VIRGINIA
IT AGENCY

WELCOME TO THE

MAY 4, 2022

ISOAG MEETING

VIRGINIA IT AGENCY

Welcome/Introduction	
Cybersecurity Process Using ISO/ SAE 21434	Kevin Heaslip/VT
What if the Attack Surface were Invisible	John Joseph & Dr. Vahid Heydari/ Obtegocyber
Privacy and Computer Security Issues, A State Enforcement Perspective	Samuel “Gene” Fishel/OAG
Upcoming Events	
Adjourn	

VIRGINIA
IT AGENCY

THERE ARE NO SLIDES FOR KEVIN HEASLIP

THEY ARE IN A SEPARATE PDF

Obtego Cyber

The Invisible Attack Surface™

OBTEGO CYBER

Meet Obtego Cyber

Dr. Vahid Heydari (CTO) created our technology, which has been recognized by Sandia National Laboratories, IEEE, and others.

John Joseph IV (CEO) directs a business incubator and has cofounded/advised numerous startups.

Argonne NATIONAL LABORATORY

International conference ICCWS on Cyber Warfare & Security

Sandia National Laboratories

MACH37

RAPID REACTION Technology Office

21ST COLLOQUIUM FOR INFORMATION SYSTEMS SECURITY EDUCATION

AGC PARTNERS

OBTEGO CYBER

OBTEGO CYBER

What's the (Fundamental) Problem?

Attackers can find your attack surface – shrinking/moving it doesn't change that

What's the Solution?

Make the attack surface invisible

"I have pretty much thrown every type of NMAP scan (UDP/TCP) toward the IP which I know to try. So far…there have been no ports or services returned through these scans. The external attack surface is ***totally hidden*** *from these scans."*

- Brian Jackson, President and COO, Abacus Technologies (MSP)

How Is “Invis” Different?

- ✓ Makes attack surface invisible – attackers can’t see your servers
- ✓ Zero open ports
- ✓ Authenticates without a login page (Log4J target)
- ✓ Works for SMB
- ✓ Faster, simpler install and no impact on performance

When Attackers Pursue the Attack Surface, What Will They See?

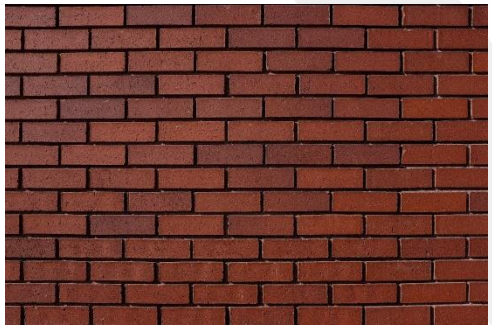
Status Quo: Easy Entry

Standard Zero Trust: Shrinks

```
nmap -T4 -A -v [redacted]

PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http nginx
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: nginx
```

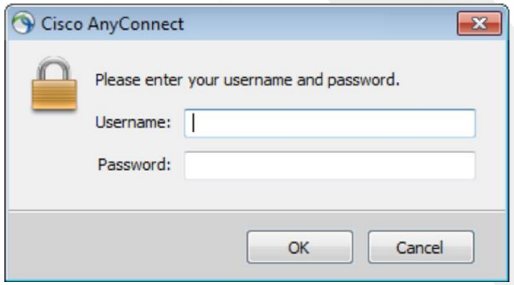
Obtego : Invisible

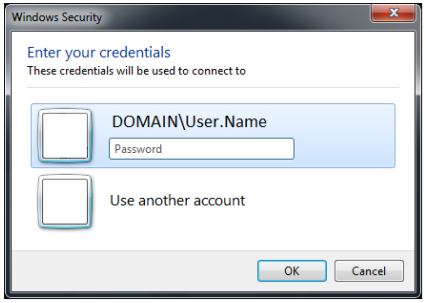


```
$ nmap  -p0-65535 50.19.51.201 -T5:
Host is up (0.0015s latency).
```

All 65536 scanned ports on 54.39.59.202 are closed

Make These Invisible





In Addition: Prevents Malware Lateral Movement

VPN	Remote users have access to the entire LAN
Micro-Segmentation	Limits remote users to a Subnet
Obtego	**Limits remote users to a Single App on a Single Server**

Obtego Solution vs Status Quo

	VPNs	Standard Zero Trust	Obtego
Provides principle of least privilege	✗	✓	✓
Does not change the IP of users	✗	✓	✓
Helps prevent lateral movement of ransomware (Remote user only has access to a specific port on a specific server instead of all ports of all network devices)	✗	✓	✓
Supports SMB (sharing access to files etc.)	✓	✗	✓
Makes the Attack Surface Invisible (no open TCP or UDP ports)	✗	✗	✓
Does not sacrifice performance	✗	✗	✓

Take A Next Step with Us?

- **Step 1:** We send you quick and easy deployment instructions and are available to answer questions
- **Step 2:** We enable you to make the technology available to users inside a testing environment
- **Step 3:** We schedule a meeting to assess results and metrics and discuss options for moving forward

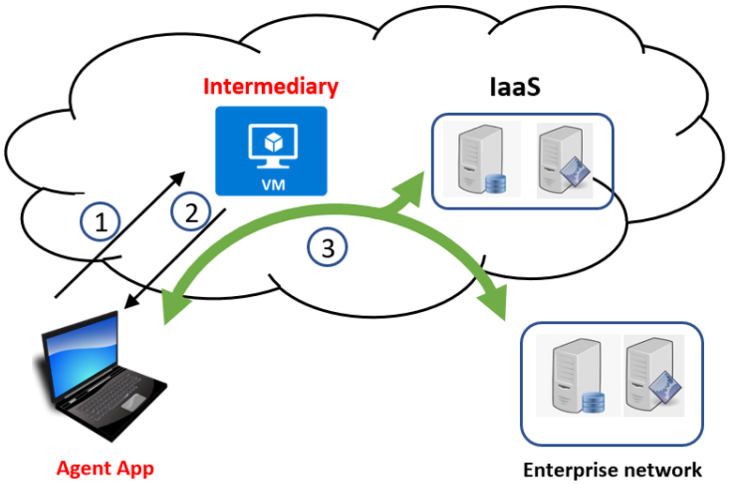
Questions?

Obtego Cyber

The Invisible Attack Surface™

Appendix

Obtego Secure Remote Solution Framework



1	Authentication Request
2	List of Authorized Applications
3	Data Communication via Intermediary

Key Info

Current Product	Built for users needing remote access (Windows)
Attacks We Address	DDoS Attacks: SYN Flooding, HTTP Flooding, SSL/TLS Exhaustion; Authentication Bypass Attacks: Password attacks, Direct page request, Parameter modification, Session ID prediction, SQL injection, Path Traversal, arbitrary code execution, arbitrary file reading; etc.
Zero Day	Combat Zero-day exploits on TCP/UDP Port Vulnerabilities
Ransomware	Prevent lateral movement of ransomware from remote device to enterprise network
Future State	Contain ransomware spread *inside* perimeter and minimize phishing attack spread

OBTEGO CYBER

Product Development Roadmap

- **Gen 1: Invisible attack surface with easier install and no open ports**
- **Gen 2: Rotating IP product for IPv6**
- **Gen 3: Isolate internal attackers**

OBTEGO CYBER

OBTEGO CYBER

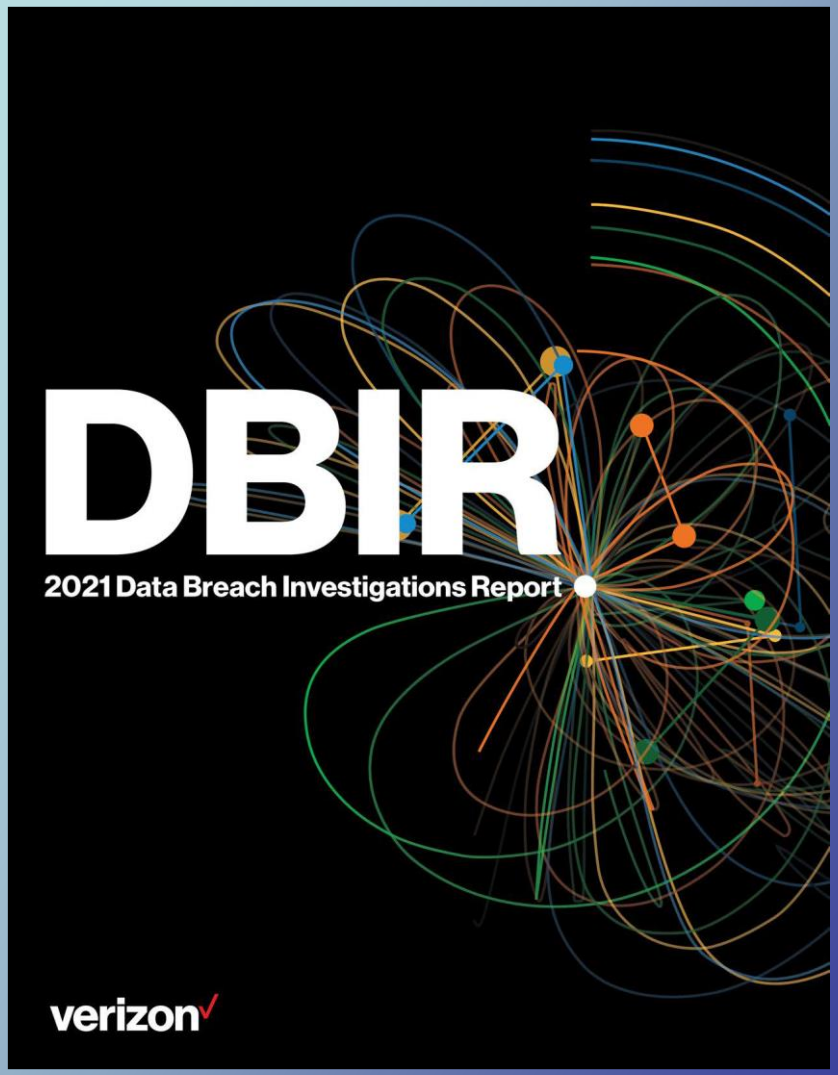
Privacy and Computer Security Issues: A State Enforcement Perspective

Gene Fishel
Senior Assistant Attorney General
Chief, Computer Crime Section
Virginia Attorney General's Office

Outline

- Database Breaches
- Identity Theft
- Phishing
- Computer Trespass
- Computer Fraud

Database Breaches



Verizon Database Breach Report 2021

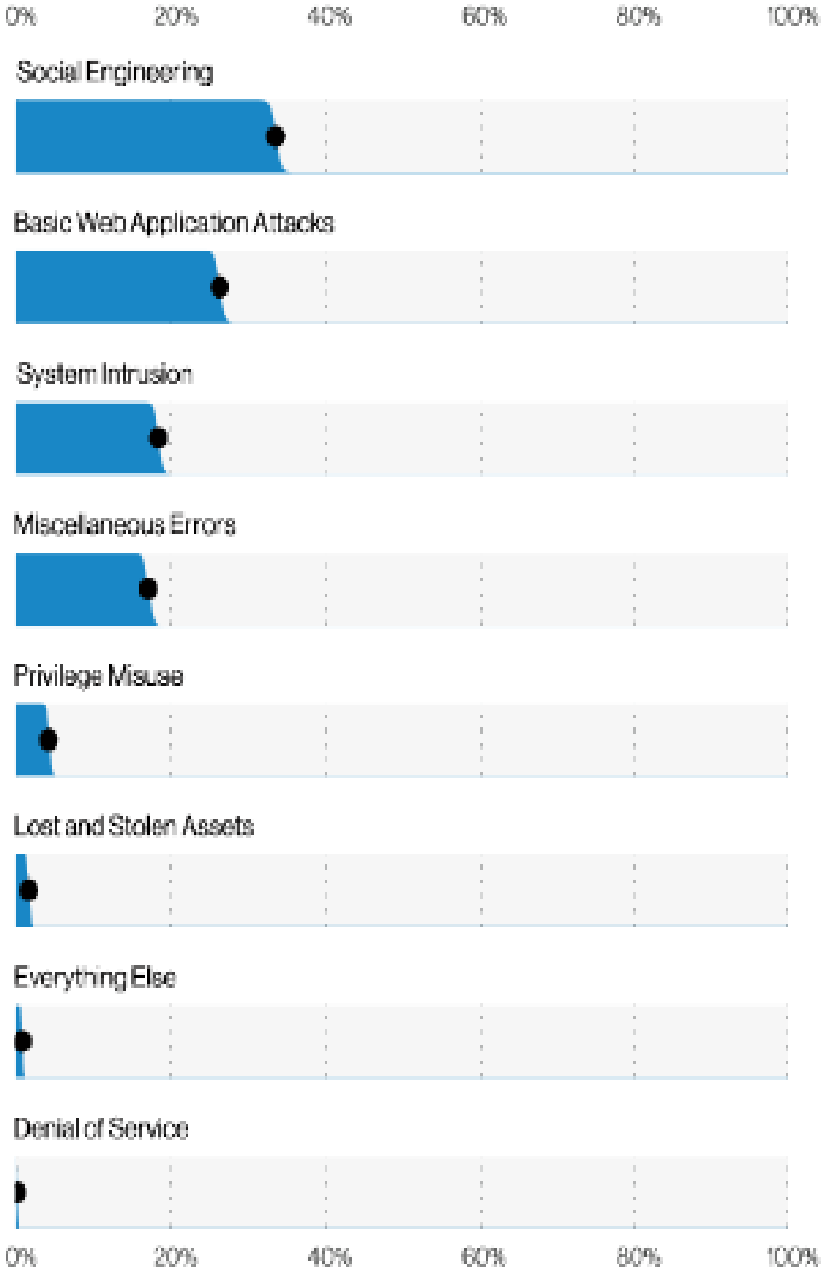


Figure 5. Patterns in breaches (n=5,275)

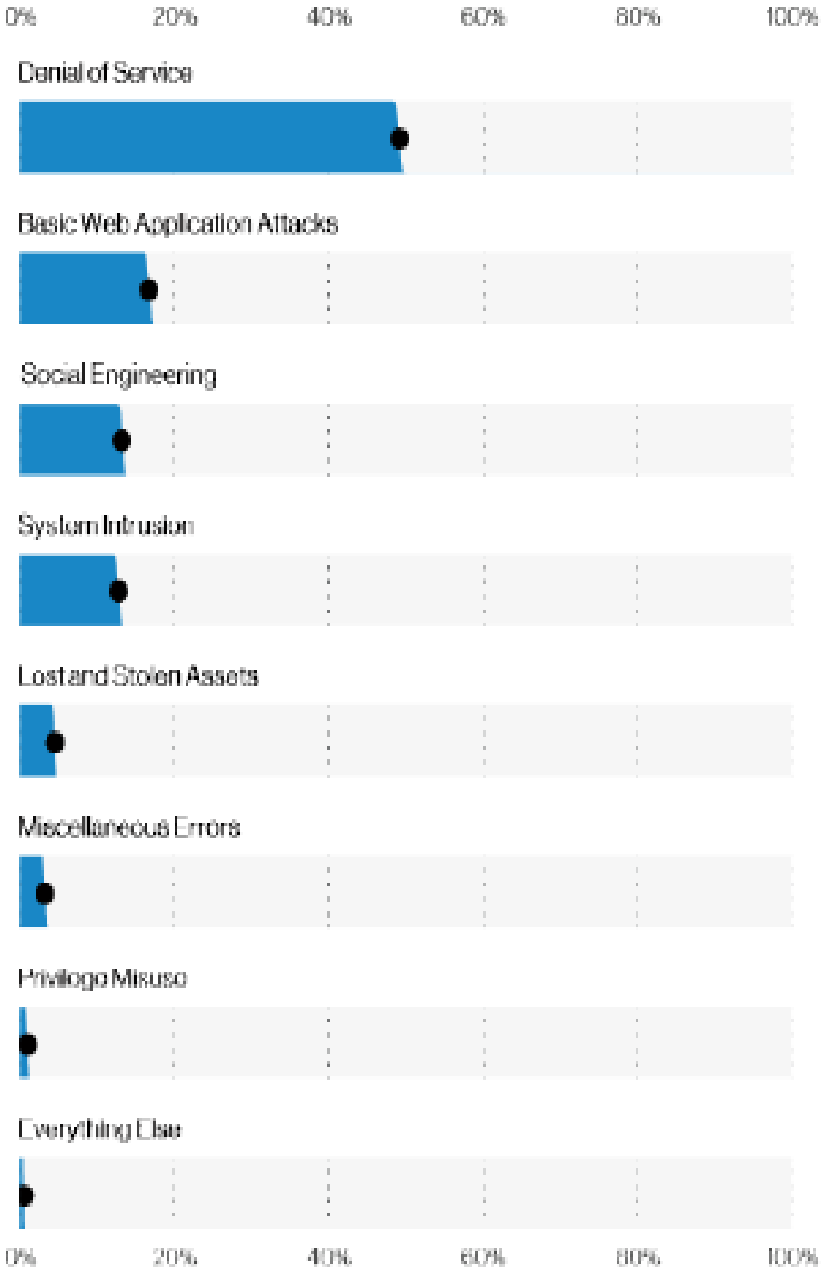


Figure 6. Patterns in incidents (n=29,206)

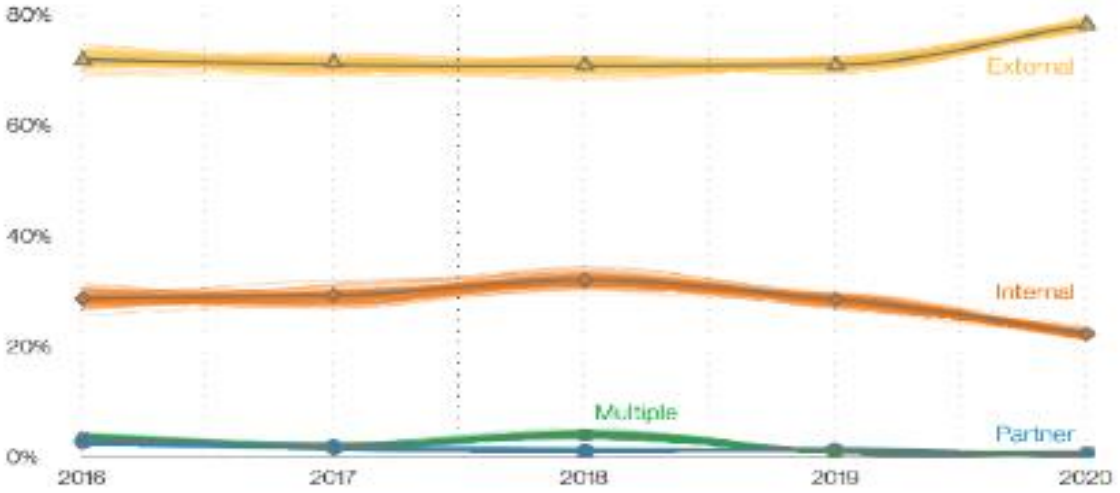


Figure 14. Threat actor over time in breaches

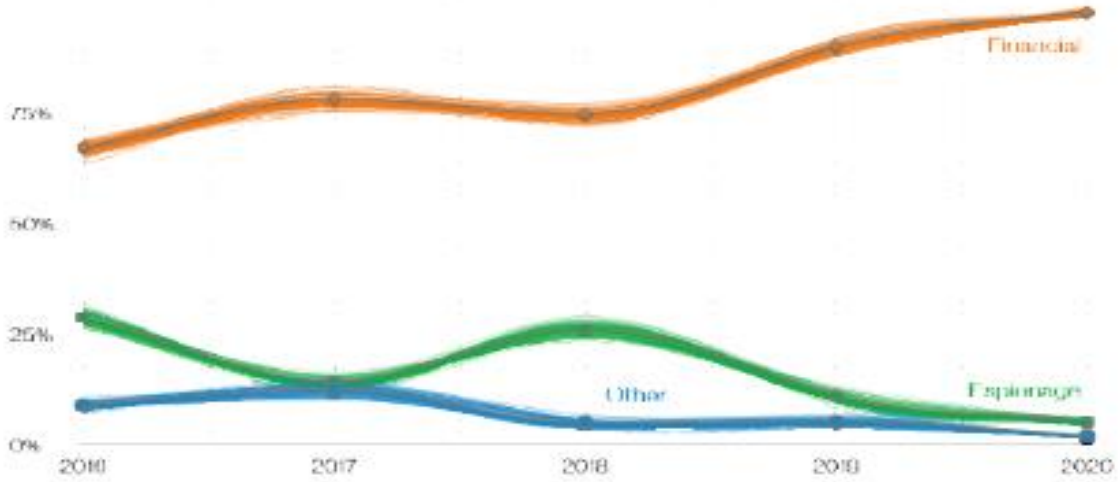


Figure 15. Top threat actor motive over time in breaches

As in past years, financially motivated attacks continue to be the most common (Figure 15), likewise, actors categorized as Organized crime continue to be number one (Figure 16).

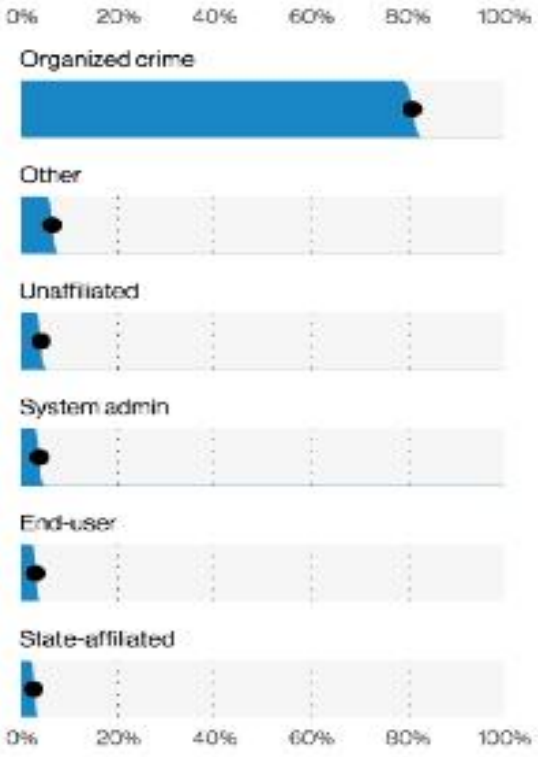


Figure 16. Top threat actor varieties in breaches (n=2,277)

14 As You Like It, William Shakespeare.
15 Anyone know if the Cyber+ trademark is available?

Public Administration NAICS 92

Summary

By far the biggest threat in this industry is the social engineer. Actors who can craft a credible phishing email are absconding with Credentials at an alarming rate in this sector.

Frequency	3,236 incidents, 885 with confirmed data disclosure
Top Patterns	Social Engineering, Miscellaneous Errors and System Intrusion represent 92% of breaches
Threat Actors	External (83%), Internal (17%) (breaches)
Actor Motives	Financial (96%), Espionage (4%) (breaches)
Data Compromised	Credentials (80%), Personal (18%), Other (6%), Medical (4%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Access Control Management (6), Account Management (5)

The Social Engineering pattern was responsible for over 69% of breaches in this vertical (Figure 116). Clearly, this industry is a favorite honey hole among the phishing fiends. The Social actions were almost exclusively Phishing with email as the vector (Figure 117). Pretexting was rarely leveraged at all, and why should they go to all the work of inventing a scenario when a straight up phish gets the job done?

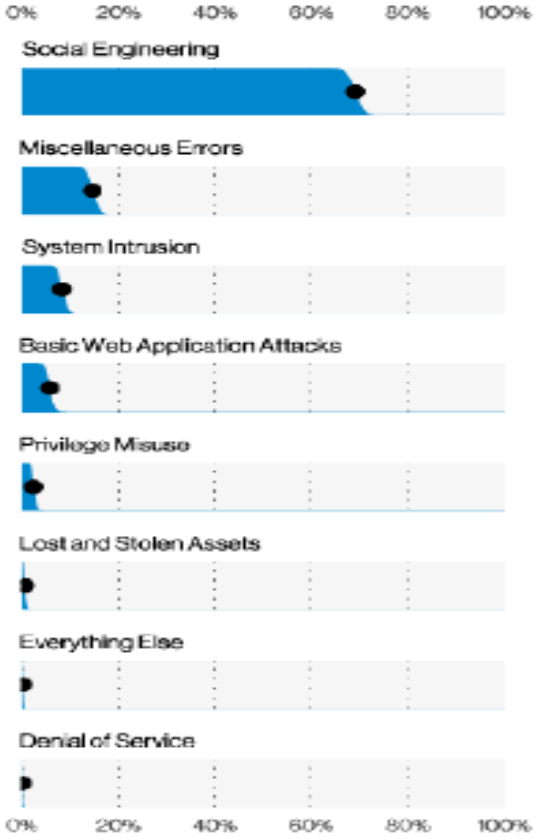


Figure 116. Patterns in Public Administration breaches (n=885)

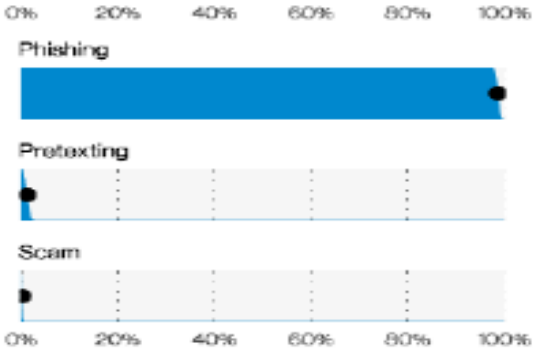


Figure 117. Social varieties in Public Administration breaches (n=611)

Database Breach Laws

50 State Laws +

Virginia Code §18.2-186.6

- Applies to any legal entity; broad application
- Unencrypted data accessed or acquired by unauthorized person (only electronic data)
- Must have caused or *reasonably believe* will cause fraud or identity theft to resident
- Must notify Atty General's Office and affected resident without *unreasonable delay*

Database Breach Laws

- Pertinent Provisions
  - Law enforcement delay acceptable
  - Provisions also apply to encrypted data acquired in an unencrypted form or if person has access to the encryption key
  - If more than 1,000 affected residents, must also notify consumer reporting agencies

Database Breach Laws

- Pertinent Provisions
  - Data = “personal information” to include first and last name AND = SSN, financial acct/credit card numbers along with access code, driver’s license number
  - Tax identification numbers and tax witheld (to counter prevalent payroll breaches / IRS scams)
  - Passport numbers, military ID numbers

Database Breach Laws

- Pertinent Provisions
  - Notice = written, electronic, telephone or substitute
  - Substitute Notice = over $50K in cost, over 100,000 residents, or no sufficient contact info…can then post conspicuously on website, or notify statewide media

Database Breach Laws

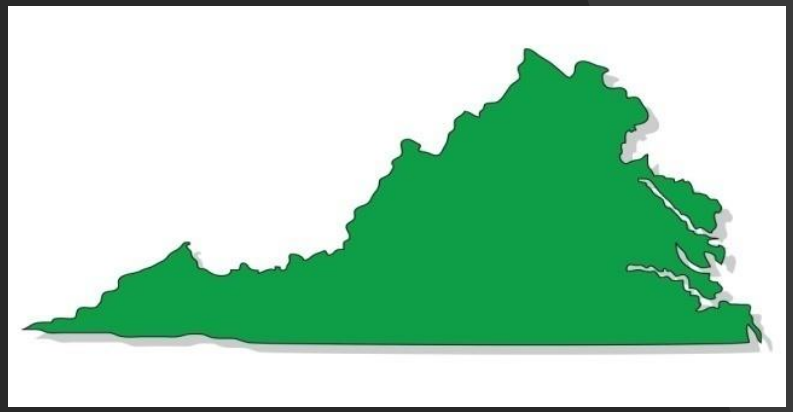
- Pertinent Provisions
  - Notice must include:
    - Incident in general terms
    - Type of information accessed
    - The general acts of entity to prevent further unauthorized access
    - Telephone number for affected persons to call
    - Advice directing person to remain vigilant of accounts and monitor free credit reports

Database Breach Laws

- Pertinent Provisions
  - Attorney General's Office can bring civil enforcement action for failure to comply with notice provisions
  - $150,000 penalty per breach
  - Does not prohibit affected residents from filing individual claims

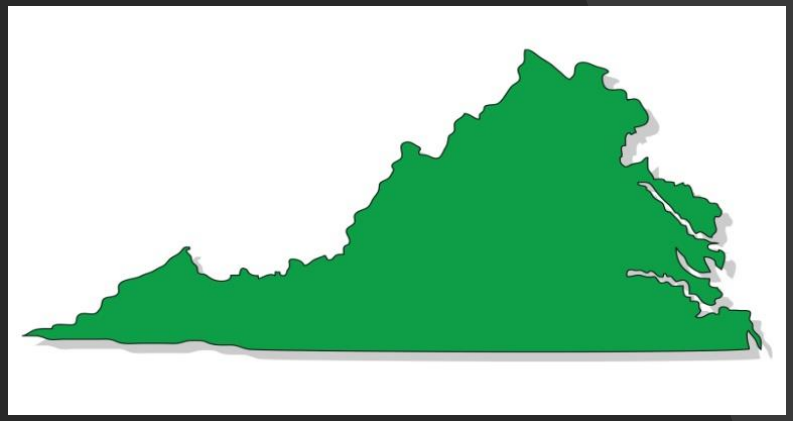
Enforcer’s Perspective

- 1530 database breach notices received in VA in 2021 (1175 in 2020)
- Broad cross-section of industry
- Intrusion, lost equipment, theft are most common occurrences
- Small breaches dominate



Enforcer's Perspective

- From 1 resident to over 1 million residents affected in a single breach
- Work with your attorneys
- Contact law enforcement
- Work with our office



Recent Judgments

UBER

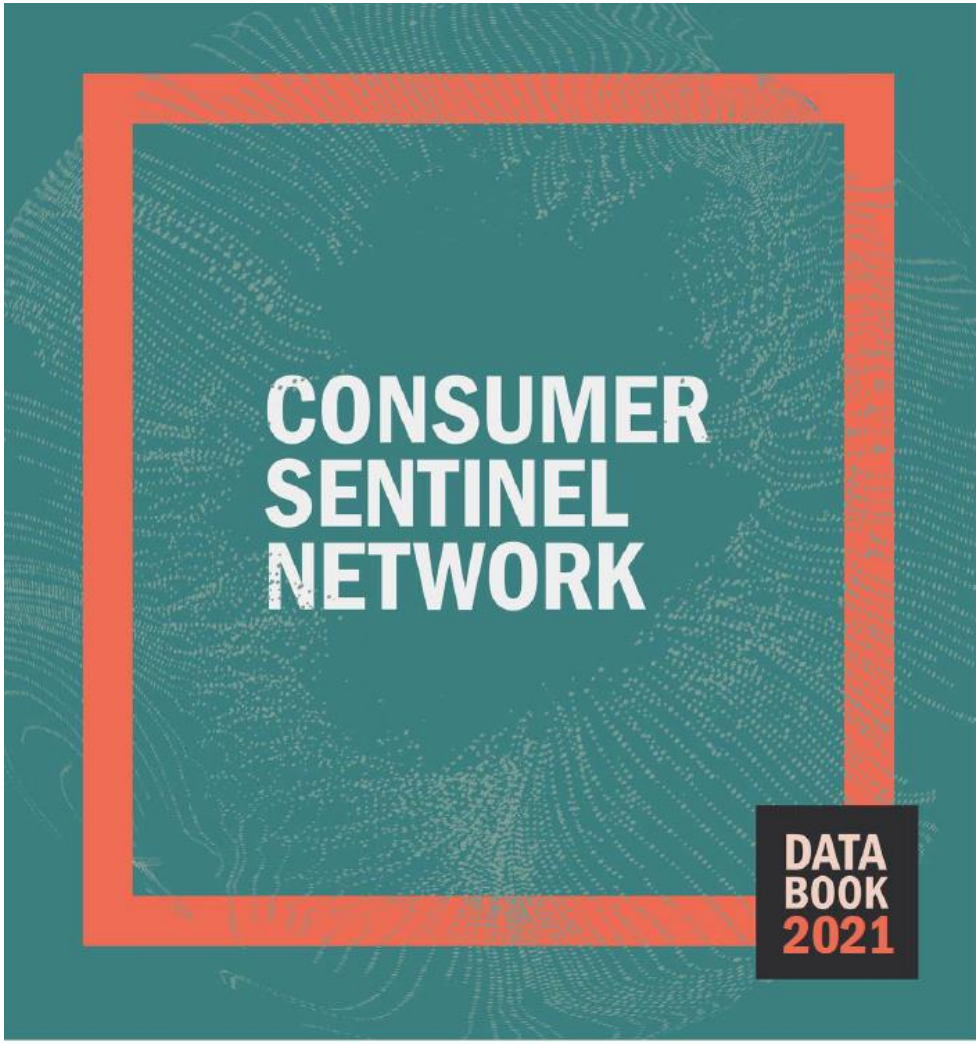
- Intentionally concealed breach for over one year
- Driver's license numbers involved
- 20,000 Virginia drivers affected
- Paid $3 million to Virginia in penalties

BOMBAS

- Did not report for three years (unintentional)
- Credit card numbers of 1,200 Virginians
- Paid $25,000 in penalties to Virginia

Identity Theft

FTC Annual Report



CONSUMER SENTINEL NETWORK
DATA BOOK 2021

SNAPSHOT

5.7 MILLION REPORTS

TOP THREE CATEGORIES

1 Identity Theft

2 Imposter Scams

3 Credit Bureaus, Info Furnishers and Report Users

2.8 million fraud reports

25% reported a loss

$5.9 billion total fraud losses

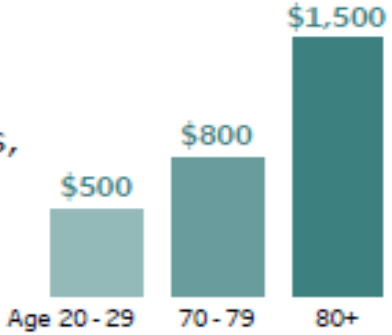
$500 median loss

Younger people reported losing money to fraud **more often than older people.**

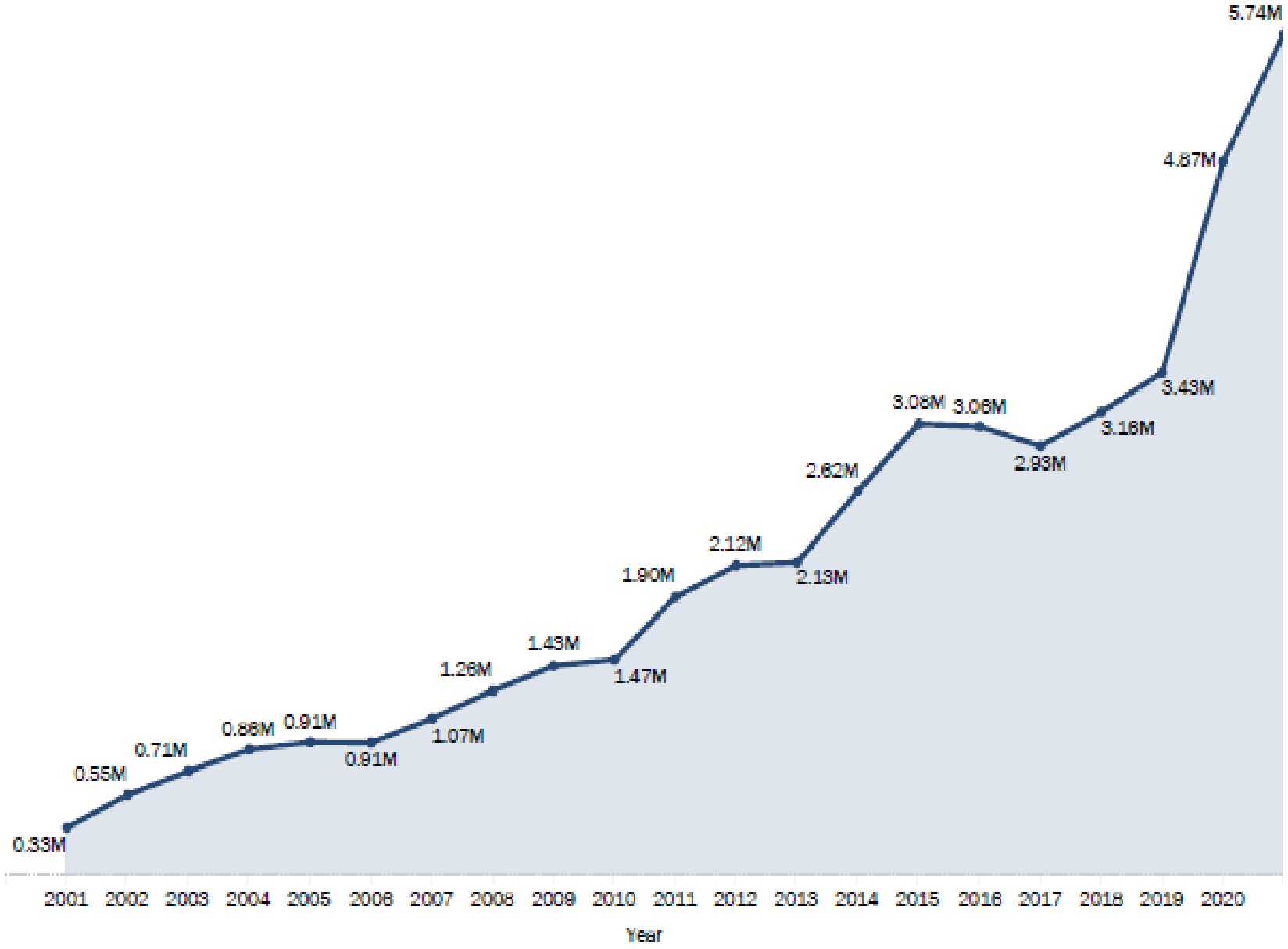
41% Age 20-29

18% Age 70-79

But when people aged 70+ had a loss, **the median loss was much higher.**



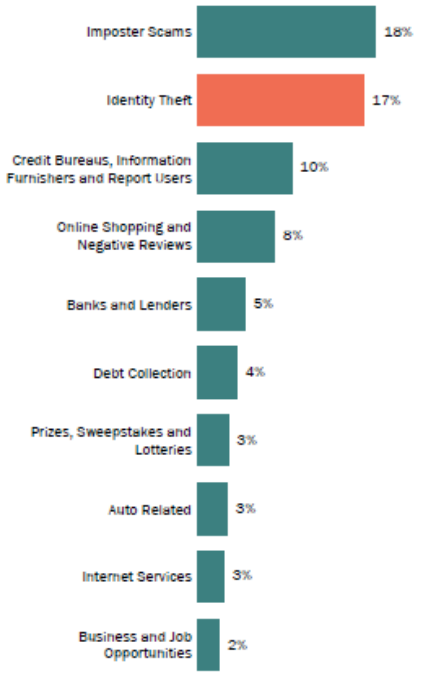
Number of Fraud, Identity Theft and Other Reports by Year



VA Stats

Virginia

Top Ten Report Categories



Fraud & Other Reports

14th
State Rank
(Reports per 100K Population)

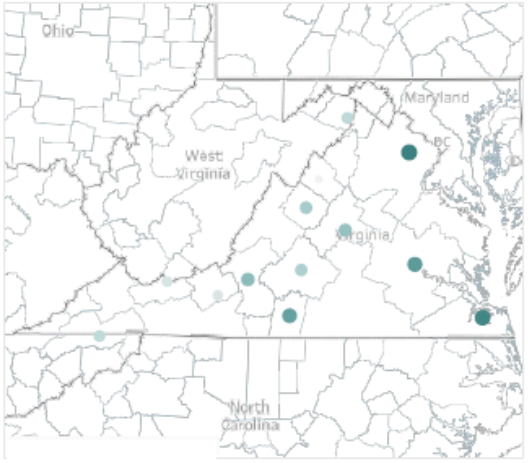
93,763
Total Fraud & Other Reports

Fraud Losses

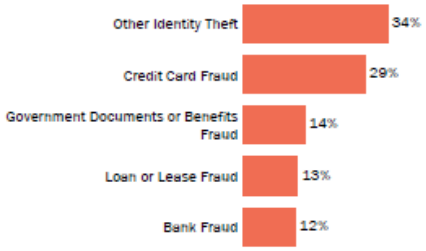
$112.9M
Total Fraud Losses

$500
Median Fraud Losses

Fraud & Other Reports by Metropolitan Area



Top Identity Theft Types



Identity Theft Reports

25th
State Rank
(Reports per 100K Population)

19,214
Identity Theft Reports

Identity Theft

A. Unlawful for any person, without authorization….to:

1. Obtain, record or access identifying information which is not available to the general public that would assist in accessing financial resources…;

2. Obtain money, credit, loans, goods or services through the use of identifying information of such other person;

3. Obtain identification documents in such other person's name

Identity Theft

A. Identifying Information

(i) name;
(ii) date of birth;
(iii) social security number;
(iv) driver's license number;
(v) bank account numbers;
(vi) credit or debit card numbers;
(vii) personal identification numbers (PIN);
(viii) electronic identification codes;
(ix) automated or electronic signatures;
(x) biometric data;
(xi) fingerprints;
(xii) passwords; or
(xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain money, credit, loans, goods, or services.

Identity Theft

- Penalties
  - Up to 12 months jail
  - If over $200, 1-5 years imprisonment
  - If 50 or more person’s identifying info stolen, 1-5 years
  - 1-10 years if information is used to commit another crime

Identity Theft

WHAT CAN YOU DO?

- Protect your social security number
- Use caution when giving out personal info (phishing)
- Treat your trash carefully
- Protect your postal mail
- Check your bank statements often

Identity Theft

WHAT CAN YOU DO? cont…

- Check your credit reports (1 free report annually)
  - Annualcreditreport.com (recommended by FTC)
- Protect your computer (firewall, anti-virus, lock wireless networks)
- Use some plain common sense (i.e. too good to be true)

Identity Theft

HOW TO SPOT IT…

- You see withdrawals from your bank account that you can’t explain
- You don’t get your bills or other mail
- Debt collectors call you about debts that aren’t yours
- You find unfamiliar accounts or charges on your credit report

Identity Theft

WHERE TO REPORT IT…

- Creditors (Card Issuers & Utilities)
- Credit Bureaus
- Federal Trade Commission (FTC)
- Local/State Law Enforcement
- Office of the Attorney General

ID THEFT RESOURCE

How to Avoid Identity Theft

A Guide for Victims

Office of the Attorney General of Virginia
Victim Notification Program

Phishing

- Using a computer to gather identifying information
  - A. Unlawful to use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information – 1-5 years imprisonment
  - B. Distribution of material – 1-10 years
  - C. Uses such information to commit another crime – 1-10 years

From: Wells Fargo <security@onlinebank-wellsfargo.com>
To: Fishel, Samuel
Cc:
Subject: Your Account Security Notification

WELLS FARGO ADVISORS

Dear Wells Fargo Customer,

We recently reviewed your account and suspect that your Wells Fargo account may have been accessed from an unauthorized computer.

This may be due to changes in your IP address or location. Protecting the security of your account and of the Wells Fargo network is our primary concern.

We are asking you to immediately log in and report any unauthorized withdrawals and check your account profile to make sure no changes have been made.

To protect your account please follow the instructions below:

*LOG OFF AFTER USING YOUR ONLINE ACCOUNT

Please log in your account by clicking on the link below.

https://onlinebank-wellsfargo.com/signon

Verify the information you entered is correct.

We apologize for any inconvenience this may cause and appreciate your

Phishing

- Supervisor Scams
  - Posing as supervisor
  - Requests transfer money, bank account numbers, payroll info
- Employee test emails
- If unsure, check with actual source. Don’t hit reply.

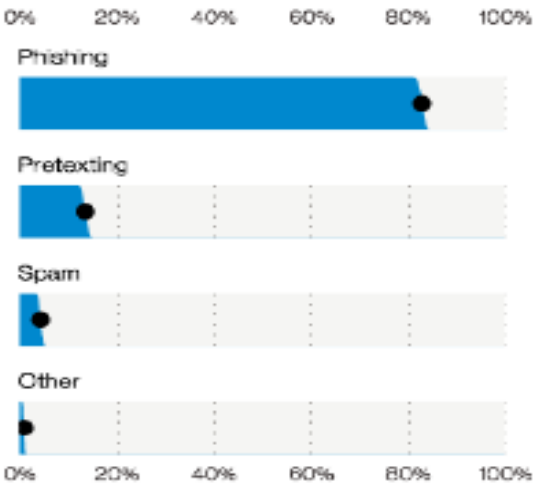


Figure 73. Top Social varieties in Social Engineering incidents (n=3,810)

A lot of Social Engineering breaches steal Credentials[61] and once you have them, what better thing to do than to put those stolen creds to good use, which falls under Hacking. On the other hand, that Phishing email may have also been dropping Malware, which tends to be a Trojan or Backdoor of some type (Figure 74), a trap just waiting to be sprung.

As with past years, Social actions are predominantly Phishing, though Pretexting, normally associated with the BEC,[62] also makes a strong showing. Remember those children and their great stories? This is the grownup version of why they need what you have.

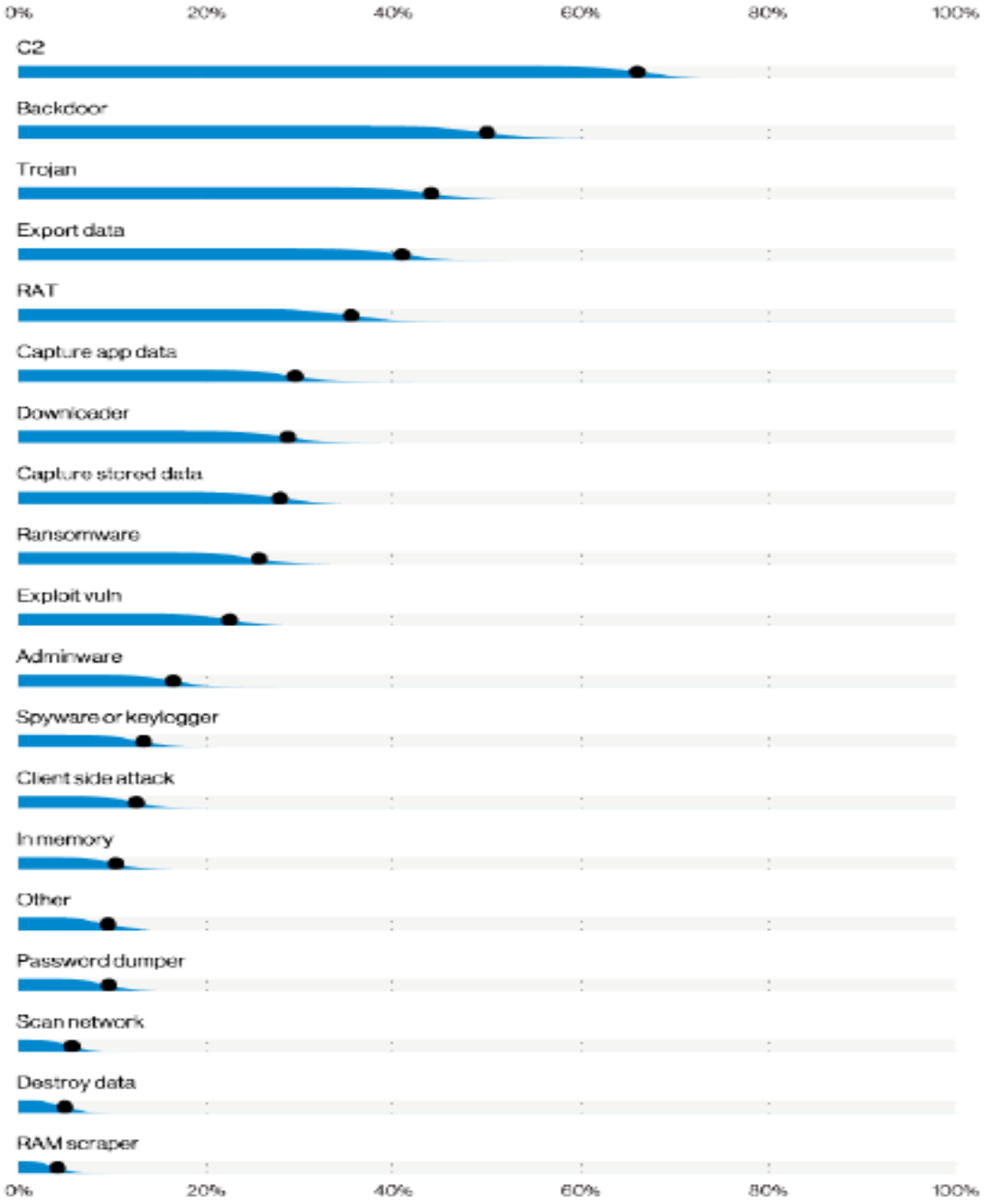


Figure 74. Malware varieties in Social Engineering incidents (n=130)

Computer Trespass

- Unlawful, with malicious intent, to:
  - Remove, halt, or disable computer data or program
  - Cause a network to malfunction
  - Alter, disable, or erase computer data, programs, or software
  - Effect the creation or alteration of financial instruments
  - Use a computer to cause physical injury to property
  - Use a computer to make unauthorized copy
  - Install keystroke logger
  - Install software to take control of computer in order to cause damage or disrupt transmissions

Computer Trespass

- Penalties:
  - Up to 12 months jail
  - Damage over $1K, 1-5 years imprisonment
  - Installs software on more than 5 computers, 1-5 years
  - Keystroke logger violation, 1-5 years
  - Exception for ISPs

Computer Trespass

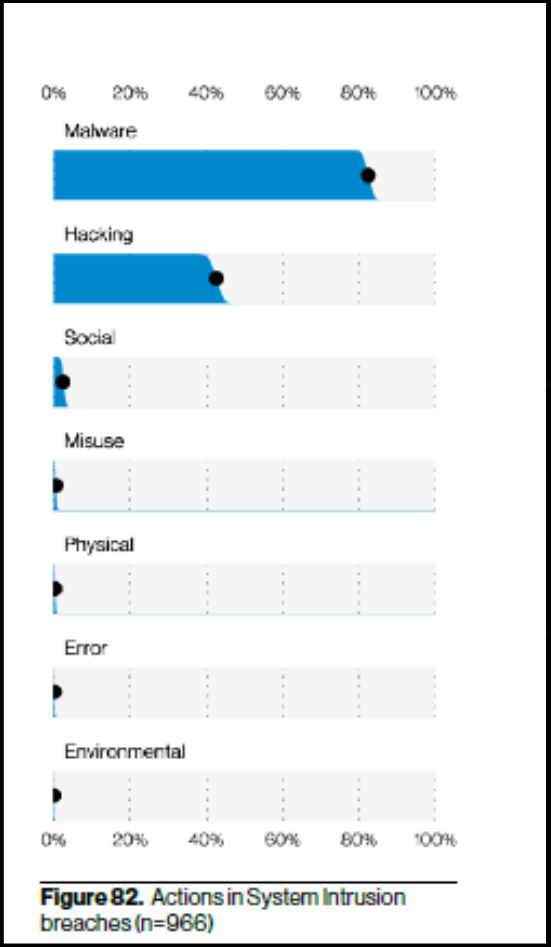


Figure 82. Actions in System Intrusion breaches (n=966)

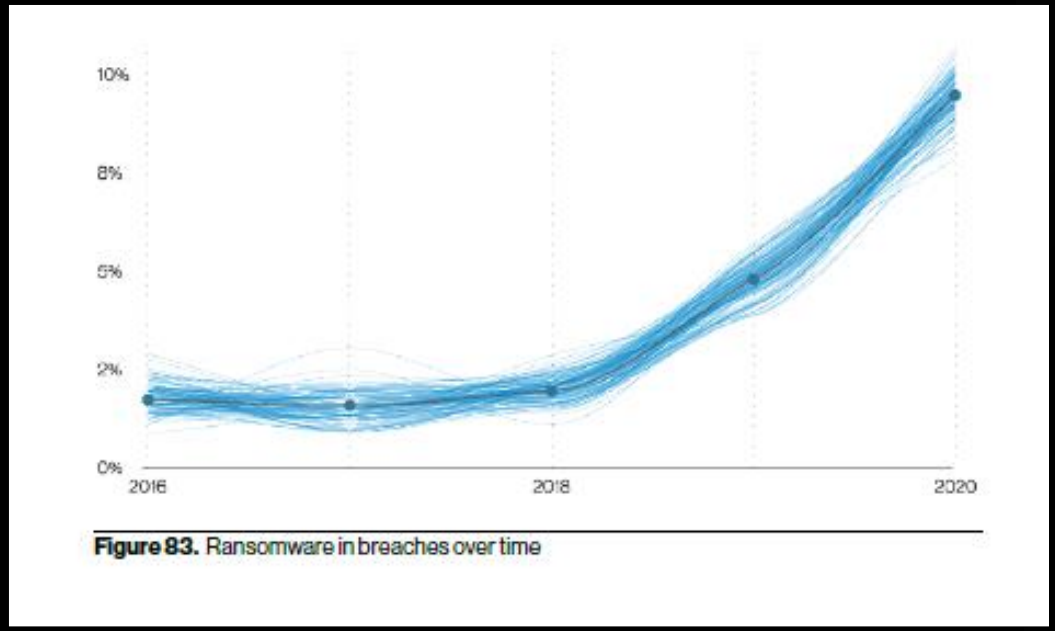


Figure 83. Ransomware in breaches over time

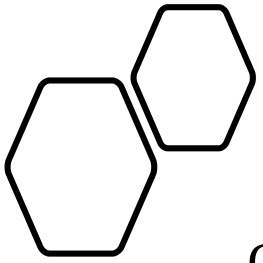
Computer Trespass

- Preventative measures:
  - Employee training
  - Updated security software
  - Firewalls
  - Strong passwords, or two factor authentication
  - Encryption vs. plain text
  - Tabletop exercises

Computer Fraud

- Use a computer without authority to:
  - Obtain property or services by false pretenses
  - Embezzle or commit larceny
  - Convert the property of another
    - Value is $200 or more – 1-10 years imprisonment
    - Otherwise up to 12 months in jail

VA Computer Crimes



- Civil Remedy
  - Any individual wronged by any violation of aforementioned prohibitions may bring suit
  - For any damages sustained and cost of suit
  - Loss of profits
  - Malicious intent NOT required

RESOURCES

VA Office of the Attorney General
http://www.ag.virginia.gov

Internet Crime Complaint Center
http://www.ic3.gov

Federal Trade Commission (FTC)
http://www.ftc.gov

Thank You

Gene Fishel
Sr Asst Attorney General
sfishel@oag.state.va.us
804-786-2071

www.ag.virginia.gov

DISCLAIMER: The information provided in this presentation is not intended as legal advice and does not represent an official or unofficial OAG opinion.

VIRGINIA
IT AGENCY

Upcoming events

THE COMMONWEALTH OF VIRGINIA SECURITY CONFERENCE WILL BE HELD ON AUG. 18, 2022 VIRTUALLY.

MORE DETAILS WILL BE FORTHCOMING.

VIRGINIA IT AGENCY

VASCAN
CALL FOR PROPOSALS

VASCAN 2022 - Call for Proposals (google.com)

The VASCAN 2022 conference will be held at Virginia Commonwealth University in Richmond, Virginia, on Oct. 3 and 4, 2022.

The VASCAN conference relies largely on its member institutions in sharing their experiences and best practices to help all member institutions to grow. The following call-for-proposals (CFP) is open to all Virginia public and private institutions as well as public and private organizations affiliated with the VASCAN community.

Selected presentations will be featured at the conference and a complimentary registration will be provided to the presenter.

Please consider submitting a presentation and share your experiences with all the VASCAN community this year. The CFP will close on Friday, Sept. 9, 2022.

JUNE 2022 ISOAG

June 4, 2022, from 1 to 4 p.m.

Presenters:

Rick Tiene -- MissionSecure

Alan Gernhardt --- Virginia Freedom of Information Advisory Council

Benjamin Sady -- Dixon Hughes Goodman LLP

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!