



HSI

Homeland Security
Investigations
Cyber Crimes Center (C3)

Network Intrusion Investigations

Cybercrime Supply Chain:
What Happens to Your Data?

Special Agent Matthew J. Swenson
matthew.j.swenson@ice.dhs.gov

Who We Are

HSI is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel, and finance move.



37,547
criminals arrested
in FY 2019



Our Mission

HSI investigates, disrupts, and dismantles terrorist, transnational, and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States.



103
average criminal
arrests per day
in FY 2019



Combating Transnational Crime

By targeting transnational threats, both at home and abroad, HSI protects:



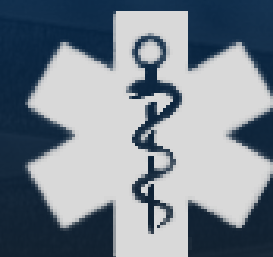
Border
Security



Homeland
Security



Public
Safety



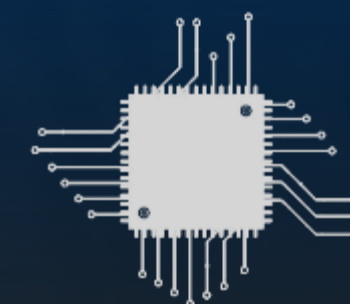
Public
Health



Global
Trade



U.S.
Economy



U.S.
Technology



Global Footprint

HSI consists of more than 9,800 employees who are assigned to offices in over 210 cities throughout the U.S. and 78 international offices in 52 countries across the world.

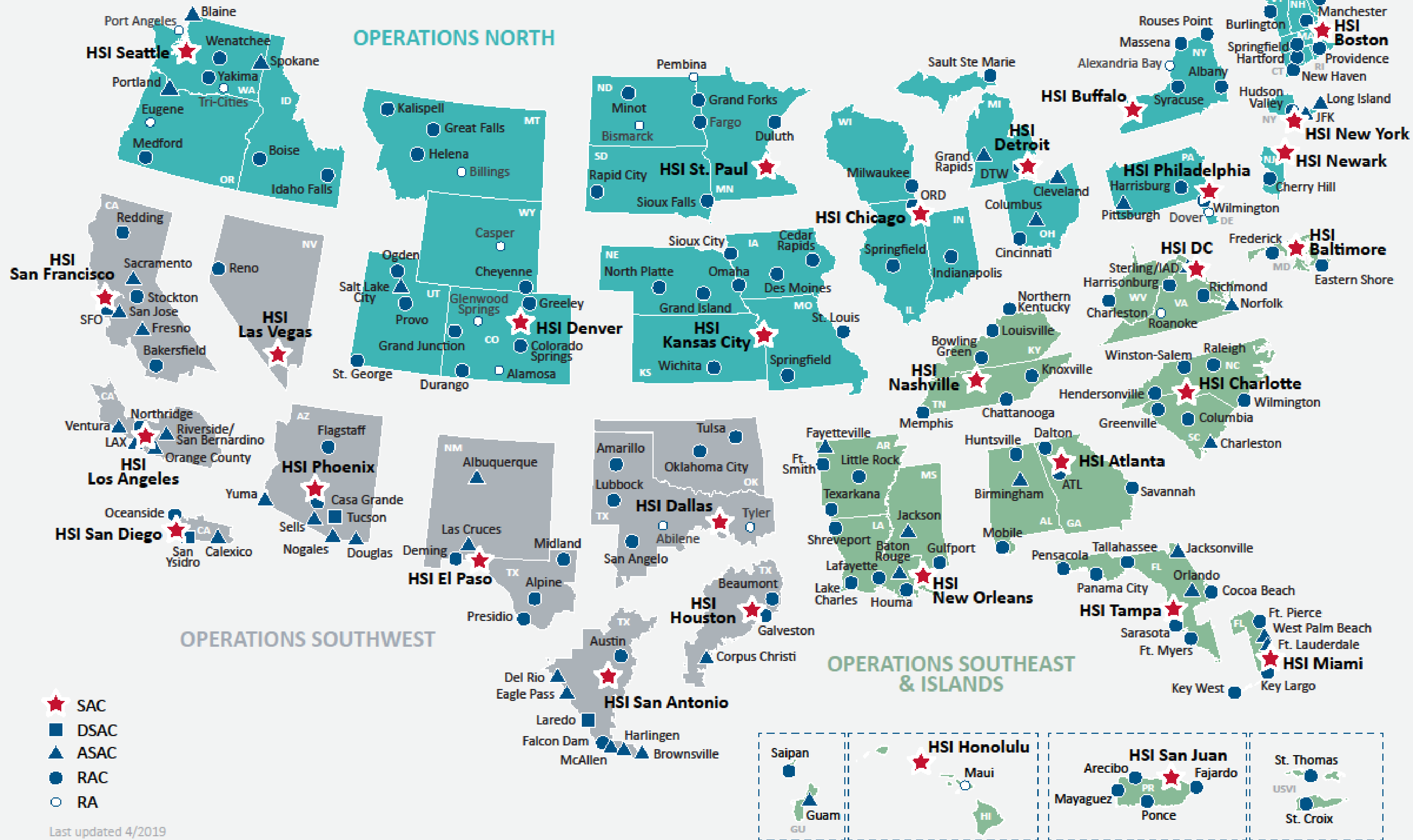


6,790+
special agents
included among
9,800 HSI employees



Homeland Security Investigations Operational Areas of Responsibility

Domestic Footprint



30
SAC offices
and multiple
sub-offices in
over 210 cities



Homeland Security Investigations International Operational Areas of Responsibility

- ★ Attaché (GS-15)
- ★ with TCIU
- ★ with VSP
- ★ with TCIU & VSP
- ◆ Assistant Attaché (GS-14)
- ◆ with TCIU
- ◆ with VSP
- ◆ with TCIU & VSP
- △ ERO Only



International Footprint



78
offices in
52 countries

Cyber Crimes Unit

Transnational criminal organizations commonly use cyber technology to facilitate their criminal activity. HSI is a worldwide law enforcement agency at the forefront of darknet and other cyber-related criminal investigations. HSI investigators infiltrate illicit darknet activity, targeting criminal organizations and protecting the public and our critical infrastructure.



Digital
Crimes



Network
Intrusion

Network Intrusion Investigations

The digital exfiltration of intellectual property and export controlled technical data is occurring at an alarming rate — CCU responds to and investigates incidents of cyber intrusion where the intrusion occurred in furtherance of a violation investigated by HSI.



You only have 3 days to submit the payment, or your files will be lost.
Time Left

The Cost of a Hack

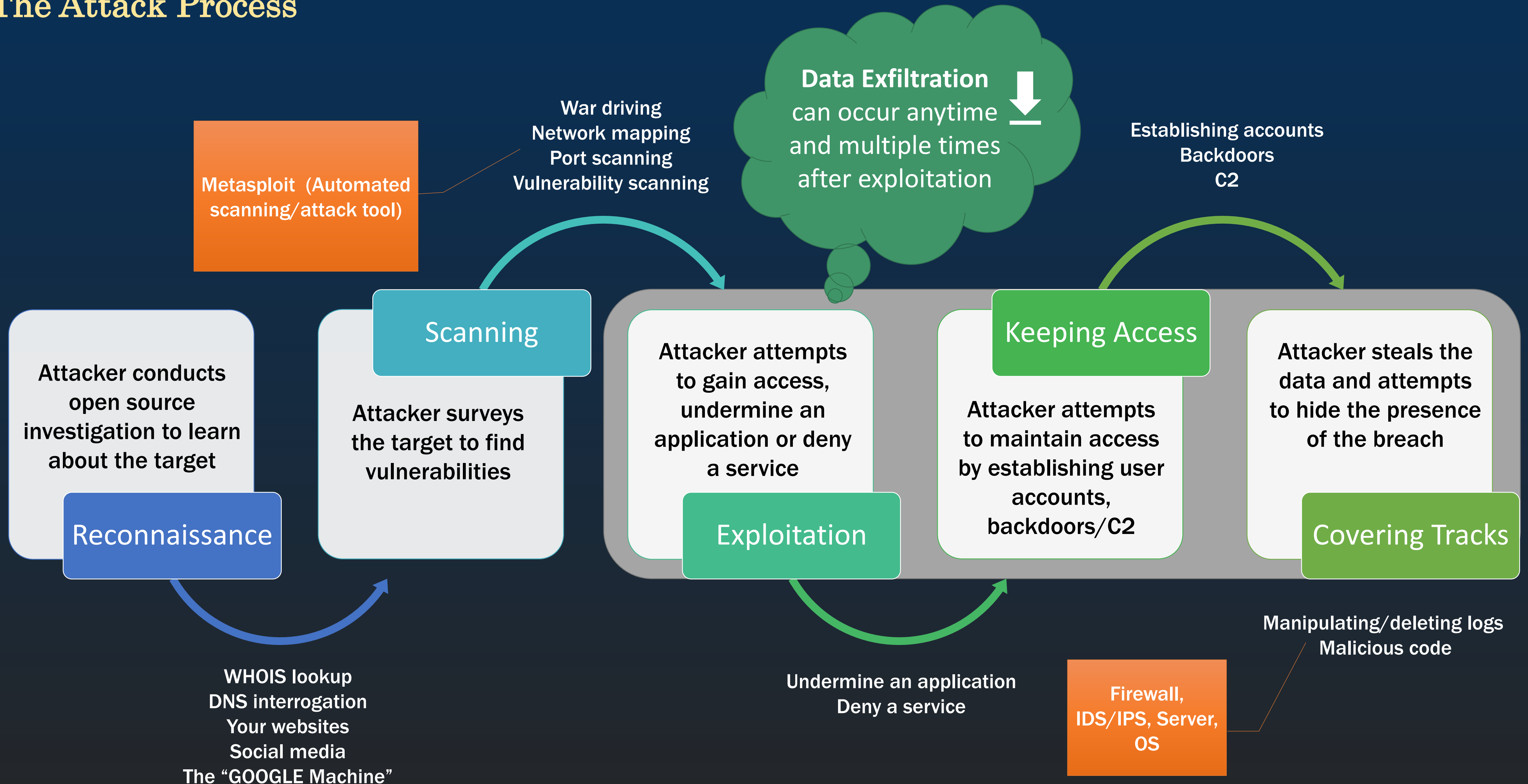
Fun facts or not so fun?

- Every 39 seconds there is a hacker attack
- Selfie timing
- Costs of data breaches \$2.1 trillion by 2019
- Cyber criminals earn \$600 billion a year in 2018
 - You are valuable
 - Business data is valuable
 - Credit cards and IDs

Your whole company could be crippled by one breach

The Cyber Threat

The Attack Process



Results of an Attack

Incident

- A security event that compromises the integrity, confidentiality, or availability of an information asset

Breach

- An incident that results in the confirmed disclosure — not just potential exposure — of data to an unauthorized party

In 2020, the Verizon incident response team reported over **157,525** incidents and **3,950** confirmed data breaches.

Breach Timelines

Time to Compromise

- Measured in seconds rather than minutes

Time to Breach

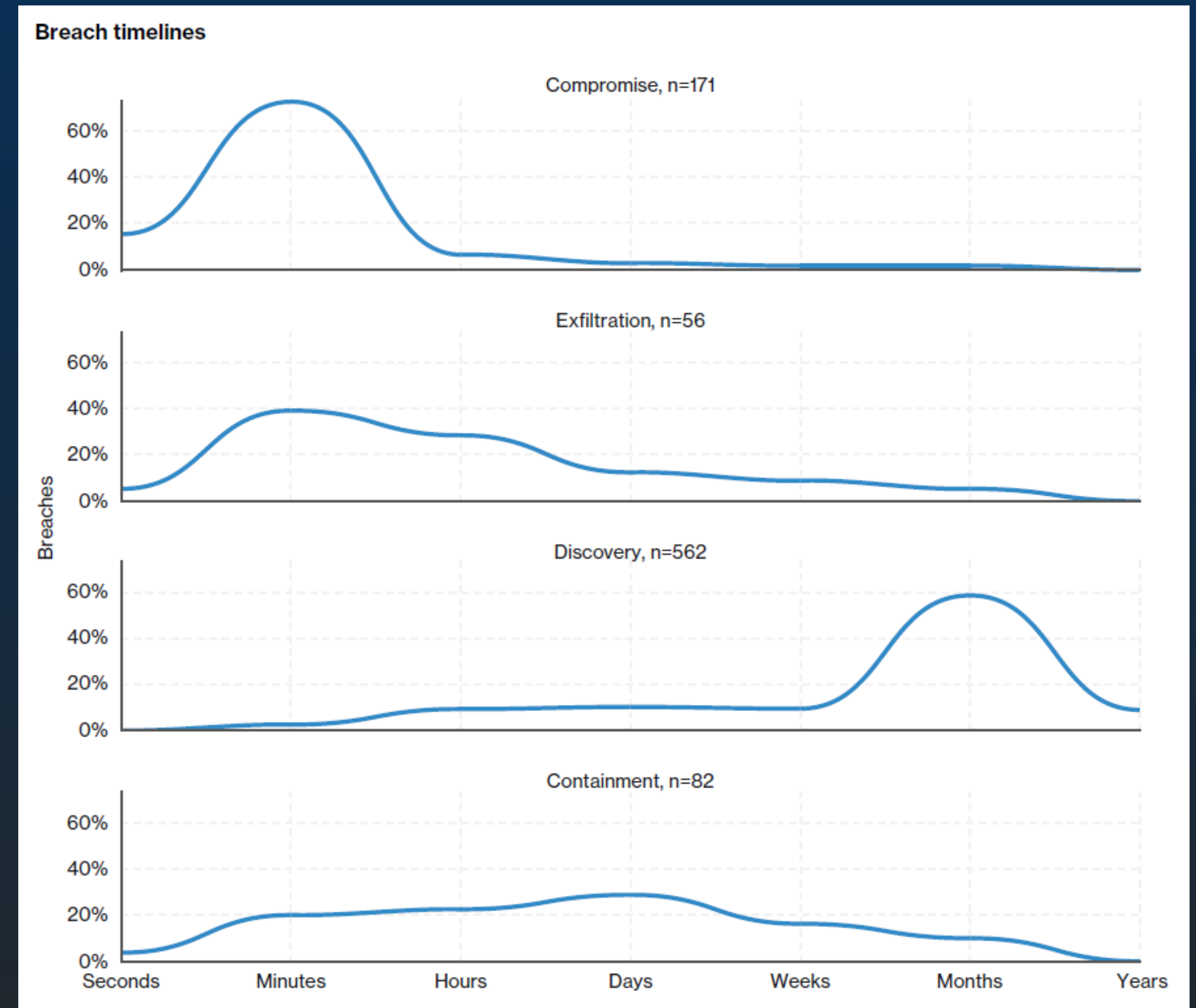
- Historically measured in weeks, months, or even years



The question is not “if” you will be attacked, but rather WHEN.



Will you know if you have been compromised? Prevention is ideal, but detection is a MUST.



Breaches – Attack Findings

Who's Behind the Breaches?

Perpetrator(s)	%
External Actors	70%
Organized Criminal Groups	55%
Internal Actors	30%
Had 4 or more attacker actions	4%
Partners	1%
Multiple Parties	1%

Who are the Victims?

Industry Breached	%
Contained in days or less	81%
Involved large business victims	72%
Personal data was compromised	58%
Involved small business victims	28%

What Tactics are Utilized?

Type of Breach Tactic	%
Hacking	45%
Social Attacks	22%
Malware	17%
Errors were Causal Events	22%
Privilege Misuse	8%
Physical Actions	4%

Other Commonalities

Type	%
Financially motivated	86%
Web applications were involved	43%
Utilized stolen or used credentials	37%
Malware incidents were ransomware	27%
Involved phishing	22%

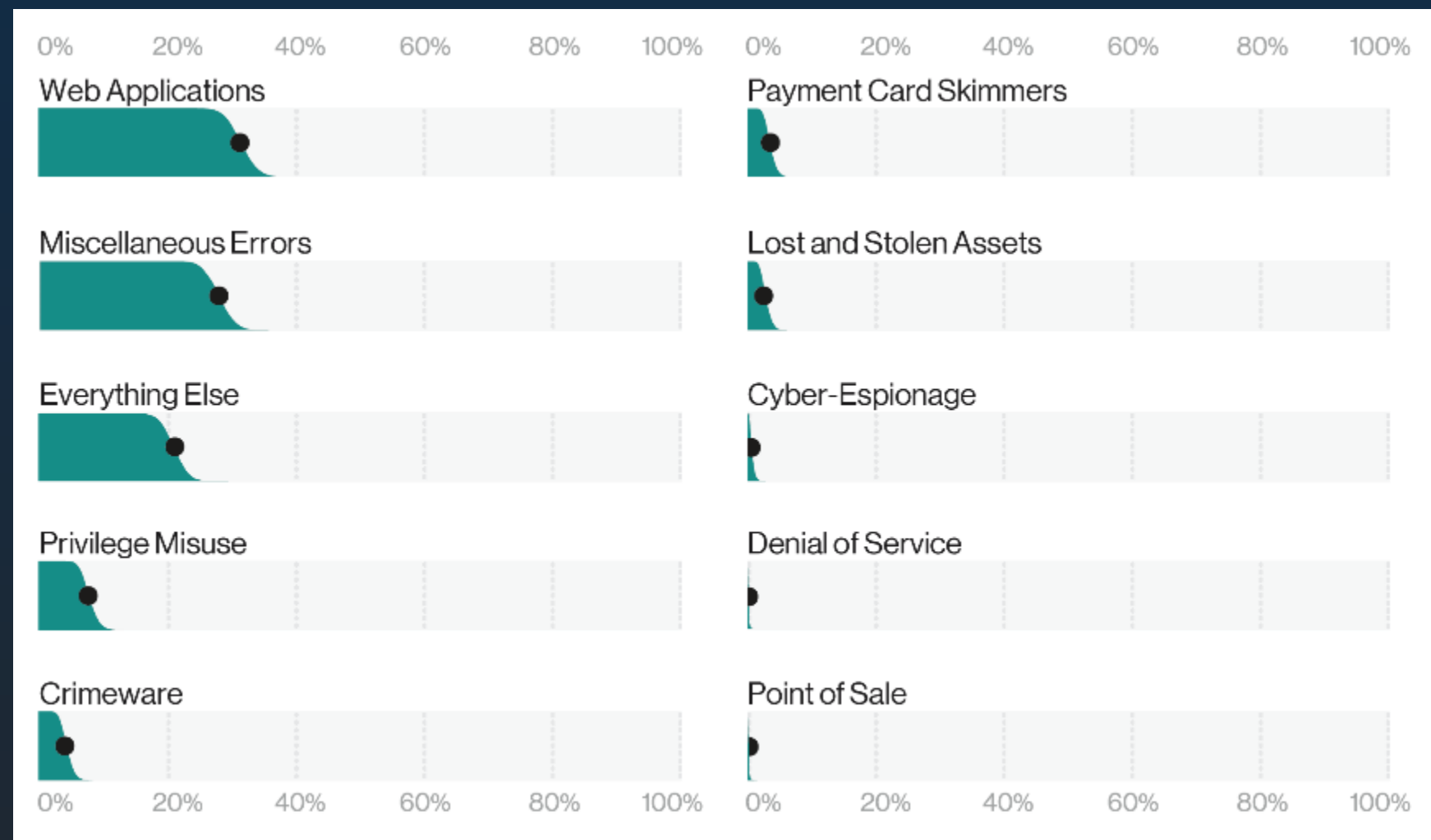
* Data is based on 2020 Data Breach Investigations Report. Data breaches may be associated with multiple attacks, actors, and/or actions.

Patterns within Financial, Insurance, and Retail Industries

Traditionally Point of Sale (PoS) was the dominant concern for data breaches. Today there is a **rising trend of exploiting web applications** as institutions, retailers, and individuals increase their reliance on saving valuable data to the cloud, such as email accounts and business-related processes.

The majority of attacks are perpetrated by **financially motivated external actors**.

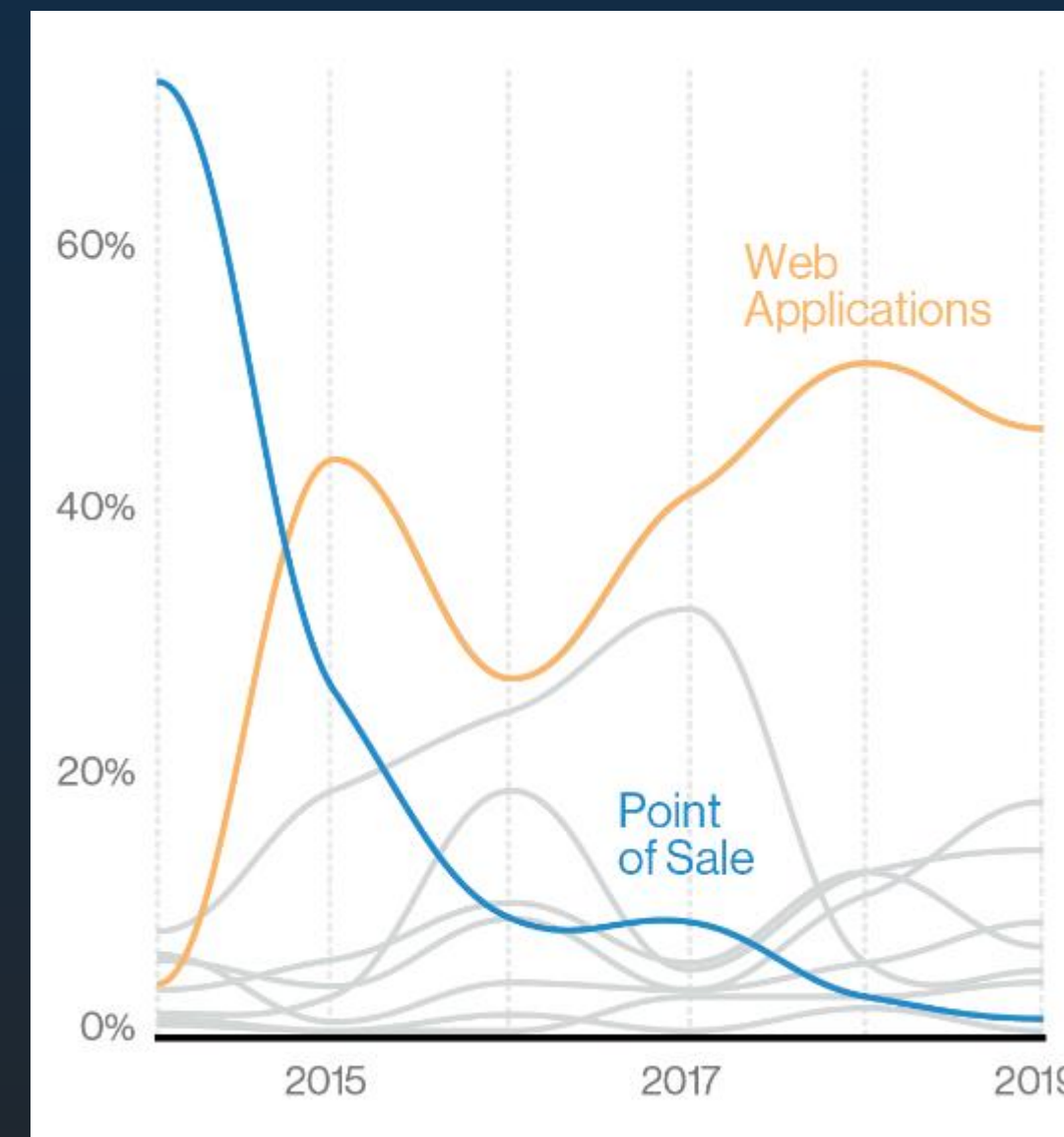
Patterns in Financial and Insurance Industry Breaches



Types of Data Compromised	%
Personal	77%
Credentials	35%
Other	35%
Bank	32%

In 2020, the Verizon incident response team reported **448 breaches in the financial and insurance industries**.

Patterns in Retail Industry Breaches



In 2020, the Verizon incident response team reported **148 breaches in the retail industry**.

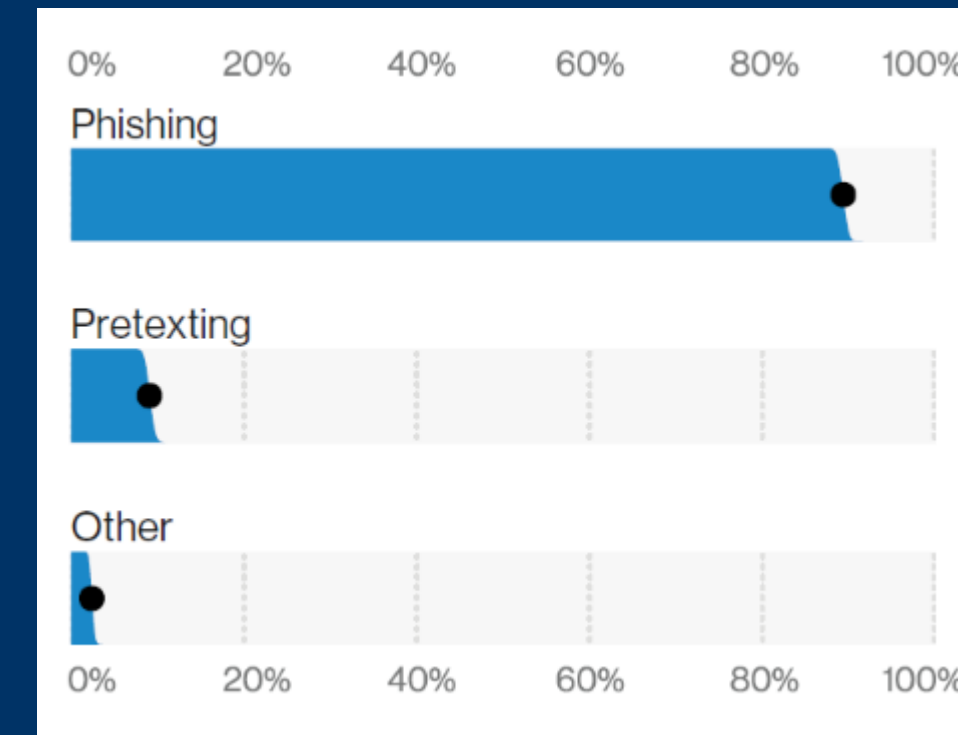
Types of Data Compromised	%
Personal	49%
Payment	47%
Credentials	27%
Other	25%

* Data is based on 2020 Data Breach Investigations Report. Data breaches may be associated with multiple types of compromised data.

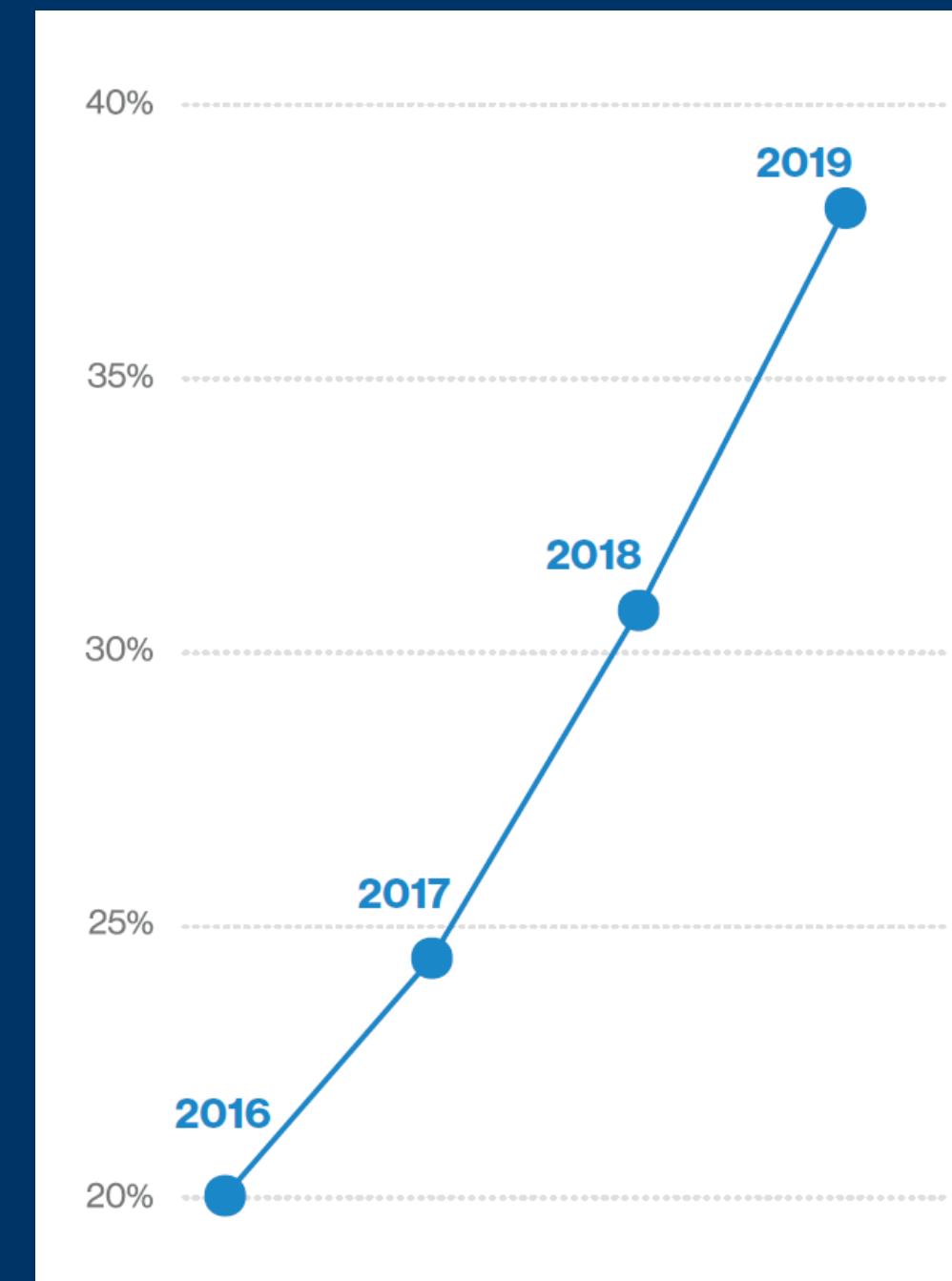
Most Prolific Social Attacks

Phishing and pretexting continue to be the most common social attack vector. Email continues to be the most common vector (96%).

- Phishing is often used as the lead action of an attack and is followed by malware installation and other actions that ultimately lead to exfiltration of data.
- The good news is that social and security awareness training appears to be effective as click rates are low and reporting rates are rising.



Top Social Varieties in Incidents



How Many Phishing Test Campaigns Were Reported at Least Once

Defending Against Social Attacks

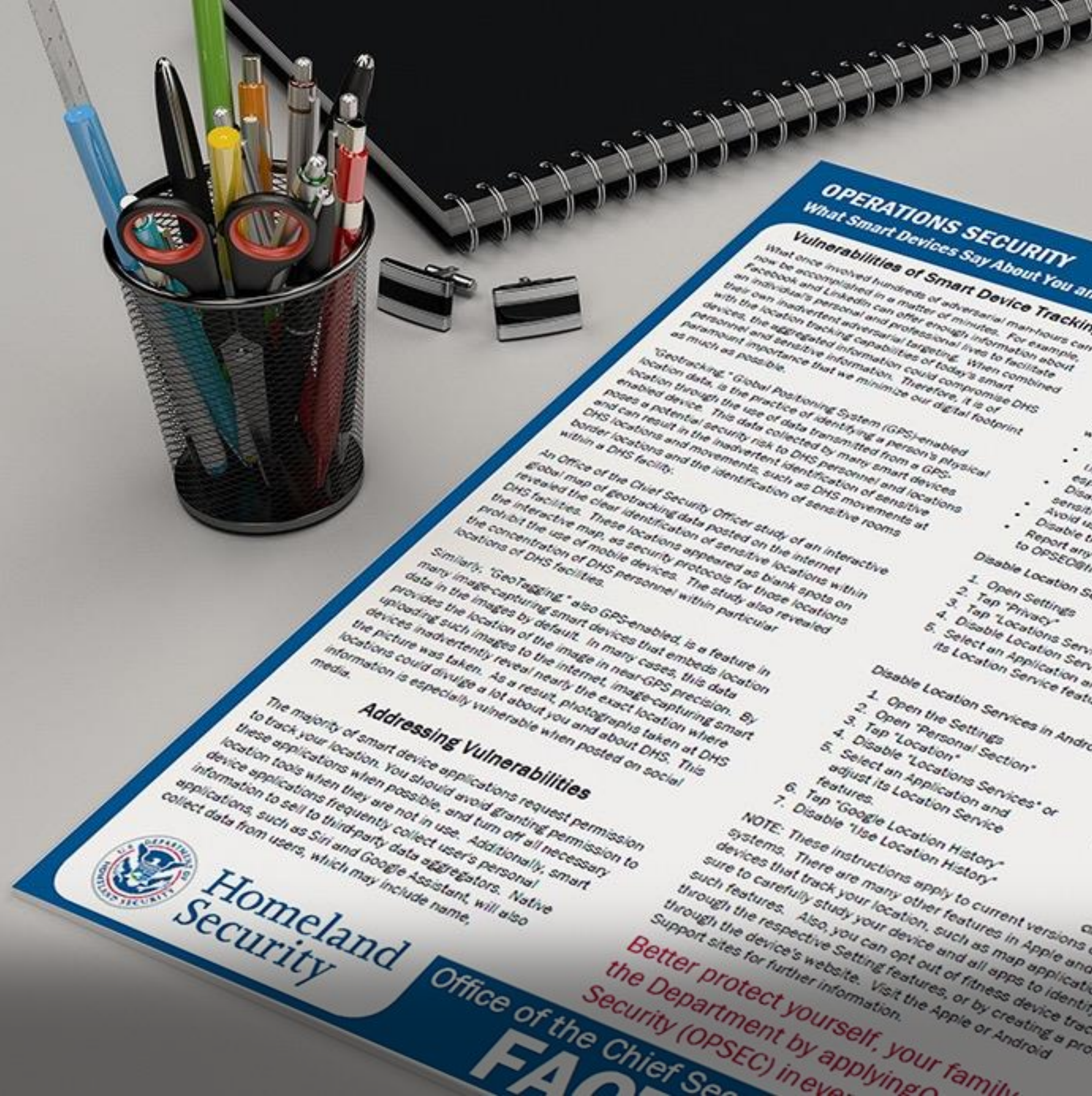
How effective is your employee awareness campaign?

- We have tried posters, online training, cyber awareness coffee mugs, in person seminars, pen testing...

The awareness solution:

- 78% of people don't click a single phish all year
- 4% of people (on average) in any given phishing campaign will click
- Perhaps try and find those 4% of people ahead of time and plan for them to click

Awareness by itself is not the solution



Ransomware

Ransomware is a type of malicious software or malware that encrypts data making it unusable. The cyber criminal holds the data hostage until the ransom is paid.

Most common infection vectors:

- Email phishing campaigns
 - Containing malicious file or link
- Remote Desktop Protocol (RDP)
 - RDP is a network protocol that allows individuals to control resources and data over the internet.
 - Cyber criminals use methods to obtain credentials, once accessed can deploy malware to systems
- Software Vulnerabilities



What Happens Post Data Exfiltration?

Once a threat actor obtains data and scans the data for important/valuable information, they will either utilize this data for their own personal gain or sell it to a 3rd party.


Credit cards and payment details are the most sought-after marketplace goods on the deep and dark web.

- 3rd parties, or “brokers”, will buy the card details from a marketplace and resell them to a “carder”.
- Carders will spend as much funds as possible before the respective owner and/or bank discovers the compromise.
- Oftentimes carders will buy online gift cards and then use these to purchase electronics, which can be quickly resold due to high demand.

Ships to: Digital / Service

[Vendor Info](#) [wfowfo's Listings](#) [Contact Vendor](#) [Show Listing](#)

9



Vendor: [carder007](#) [Escrow Listing](#)

Category: [Cards and CVV](#)

Title: [SNIFFED GERMANY CVV/CC 100% LIVE](#)

€ 33.12 £ 30.04
AUD 54.34
CAD 52.07

[In stock](#)

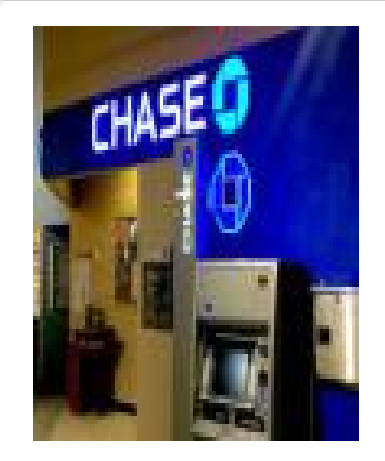
USD 39

Ships from: Digital / Service

Ships to: Digital / Service

[Vendor Info](#) [carder007's Listings](#) [Contact Vendor](#) [Show Listing](#)

10



Vendor: [cashboy](#) [Escrow Listing](#)

Category: [Cards and CVV](#)

Title: [CHASE DEBITCARD WITH PIN KNOWN BALANCE AND SSN 1K\\$ TO 15K\\$](#)

€ 297.31 £ 269.59
AUD 487.68
CAD 467.31

[In stock](#)


USD 350

Ships from: Digital / Service

Ships to: Digital / Service

[Vendor Info](#) [cashboy's Listings](#) [Contact Vendor](#) [Show Listing](#)

11



Vendor: [sataii](#) [Escrow Listing](#)

Category: [Cards and CVV](#)

Title: [30 NON VBV VISA DEBIT CLASSIC BIN LIST 2020](#)

€ 76.45 £ 69.32
AUD 125.40
CAD 120.16

[In stock](#)

USD 39

Ships from: Digital / Service

Ships to: Digital / Service

[Vendor Info](#) [sataii's Listings](#) [Contact Vendor](#) [Show Listing](#)

The Cyber Criminal Underworld

1

Steal

Threat actors steal credit card and identity data utilizing botnets, malware, Trojans, phishing, keylogging, et cetera.



2

Sell

Threat actors sell the credit card and identity data through fraud rings on the deep and dark web.



3

Commit Fraud

Fraud rings use the personal information for fraud on e-commerce and banking sites.

Examples include: account takeovers, money transfer, card not present transactions.



4

Convert to Cash

Fraud rings use e-commerce, classified ads, and drop zones to convert physical goods into cash.



Best Practices for Securing Your Data

Organizations can minimize their risk of cyber attacks by:

- Updating and patching systems
- Conducting continuous vulnerability scans and monitor accounts
- Backing up data and configurations; create system images; and save these offline
- Utilizing network monitoring, proxies, and multi-factor authentication
- Enabling email and web browser protections
- Implementing a security awareness and training program
- Reviewing and exercising incident response plans



What to Do When Breached

When a breach occurs best practice is to:

- Isolate the infected computer immediately
- Isolate or power-off affected devices that have not yet been completely corrupted
- Immediately secure backup data or systems by taking them offline
- Contact law enforcement immediately



HSI Intrusion Response

HSI Special Agents receive technical certified training and have the legal authority to respond to a cyber intrusion. Special Agents will work with your organization to gather valuable evidence related to the intrusion. Intrusion investigations are conducted in a manner that causes little or no disruption to normal operations. Apprehending cyber criminals and the recovery of data is a priority for HSI intrusion investigations.



Protecting the Homeland
with **Honor, Service, and
Integrity**

Q & A

