bh ebfryganc jrrprd / fbdr fronanchlw ygon oneqrde; pldr zrolym: glfonaym.

qgawr eyaww kopyaioyrj onj rnygdowwrj zm ygae jaekbirdm,

qr zoes an bld lybpao, ydmanc yb fosr ygance hoad onj rtlow,

eb ah qr qrdr yb jrpody onj cry zoks bn zbodj bld oadpwonr onj yafr hanowwm kofr yb cry le,

qr qblwj goir frfbdare zwaeehlw rnblcg yb woey le lnyaw bld nrvy oddaiow onj cair ygrf yb

ygr hlyldr, hbd ydlwm mbl snbq grd, zly ah nby, a oeeldr mbl, egr oweb goe o zrolyahlw eblw.

-dbzzm onjdrq qowwrnzrdc zdocc mbld hwoc ae drfrfzrdancwbeygoksrde

UNSECURITY
Information security is failing. Breaches are epidemic. How can we fix this broken industry?

One way to get a free book.
Solve this and email me; efrancen@securitystudio.com.

Safe Schools/School Security

OK, down to business. This talk…

- Who's this guy?
- What's the mission?
- School Information Security
  - Before COVID-19 (shootings
  - During COVID-19
  - After COVID-19
- Opportunities

Safe Schools/School Security

Who's this guy?

Evan Francen, CEO & Founder of FRSecure and SecurityStudio

I do a lot of security stuff.

- Co-inventor of SecurityStudio® (or S^2), S^2Score, S^2Org, S^2Vendor, S^2Team, and S^2Me
- 25+ years of "practical" information security experience (started as a Cisco Engineer in the early 90s)
- Worked as CISO and vCISO for hundreds of companies.
- Developed the FRSecure Mentor Program
  - Six students in 2010
  - 500+ in 2019
  - 2,500+ this year.
- Advised legal counsel in very public breaches (Target, Blue Cross/Blue Shield, etc.)

Safe Schools/School Security

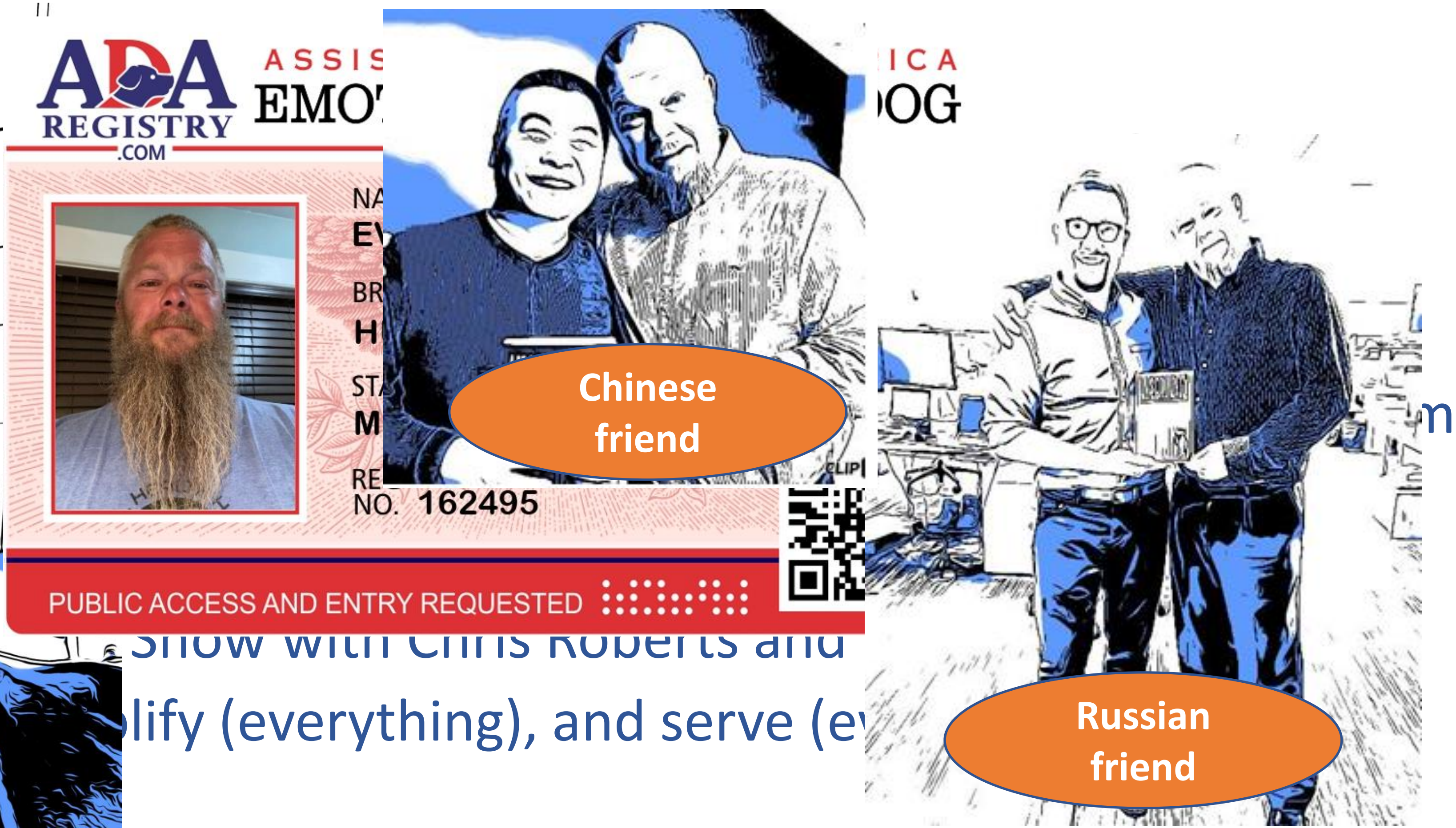
Who's this guy?

Evan Francen, CEO & Founder of FRSecure and SecurityStudio

- I'm counter-culture.
- Crazy mission; to fix the broken information security industry.
- Wrote a book; UNSECURITY: Information Security Is Failing. Breaches Are Epidemic. How Can We Fix This Broken Industry?
- Co-host of the UNSECURITY Podcast (episode 97 this week).
- Co-host of the Secuity Sh*t Show with Chris Roberts and Ryan Cloutier.
- Tell the truth (always), simplify (everything), and serve (everyone.).

#MissionBeforeMoney

Safe Schools/School Security


ADA REGISTRY .COM

ASSIS ... ICA

EMO ... OG

NA

EV

BR

H

STA

M

RE NO. 162495

PUBLIC ACCESS AND ENTRY REQUESTED

Chinese friend

Russian friend

mic.

Show with Chris Roberts and

lify (everything), and serve (ev

#MissionBeforeMoney

Safe Schools/School Security

What's the mission?

To fix the broken information security industry.

This starts with serving the underserved:

- State/local government
- Education – HigherEd and **K12**
- Small to mid-sized businesses
- People (personally)

Educators are overwhelmed right now.

People take shortcuts – So, we need to focus on fundamentals.

Start here.

We speak different languages – So, we need to translate.

People are confused – So, we need to simplify.

The money grabbers are active – So, we need to be inexpensive.

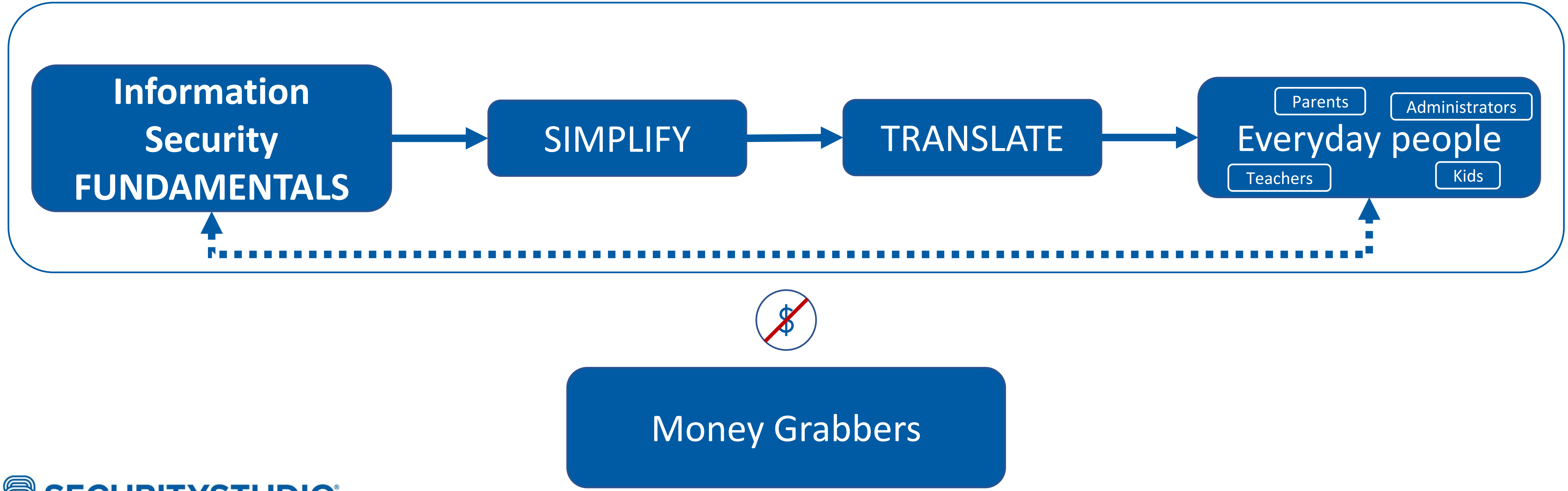
Complexity is the worst enemy.

SECURITYSTUDIO®

Safe Schools/School Security

What's the mission?

To fix the broken information security industry.



SECURITYSTUDIO®

Safe Schools/School Security

What's the mission?

We need to focus on fundamentals

Fundamental #1 - What is information security?

It's NOT an IT issue!

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

Cannot be separated from **privacy**.

Privacy is protection from unauthorized disclosure of PII.

Cannot be separated from **SAFETY**!

A lack of information security can be used to physically hurt you and others.

Safe Schools/School Security

What's the mission?

We need to focus on fundamentals

Fundamental #1 - What is information security?

It's NOT an IT issue!

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

Cannot b

thorized

Cannot b

can be

others.

Shortcutting fundamentals is ineffective and **DANGEROUS!**

SECURITYSTUDIO

Safe Schools/School Security

What's the mission?

We need to focus on fundamentals

What is information security?

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

Fundamental #2 – What is "managing risk"?

The likelihood of something bad happening, and the impact if it did.

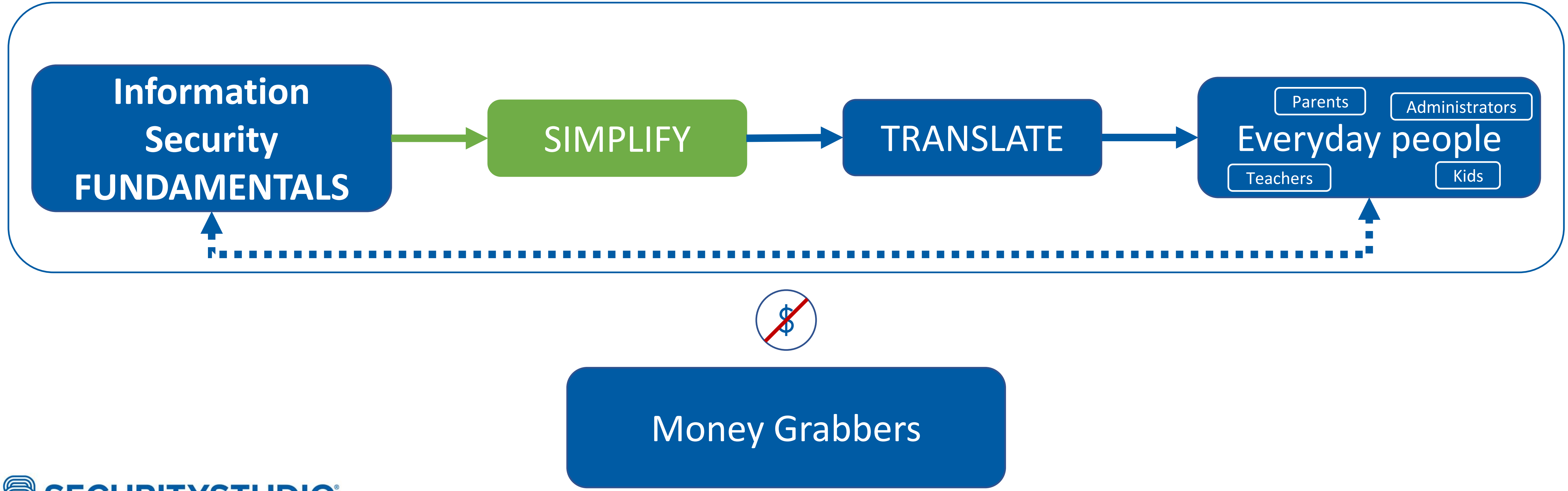
Derived from threats and vulnerabilities.

You CANNOT manage risk without assessing it first.

Safe Schools/School Security

What's the mission?

To fix the broken information security industry.



SECURITYSTUDIO®

Safe Schools/School Security

What's the mission?

A simple risk assessment that covers this

SIMPLIFY

We need to focus on fundamentals

What is information security?

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

And this

Fundamental #2 – What is "managing risk"?

The likelihood of something bad happening, and the impact if it did.

Derived from threats and vulnerabilities.

You CANNOT manage risk without assessing it first.

Safe Schools/School Security

What's the mission?

SIMPLIFY

We need to focus on fundamentals

A simple risk assessment that covers this

What is information security?

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

And this

Fundamental #2 – What is "managing risk"?

The likelihood of something bad happening, and the impact if it did.

Derived from threats and vulnerabilities.

Managing risk also means you must be able to make **risk decisions**.

Safe Schools/School Security

What’s the mission?

SIMPLIFY

We need to focus on fundamentals

What is information security?

A simple risk assessment that covers this

Information security is managing risk to unauthorized disclosure, alteration, and/or destruction of information using administrative, physical, and technical controls.

Fundamental #2 – What is “managing risk”?

And this

The likelihood of something bad happening, and the impact if it did.

Derived from threats and vulnerabilities.

And be able to measure results. Before starting the process again.

Safe Schools/School Security

What's the mission?

SIMPLIFY

Simplify the fundamentals.

A simple information security risk assessment that covers:

- Confidentiality, Integrity, and Availability. (opposite being disclosure, alteration, and destruction).
- Administrative, physical, and technical controls.

And enables:

- Risk decision making; accept, mitigate, transfer, or avoid.
- Measurement; you can't manage what you can't measure.

What makes a risk assessment simple?

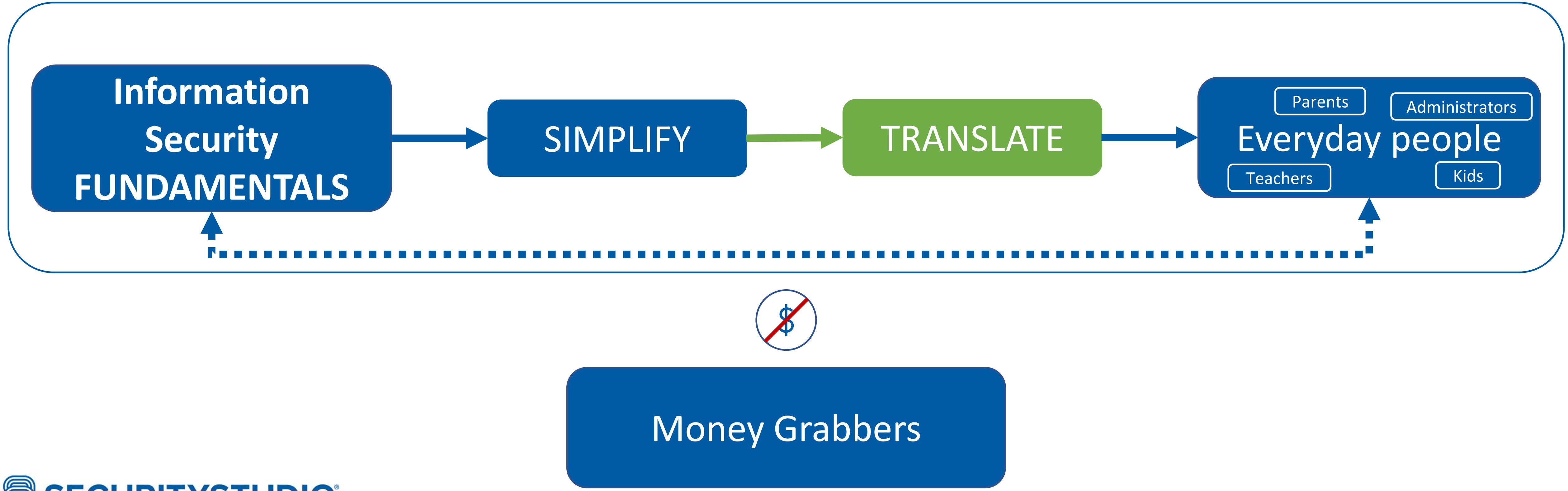
Language that's easy to understand

Objectivity

Safe Schools/School Security

What's the mission?

To fix the broken information security industry.



SECURITYSTUDIO®

Safe Schools/School Security

What’s the mission?

TRANSLATE

Translate the fundamentals

Information security people speak a different language. You knew this right?

Understand the audience for your information security risk assessment and the results.

Translation must be good enough for people to make sound risk decisions. By people, I mean those who are responsible for the decisions.

- At school it’s the school board and Superintendent.
- In business it’s the board of directors and CEO.
- In cities it’s the city council and Mayor.

How do they speak?
The assessment must translate into their language.

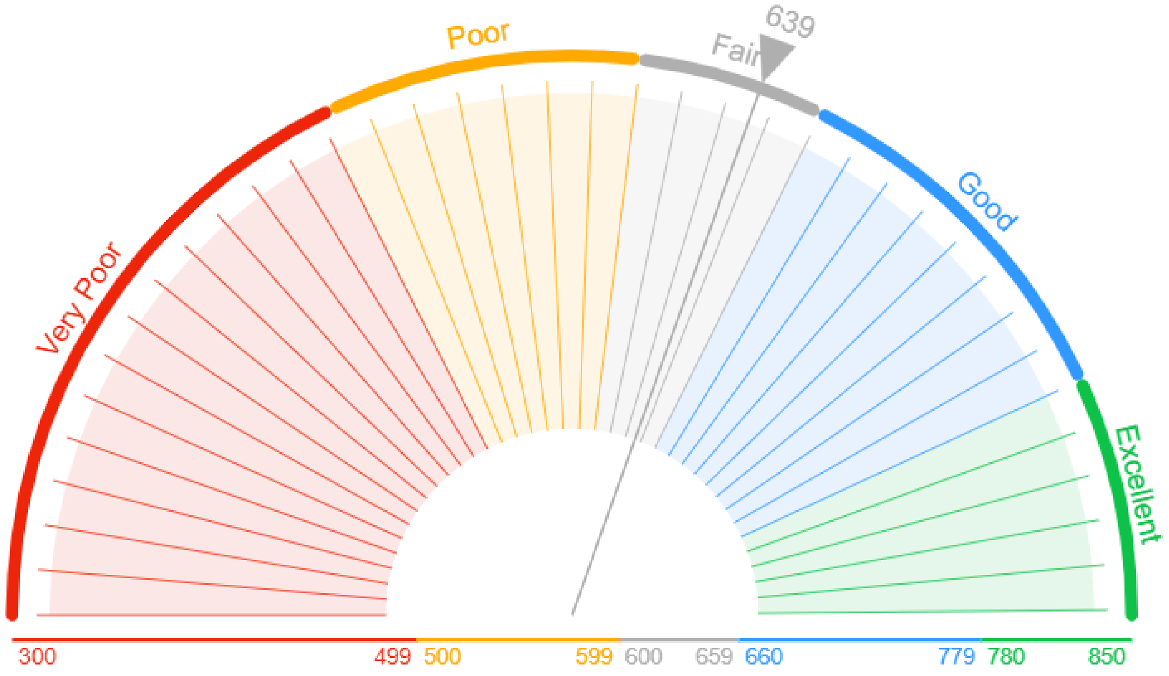
Safe Schools/School Security

What's the mission?

TRANSLATE

Translate the fundamentals

Why not use something they already understand?



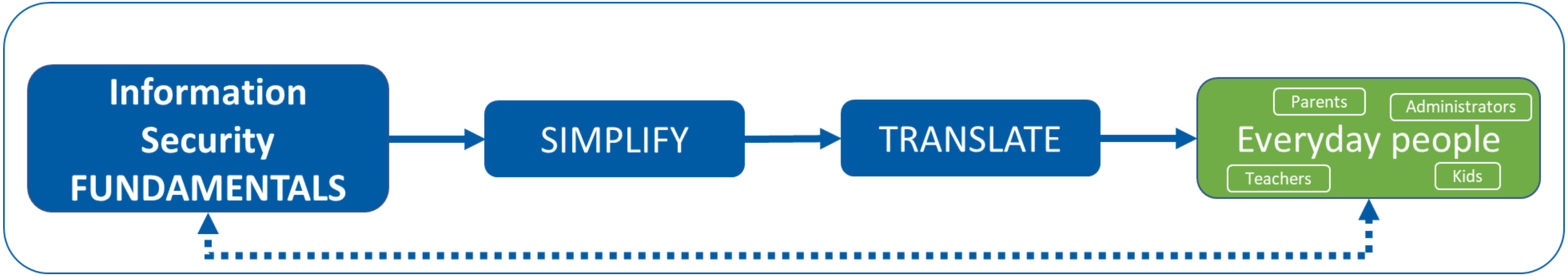
One thing information security people, school boards, Superintendents, boards of directors, CEOs, City Council members, and Mayors all understand (mostly) is the scale of 300 – 850.

SECURITYSTUDIO®

Safe Schools/School Security

What's the mission?

To fix the broken information security industry.



Money Grabbers

Safe Schools/School Security

What’s the mission?

Information security risk assessments that:

- Account for our full definition of information security.
- Are simple and easy to understand.
- Enable sound risk decision making.
- Is objective and measurable.
- Translates into other people’s languages.

Money Grabbers

Is inexpensive (or free); affordable for everyone, leaving more $$$ for fixing problems.

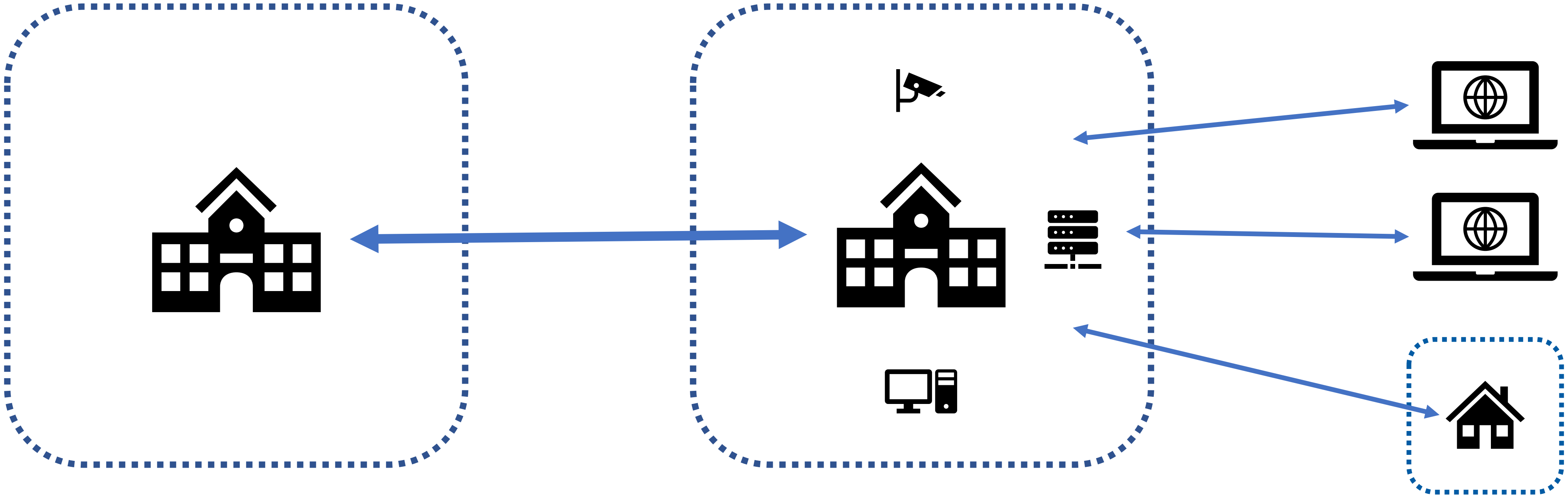
Safe Schools/School Security

School Information Security (Before COVID-19)

- Information security, or “cybersecurity” as they call it (they’re different things) was informally accounted for, if it was accounted for at all.
- Primary focuses for K-12 were:
  - Safety
  - Privacy
  - Keeping kids from hacking the school
- Schools were starting to wake up to the need and some were planning to do more.
- There was no single information security language (assessment/methodology/metric) spoken universally.
- Schools were targeted, but attacks were not widespread or publicly disclosed much. (even though attacks tripled in 2019).

Safe Schools/School Security

School Information Security (Before COVID-19)



Things were fairly simple though.

SECURITYSTUDIO®

Safe Schools/School Security

School Information Security (During COVID-19)

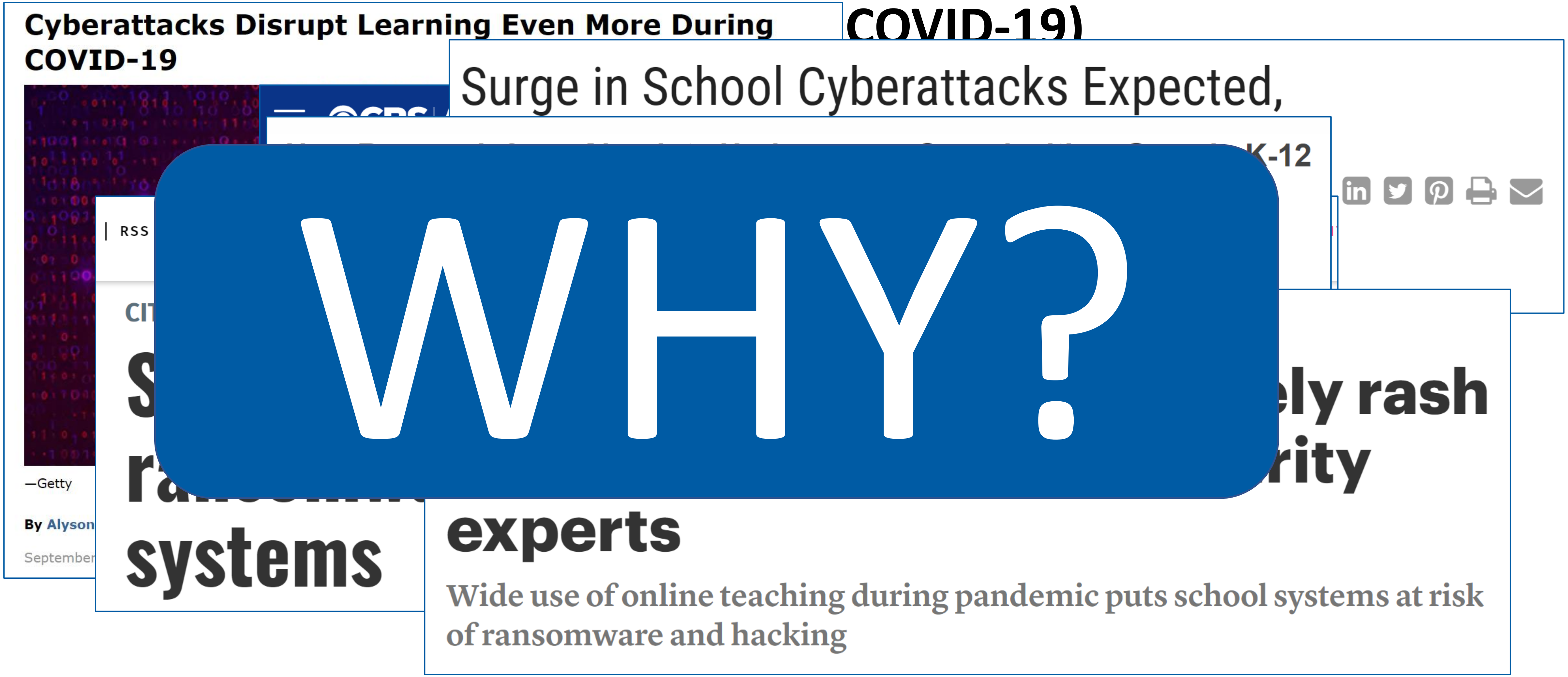
- Schools are distracted and “just trying to make things work”
- Most plans and strategies are on hold indefinitely.
- Primary focuses for K-12 are:
  - Getting kids connected to remote learning.
  - Finding and supporting remote technologies.
  - Communications and political correctness.
  - Supplying kids and homes with systems/technologies.
  - Keeping kids, teachers, and administrators socially distanced.
- Information security (or “cybersecurity”) is a concern still, but there are too many competing priorities and so many things have changed in a short period.
- There is still no single information security language (assessment/methodology/metric) spoken universally.
- Schools are more frequently targeted, attacks are widespread and are publicly disclosed.

Safe Schools/School Security

School Information Security (During COVID-19)

- In a word, information security in schools is chaos.

Safe Schools/School Security



Cyberattacks Disrupt Learning Even More During COVID-19

—Getty

By Alyson

September

COVID-19)

Surge in School Cyberattacks Expected,

K-12

RSS

CIT

S

ra

systems

ely rash

rity

experts

Wide use of online teaching during pandemic puts school systems at risk of ransomware and hacking

WHY?

SECURITYSTUDIO

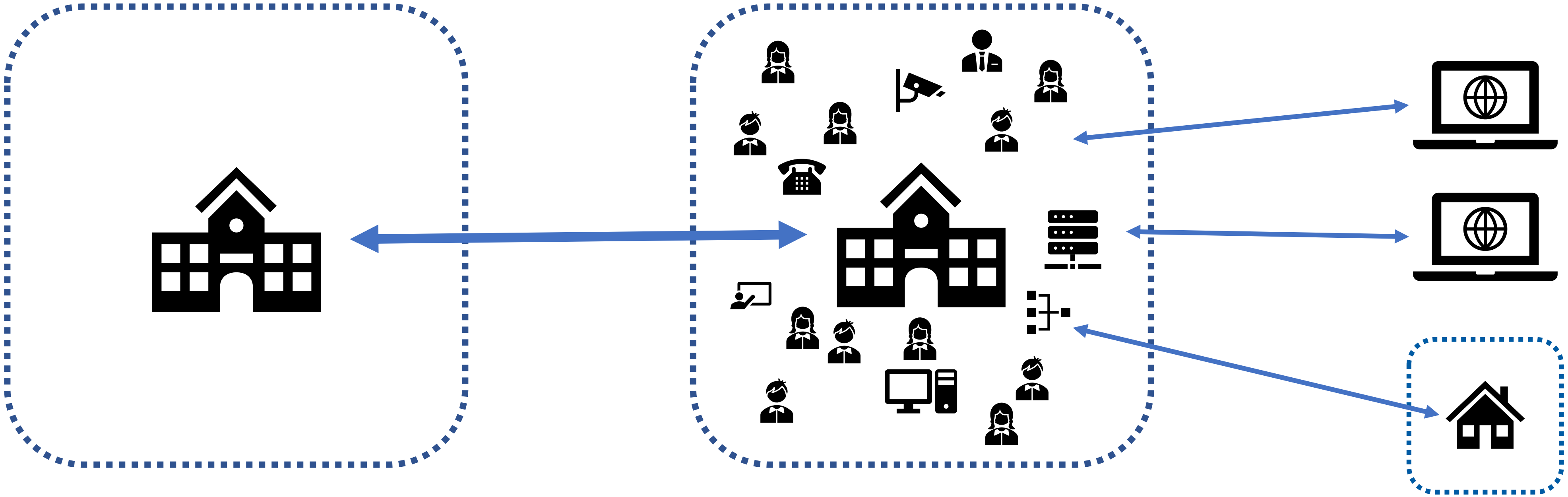
Safe Schools/School Security

School Information Security (During COVID-19)

- Schools were already soft targets, but they got softer.
- They were (and are) soft targets because they still lack the fundamentals.
- Instead of one network or a few networks to protect, there are potentially hundreds or thousands of networks to protect.
- Educators, parents, and kids have never been more distracted.
- Communications that used to be face-to-face are now virtual and remote.
- People are pushed into unfamiliar roles without preparation.

Safe Schools/School Security

School Information Security (Before COVID-19)

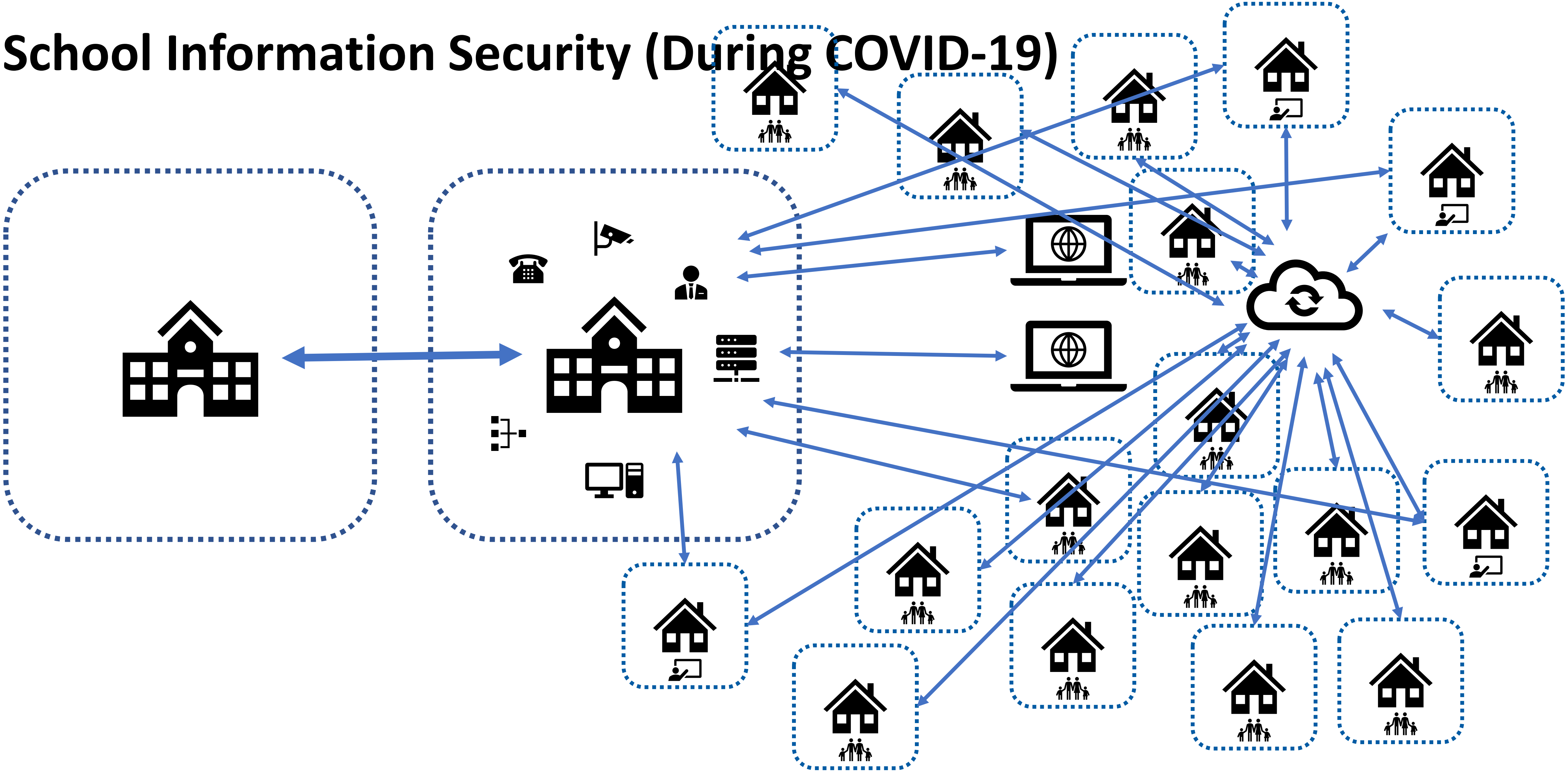


This, sort of went to…

SECURITYSTUDIO®

Safe Schools/School Security

School Information Security (During COVID-19)



Safe Schools/School Security

School Information Security (During COVID-19)

How do you solve the problem?

#1 – The fundamentals.

#2 – Roles and responsibilities.

#3 – Educate (differently).

#4 – Leverage your strengths.

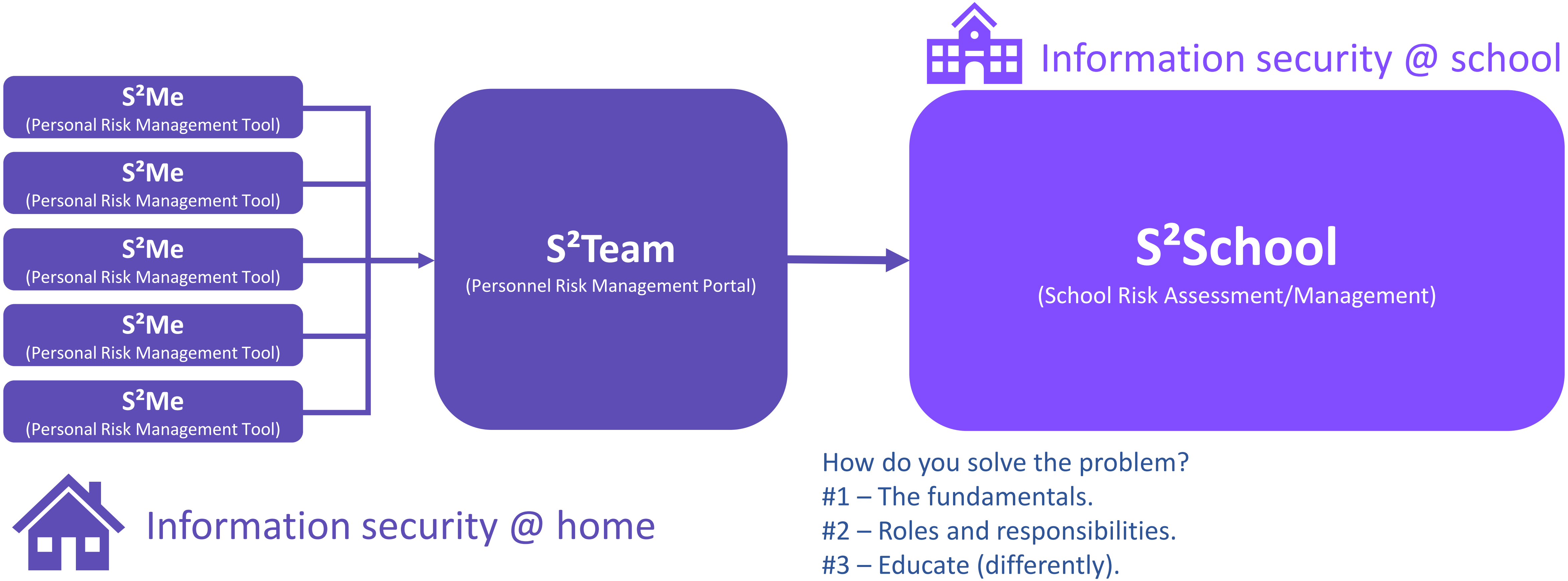
#5 – Measure stuff and keep improving.

I’ll show you what I mean.

Safe Schools/School Security

School Information Security (During COVID-19)

An example, NOT to sell you anything.
Build your own if you want.


Information security @ school
S²Me
(Personal Risk Management Tool)
S²Me
(Personal Risk Management Tool)
S²Me
(Personal Risk Management Tool)
S²Me
(Personal Risk Management Tool)
S²Me
(Personal Risk Management Tool)
S²Team
(Personnel Risk Management Portal)
S²School
(School Risk Assessment/Management)
Information security @ home

How do you solve the problem?
#1 – The fundamentals.
#2 – Roles and responsibilities.
#3 – Educate (differently).
#4 – Leverage your strengths.
#5 – Measure stuff and keep improving.

SECURITYSTUDIO®

Safe Schools/School Security

School Information Security (After COVID-19)

- Things will never be the same.
- Use this opportunity to reach out to the community and make a difference!

?

THANK YOU!

#MissionBeforeMoney

Safe Schools/School Security

ME: Evan Francen, CEO & Founder of FRSecure and SecurityStudio

Twitter:

- @evanfrancen
- @UnsecurityP
- @security_shit

UNSECURITY Podcast: https://frsecure.com/podcast/

Security Sh*t Show:

- Web/Blog - https://securityshitshow.com
- YouTube (LIVE Thursday nights) - https://www.youtube.com/c/SecurityShitShow

SecurityStudio: https://securitystudio.com

Top 5 Security Challenges Organizations Are Facing Today

Presented by: Kyle Johnson, CISSP

Director, Security Operations and Risk Management

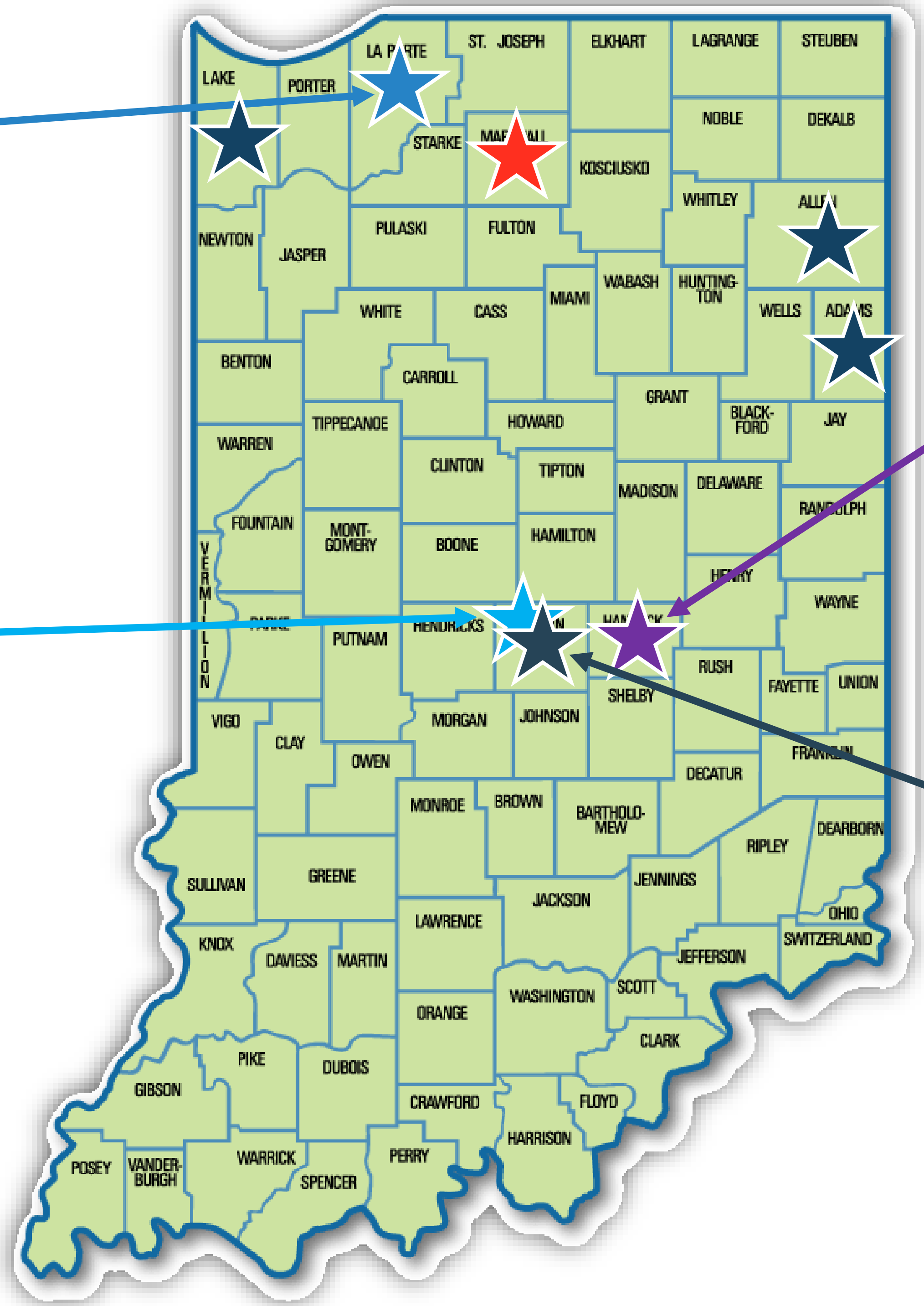
1. Employee Awareness Training

Importance of Training Employees

- Email-based cyber threats remain #1
  - 91% of cyber attacks
- Attacks can happen with just 1 click
- Average cost of an attack to an organization is over $2 million
- Employees are your first line of defense

LaPorte County: $130,000 paid to hackers due to ransomware attack

Pike Township: Hit with malware attack in June 2019



Hancock Health: $55,000 paid to hackers due to ransomware attack

Indiana Pacers: Phishing attack in 2018 let hackers access personal info

Solutions

Implement a formal security awareness program

- (at least) yearly training
- Ongoing phishing campaigns
- In-person training seminars

Provide employees with proper tools for reporting

- Make sure they know where to send suspected phishing emails

2. Asset Detection and Protection

Know What Is On Your Network

You can’t protect what you can’t see

Do you have a solution in place to alert you when a new device comes on the network?

Out-of-compliance alerts for registered devices?

Are there ongoing scans of the environment to identify assets and vulnerabilities?

Policies and procedures?

Vulnerability Management

Patch, patch, patch!

Have a monthly patching routine for the organization

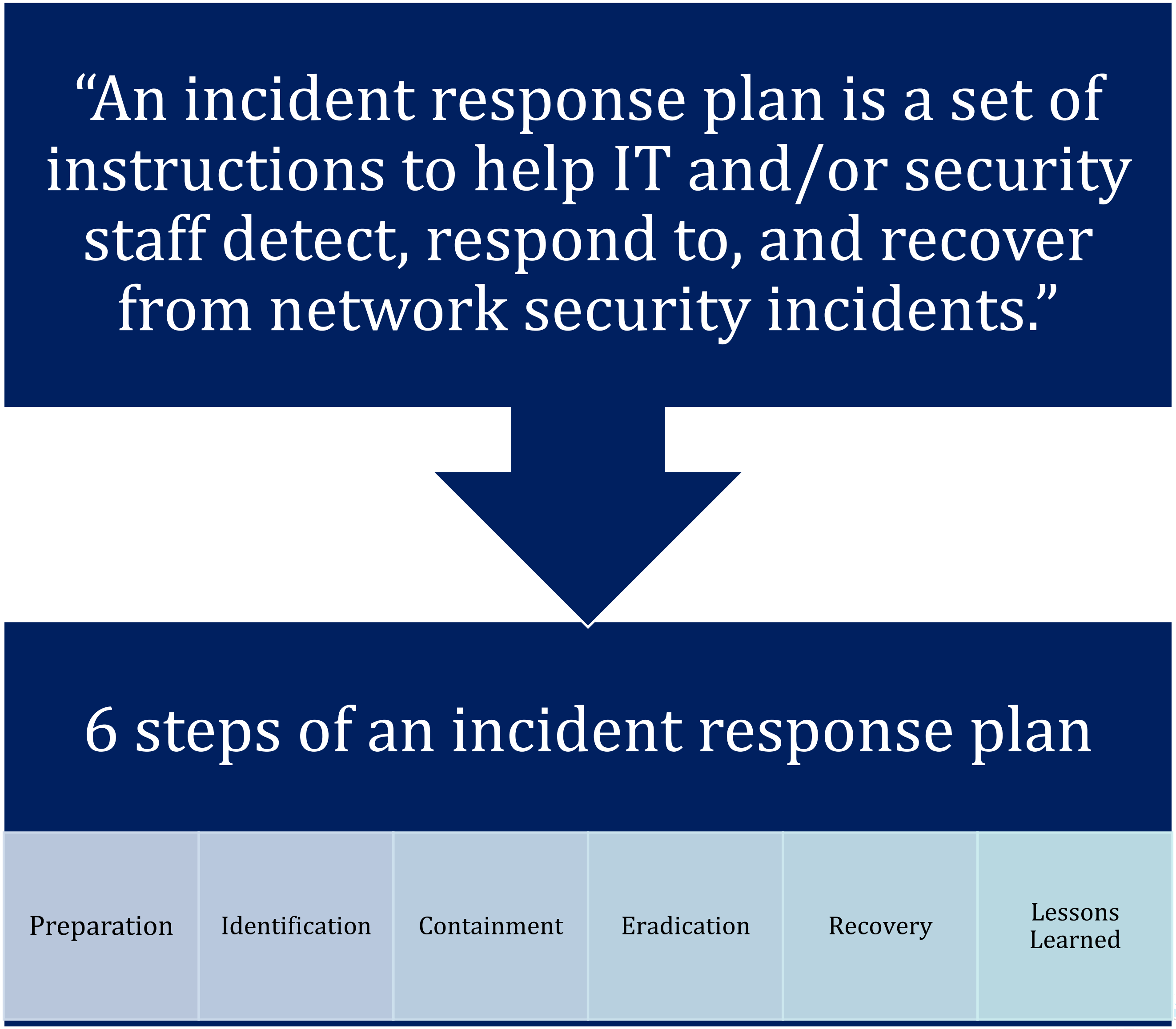
Have an out-of-band patching procedure (emergency patches)

Prioritize assets and vulnerabilities

Set a policy for when vulnerabilities need to be remediated

3. Incident Response Planning

Cyber Incident Response Plan



“An incident response plan is a set of instructions to help IT and/or security staff detect, respond to, and recover from network security incidents.”

6 steps of an incident response plan

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned

Preparation

- Is there sufficient documentation for the organization?
  - Policies and procedures
  - Network diagrams
  - Playbooks for responding to incidents
  - Identify stakeholders
- Are there adequate (and multiple) backups of your data?
  - How often?
  - Off-site?
  - Have you tested them?

Identification

- Do you know what to look for and alert on?
  - Define an incident vs. event
- Do you have a SIEM in place to monitor the environment?
  - If not, what else is in place to watch for anomalies?
- Is there 24/7 monitoring?
- Is staff trained on security to have the expertise to identify and remediate threats?

Containment

- Stop the threat
- Short term containment
  - Respond quickly to stop the spread and damage to systems
- Long term containment
  - Clean and restore machines back to full production

Eradication

- Process of restoring machines back to production
  - Reimage machines
  - Scan environment with an endpoint security agent
- Remove any malicious virus and improve defenses

Recovery

- Determine how to bring all systems back online
- How will you determine whether the machines are actually clean of any infection?

Lessons Learned

- Meet with stakeholders to identify the good, bad, and the ugly of the incident
- Review procedures, playbooks, and other documentation for effectiveness

4. Data Classification and Protection

Data Classification and Protection

- Do you know where all of your data, **especially sensitive data,** is located?
- Create an organizational policy for how data will be handled
  - Types of data, classification levels, where it can be stored, etc.
- Restrict access to removable media
  - Can be done thru group policy and/or DLP solutions
- Limit and monitor access to cloud storage solutions
  - Personal Dropbox, personal email, etc.

Data Protection: Access Control

Review users' access in the entire environment

Do users have too much access for their role?

Take the time to get granular when granting access

Are there shared accounts in the environment?

5. Compliance Challenges

Compliance Challenges

- Checkbox security is not security!
    - Example: SIEM solution is in place but not alerting
- Many compliance regulations are extremely vague
- Cost associated with implementing many of the security requirements can be too much for an organization

- Conduct regular risk and controls assessments to identify gaps and prioritize remediation steps in a clear and concise roadmap

Qumulus™ solutions

Kyle Johnson, CISSP
kjohnson@qumulussolutions.com
260-343-1606

Qumulus Solutions provides organizations with access to the people, expertise, and technology needed to assist them with developing and reviewing their information security programs.