VITA Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Feb. 5, 2020

ISOAG February Agenda

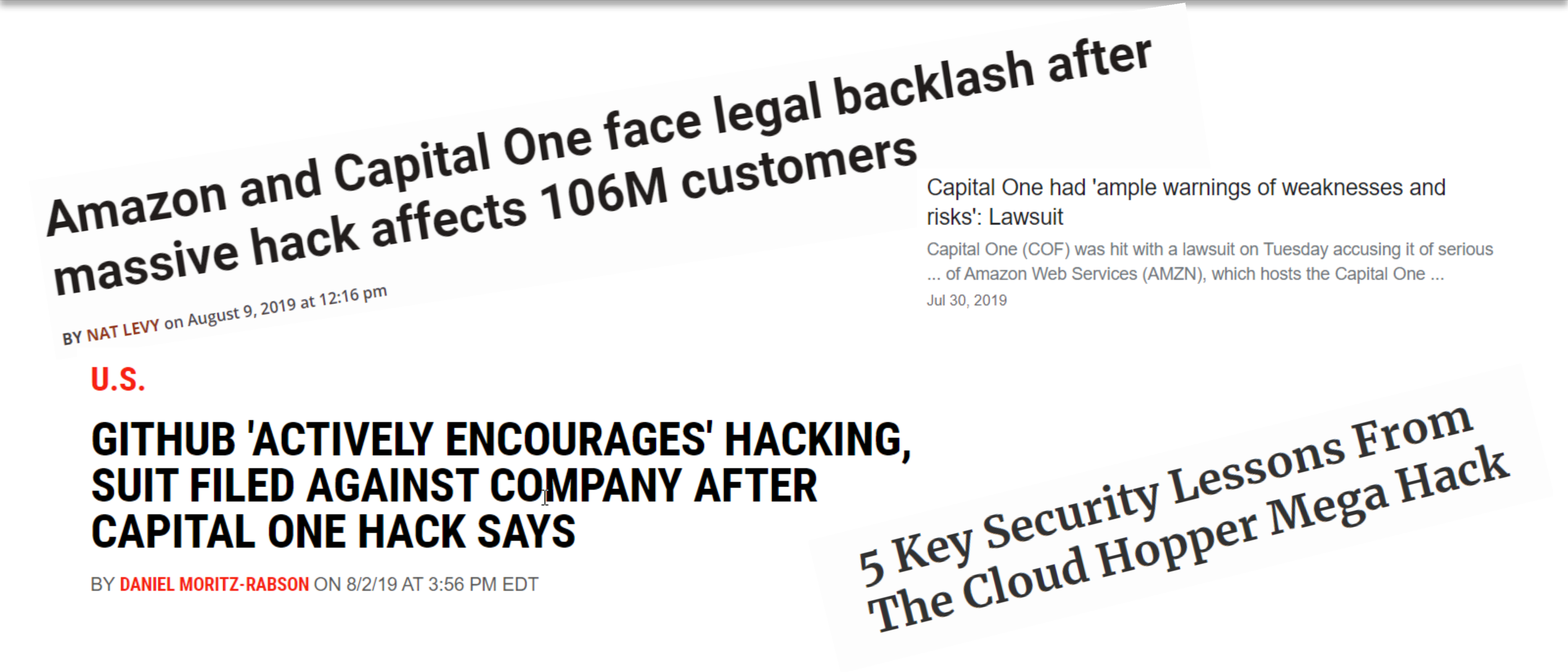
- Welcome and Opening Remarks – Mike Watson, VITA
- Risks/Benefits Moving to the Cloud – Beth Waller, Woods Rogers PLC
- Fair Quantitative Risk Management Programs – Brett Kourey, RiskLens
- Computer Security Laws and Trends – Samuel “Gene” Fishel, OAG
- New Endpoint Network Security Tools – Bill Stewart, VITA

Blue Skies or Stormy Weather: Looking at the Cloud

Liability backdrop

1

Liability



Amazon and Capital One face legal backlash after massive hack affects 106M customers

BY NAT LEVY on August 9, 2019 at 12:16 pm

Capital One had 'ample warnings of weaknesses and risks': Lawsuit

Capital One (COF) was hit with a lawsuit on Tuesday accusing it of serious ... of Amazon Web Services (AMZN), which hosts the Capital One ...

Jul 30, 2019

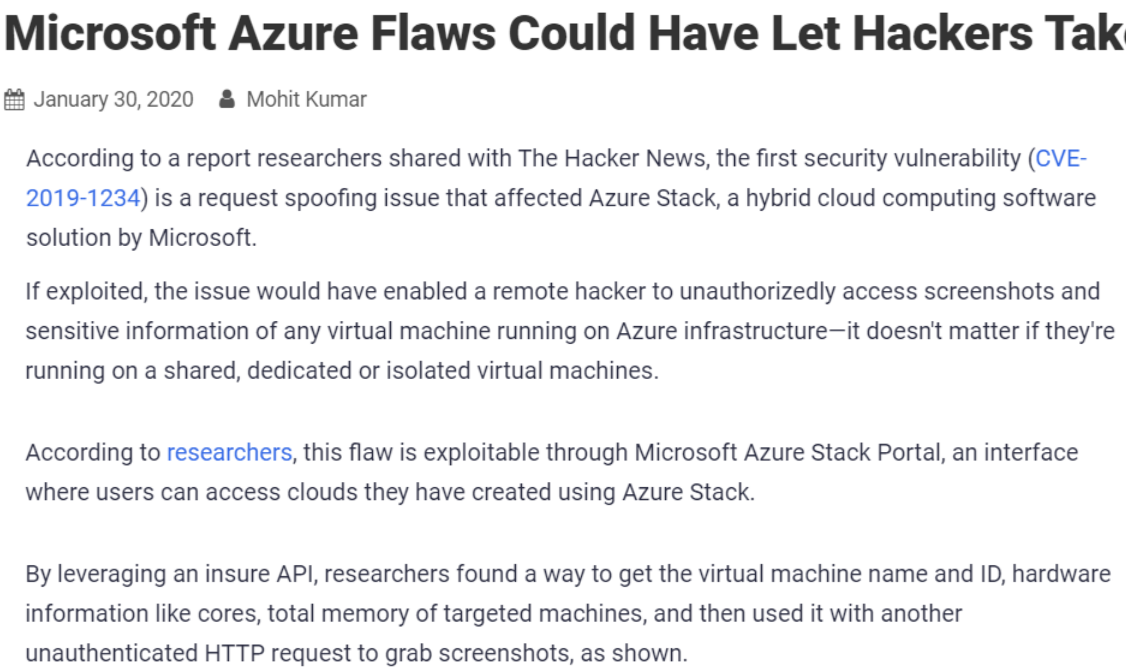
U.S.

GITHUB 'ACTIVELY ENCOURAGES' HACKING, SUIT FILED AGAINST COMPANY AFTER CAPITAL ONE HACK SAYS

BY DANIEL MORITZ-RABSON ON 8/2/19 AT 3:56 PM EDT

5 Key Security Lessons From The Cloud Hopper Mega Hack

The risk



Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Servers

January 30, 2020 Mohit Kumar

According to a report researchers shared with The Hacker News, the first security vulnerability (CVE-2019-1234) is a request spoofing issue that affected Azure Stack, a hybrid cloud computing software solution by Microsoft.

If exploited, the issue would have enabled a remote hacker to unauthorizedly access screenshots and sensitive information of any virtual machine running on Azure infrastructure—it doesn't matter if they're running on a shared, dedicated or isolated virtual machines.

According to researchers, this flaw is exploitable through Microsoft Azure Stack Portal, an interface where users can access clouds they have created using Azure Stack.

By leveraging an insure API, researchers found a way to get the virtual machine name and ID, hardware information like cores, total memory of targeted machines, and then used it with another unauthenticated HTTP request to grab screenshots, as shown.

The risk

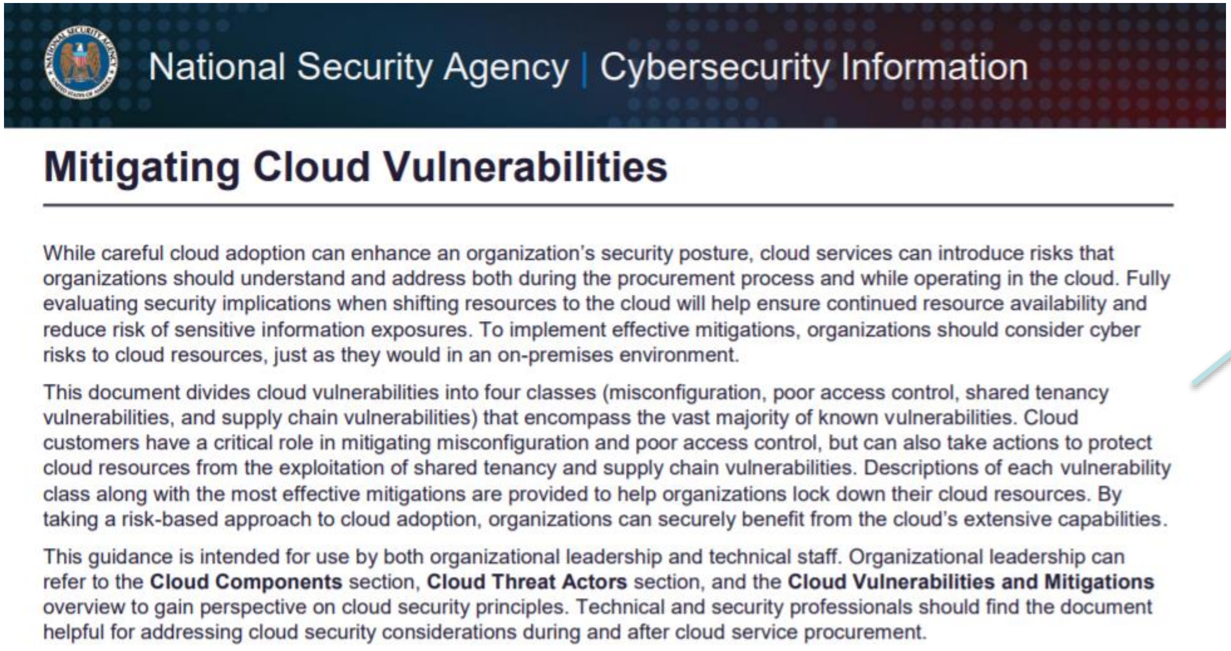
- Data breaches
- Data loss (backup issues)
- Denial of Service (Dos) attacks
- Cryptojacking
- Hijacked accounts
- Non-secure applications

aws
CapitalOne

New NSA guidance

2

NSA January 2020 release



National Security Agency | Cybersecurity Information

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures. To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities. Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources. By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

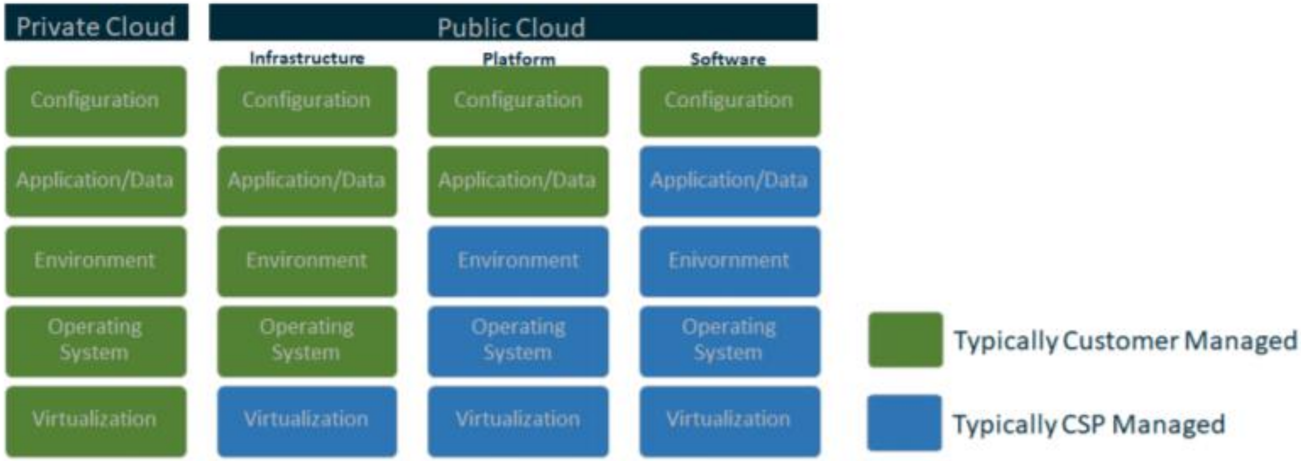
This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the **Cloud Components** section, **Cloud Threat Actors** section, and the **Cloud Vulnerabilities and Mitigations** overview to gain perspective on cloud security principles. Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement.

- Designates four classes of vulnerabilities:
  - Misconfiguration;
  - Poor access control;
  - Shared tenancy vulnerabilities;
  - Supply chain vulnerabilities.

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

CSP shared risk

- Shared cloud security responsibilities:



Private Cloud	Public Cloud		
	Infrastructure	Platform	Software
🟩 Configuration	🟩 Configuration	🟩 Configuration	🟩 Configuration
🟩 Application/Data	🟩 Application/Data	🟩 Application/Data	🟦 Application/Data
🟩 Environment	🟩 Environment	🟦 Environment	🟦 Enivornment
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization

🟩 Typically Customer Managed

🟦 Typically CSP Managed

Figure 1: Cloud Shared Responsibility Model

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

NSA January 2020 release

- Shared responsibility considerations:
  - **Threat detection** – "while CSPs are generally responsible for detecting threats to the underlying cloud platform, customers bear the responsibility of detecting threats to their own cloud based resources."
  - **Incident response** – make certain the CSPs are providing support to incident response teams
  - **Patching / Updating** – CSPs manage their own patch management but will to manage yours. Must "vigilantly deploy patches to mitigate software vulnerabilities in the cloud."

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Cloud threats

- Malicious CSP administrators
- Malicious customer cloud administrators
- Cybercriminals / nation state sponsored actors
- Untrained / neglectful cloud administrators

Mitigate risk

- Use cloud service policies to prevent users from sharing data publicly without a mission-justified role
- Use cloud or third-party tools to detect misconfigurations in cloud service policies
- Limit access to and between cloud resources with the desired state being a zero trust model
- Use cloud service policies to ensure resources default as private
- Audit access logs with automated tools to identify overly-exposed data
- Restrict sensitive data to approved storage and use data loss prevention solutions to enforce these restrictions

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Mitigate risk

- Ensure proper CSP-specific training for individuals creating or modifying cloud service policies
- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems
- Adhere to applicable standards (e.g., CSP guidance, Center for Internet Security benchmarks, DoD CCSRG)
- Configure software in cloud systems to update automatically
- Control selection of virtual machine images to require hardened baselines and enable predictable cyber defense
- Control and audit cloud service policies and IdAM changes
- Ensure that logging is enabled at all levels (e.g., user platform activity, network flow logs, SaaS/PaaS activity) to capture the reality of the environment, especially ephemeral resources, and that logs are stored immutably
- Apply traditional security practices to the cloud when possible (e.g., enable endpoint detection and response [EDR] for cloud-based endpoints)
- Follow best practices to prevent the abuse of privileged accounts (e.g., separation of duties, two-person controls)

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Mitigate risk

- Opt to modernize and take advantage of CSP services rather than "lift and shift" legacy systems
- Ensure that transitions are properly defined, funded, reviewed, and under the right leadership
- Evolve architecture and processes to incorporate new features with an understanding of changes to risk
- Understand your data and how it flows throughout various systems
- Evaluate areas where traditional IT silos of operation or infrastructure can be merged in cloud deployments
- Use CSP tools or techniques, such as infrastructure as code, to reduce the risk of misconfiguration

Source – NSA - https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Critical Steps

3

Steps

- Negotiate the risk contractually
- Audit and review options
- If vulnerabilities become known, request information from CSPs and app developers

Questions?

4

Beth Burgin Waller
bwaller@woodsrogers.com

2019

MANAGING THE ECONOMICS OF CYBER RISK

FAIR INSTITUTE

RiskLens®

CYBER RISK = BUSINESS RISK

EXPECTATIONS FOR CISOs HAVE CHANGED

FEAR, UNCERTAINTY & DOUBT → COMPLIANCE CHECKLISTS → MATURITY MODELS → CYBER RISK ECONOMICS

COMPLIANT... BUT STILL IN THE DARK

1

Qualitative Checklists & Excel

NIST CSF

Information Security Management ISO 27001 Certified

X

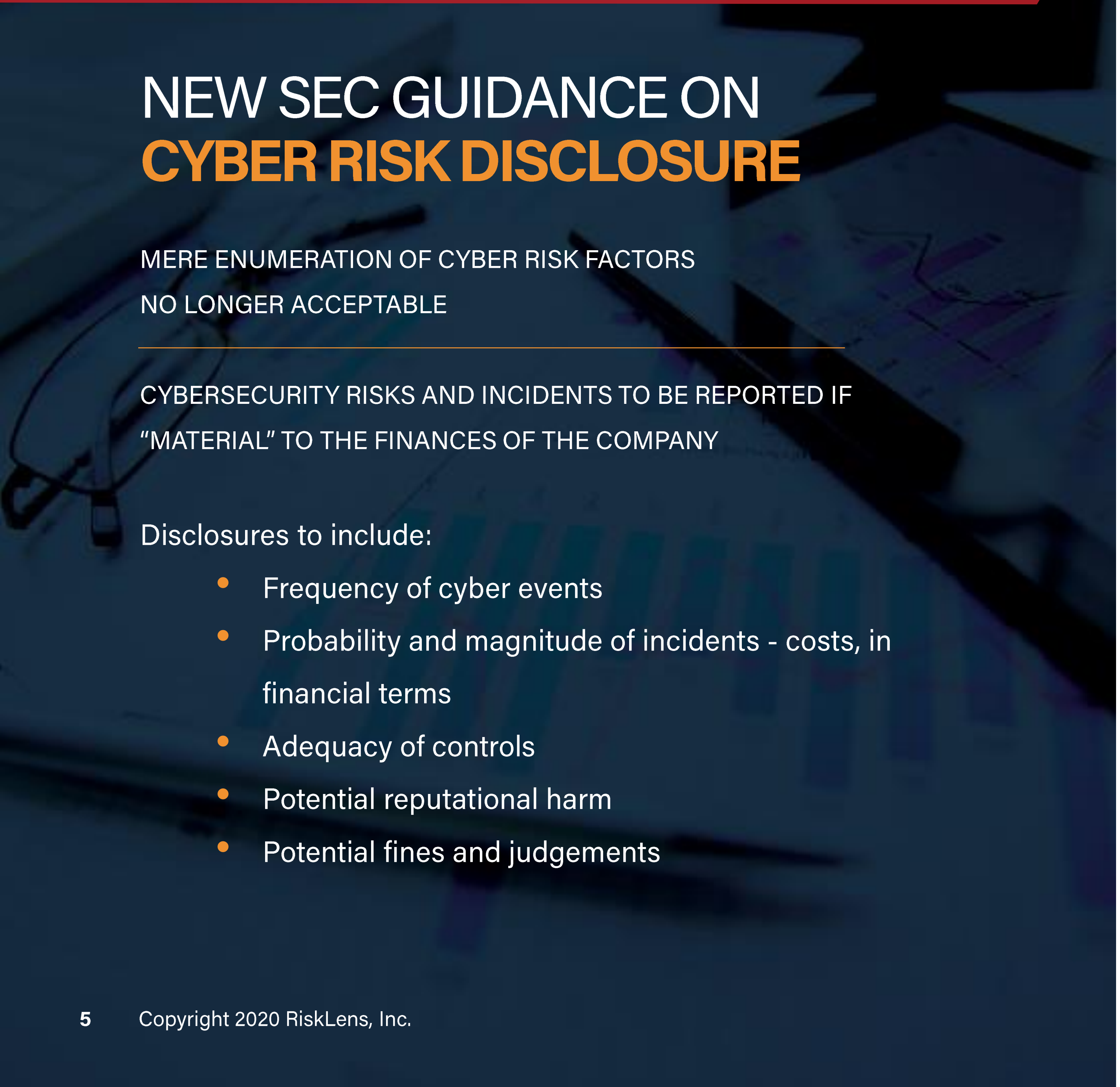
2

Governance, Risk & Compliance Tools

🟩	Very Low	1
🟩	Low	2
🟨	Moderate	3
🟧	High	4
🟥	Very Hgh	5

No embedded risk analytics capabilities in most GRC tools

The way most organizations measure risk today fails to quantify cybersecurity and operational risk in terms the business can understand and use



NEW SEC GUIDANCE ON **CYBER RISK DISCLOSURE**

MERE ENUMERATION OF CYBER RISK FACTORS
NO LONGER ACCEPTABLE

CYBERSECURITY RISKS AND INCIDENTS TO BE REPORTED IF "MATERIAL" TO THE FINANCES OF THE COMPANY

Disclosures to include:

- Frequency of cyber events
- Probability and magnitude of incidents - costs, in financial terms
- Adequacy of controls
- Potential reputational harm
- Potential fines and judgements

Controls and procedures should enable companies to

- *identify cybersecurity risks and incidents,*
- *assess and analyze their impact on a company's business,*
- *evaluate the significance associated with such risks and incidents,*
- *provide for open communications between technical experts and disclosure advisors, and*
- *make timely disclosures regarding such risks and incidents.*

SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures – Feb. 26, 2018

THE COMMUNICATION CHALLENGE

CFO

“How much risk do we have? Are we spending too little or too much on mitigation?”

AUDIT

“Did you fix those high priority issues?”

BOARD/CEO

“We don’t want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?”

CIO

“Are we spending our cybersecurity budget on the right things? What is the ROI?”

CISO

“Εχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό”

A MEASUREMENT EXAMPLE

HOW FAST ARE THEY GOING?

QUALITATIVELY

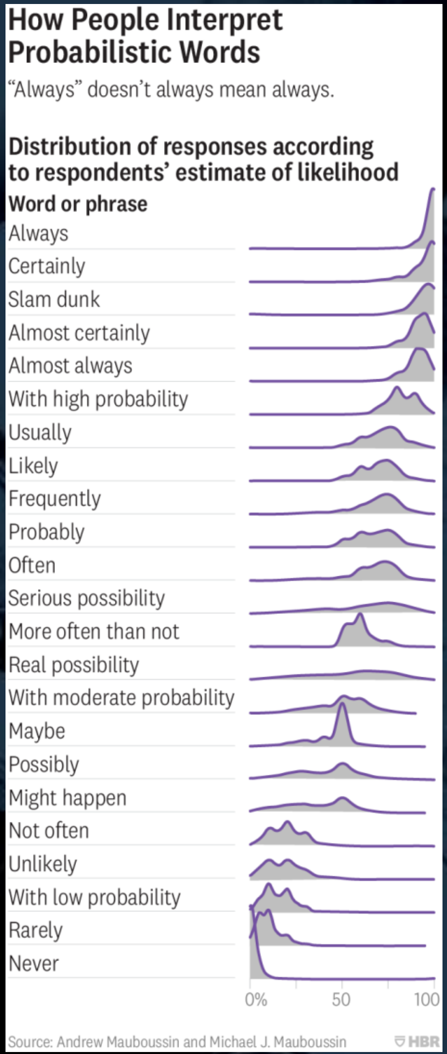
CHALLENGES

- **Is your “fast” the same as mine?**

- **What’s your formula for speed?**
  - Is it the same as mine?

- **Which car am I referring to?**
  - One in particular? (Slowest? Fastest?)
  - An average for all of them?

- **Which part of the track am I referring to?**
  - Corners?
  - The straightaway?
  - Average over the entire track?
  - This lap, or an average for the entire race?



How People Interpret Probabilistic Words

“Always” doesn’t always mean always.

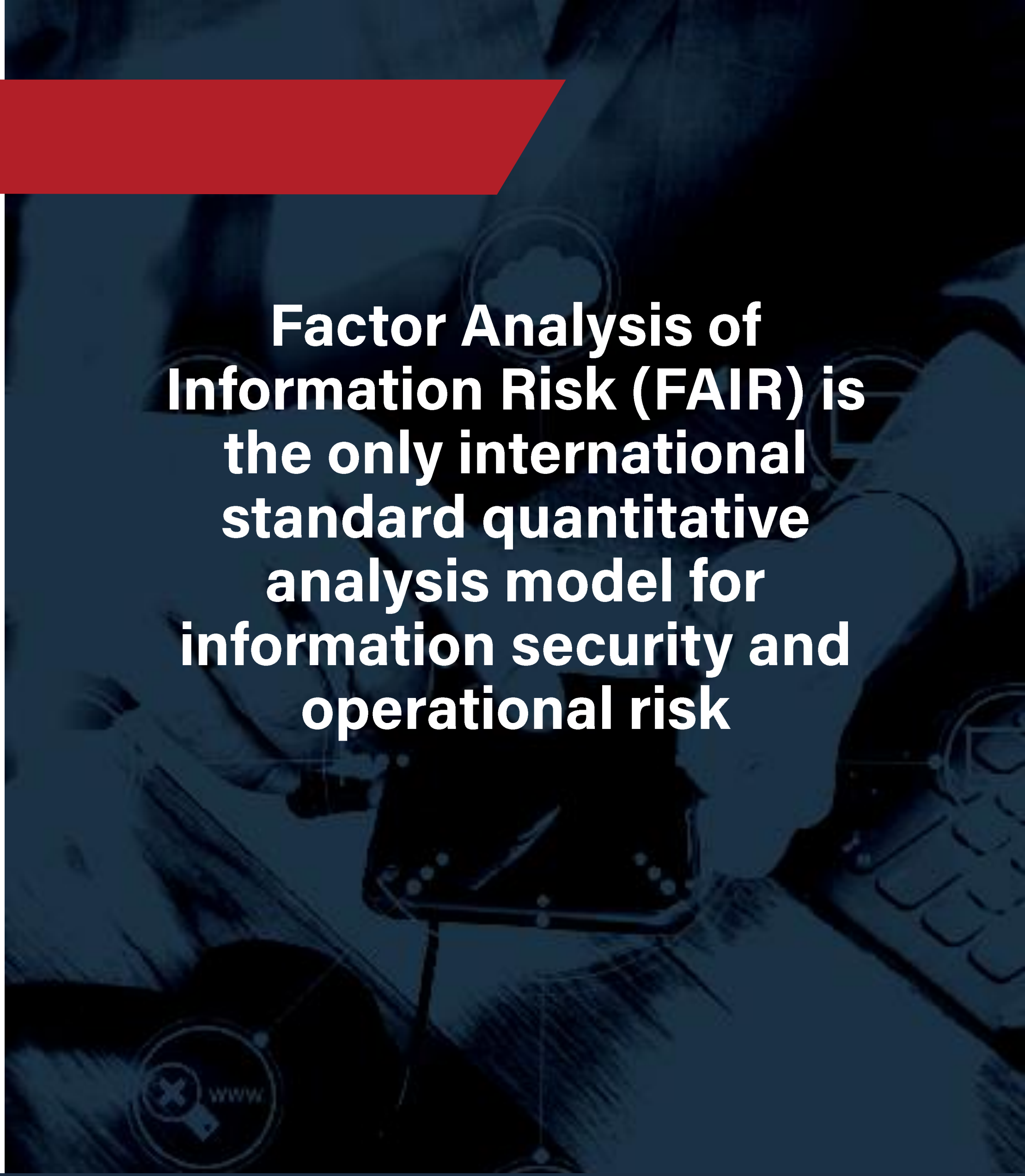
Distribution of responses according to respondents’ estimate of likelihood

Source: Andrew Mauboussin and Michael J. Mauboussin

WHAT DOES FAIR PROVIDE?

- A standard terminology and a taxonomy for information and operational risk

- A methodology for quantifying and managing risk in **financial terms**



Factor Analysis of Information Risk (FAIR) is the only international standard quantitative analysis model for information security and operational risk

FAIR: A WORLDWIDE MOVEMENT TO BETTER CYBER RISK MANAGEMENT

The FAIR Institute is a non-profit expert organization dedicated to enabling business-aligned and cost-effective risk management

Based on the Open FAIR Standard

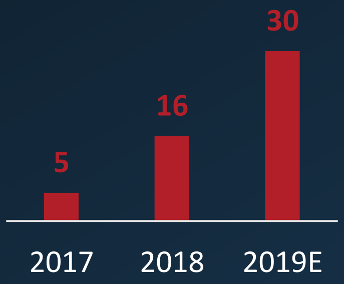
Education | Collaboration | Best Practices

7,300+
Members

17 Local Chapters

5 Workgroups

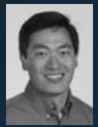
Universities offering FAIR courses



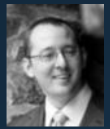
Leadership & Board Members

Jack Jones
Chairman, FAIR Institute
EVP R&D RiskLens

Bill Barouski
Deputy CISO Northern Trust
Fmr. CISO Federal Reserve



Sounil Yu
SVP, Head of R&D Security
Bank of America



Evan Wheeler
VP Risk Mgmt. & CISO
Financial Engines

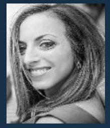
Chris Porter
CISO
Fannie Mae

Dmitry Kuchynski
Principal. Managing Director
Cisco Security Solutions

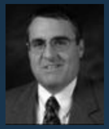
Donna Gallaher
CEO
New Ocean Enterprises

Kim Jones
Director Security Ops
Intuit

Wade Baker
Founder Cyentia Institute
Prof. Integrated Security, VA Tech



Simone Petrella
CEO
CyberVista

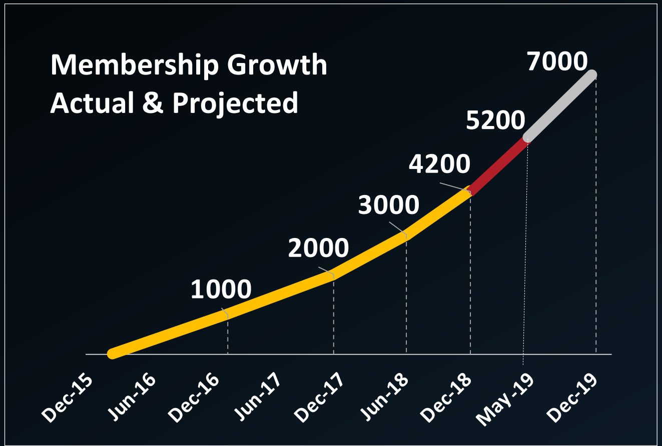


Jim Hietala
VP Security
The Open Group

Nicola (Nick) Sanna
President FAIR Institute
CEO RiskLens

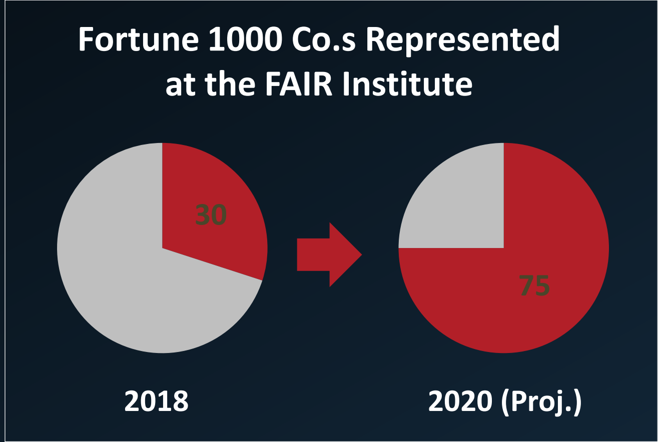
A COMMUNITY OF FORWARD THINKING EXPERTS

STRONG MEMBERSHIP GROWTH



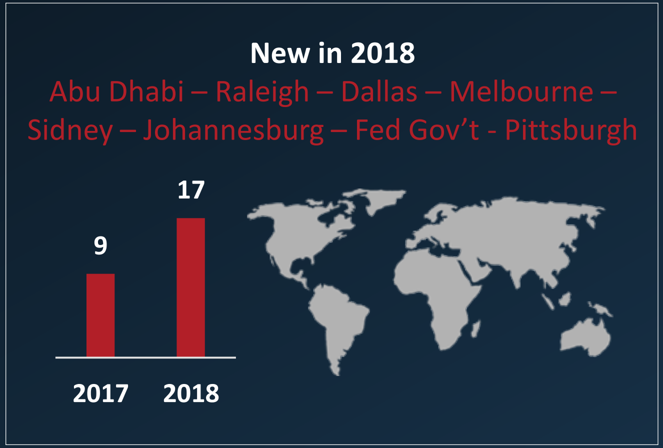
Membership Growth
Actual & Projected

FAIR EMERGING AS RISK MODEL OF CHOICE



Fortune 1000 Co.s Represented at the FAIR Institute

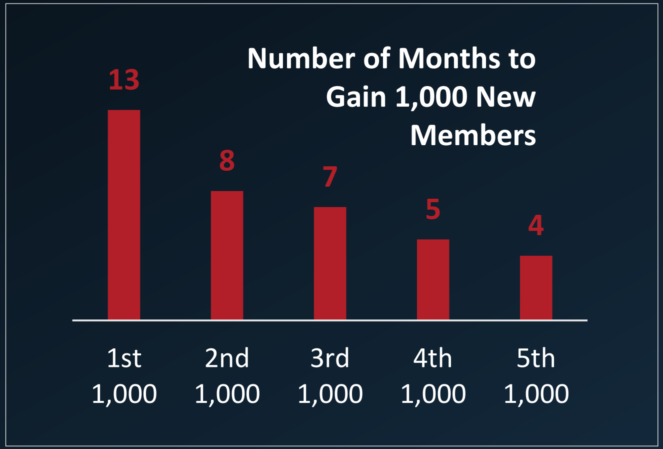
LOCAL CHAPTERS MULTIPLYING



New in 2018

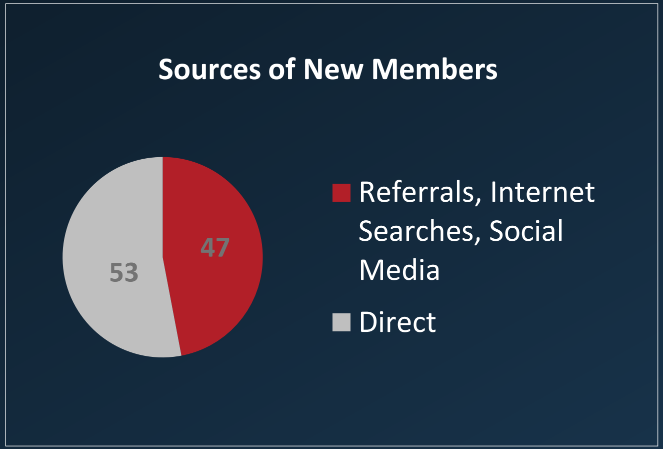
Abu Dhabi – Raleigh – Dallas – Melbourne – Sidney – Johannesburg – Fed Gov't - Pittsburgh

VELOCITY INCREASING



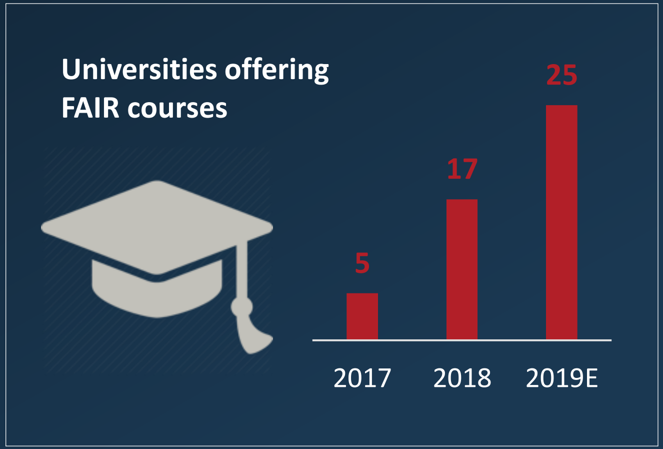
Number of Months to Gain 1,000 New Members

FAIR SPREADING VIRALLY



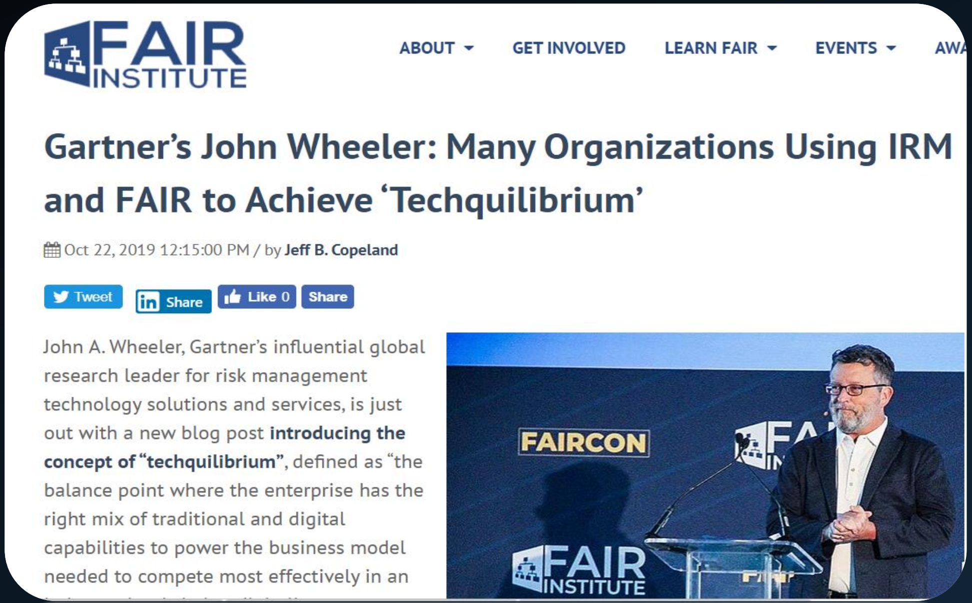
Sources of New Members

FORMING THE NEXT-GENERATION OF LEADERS



Universities offering FAIR courses

GARTNER GOING ON RECORD FOR RISK QUANTIFICATION



Gartner's John Wheeler: Many Organizations Using IRM and FAIR to Achieve 'Techquilibrium'

Oct 22, 2019 12:15:00 PM / by **Jeff B. Copeland**

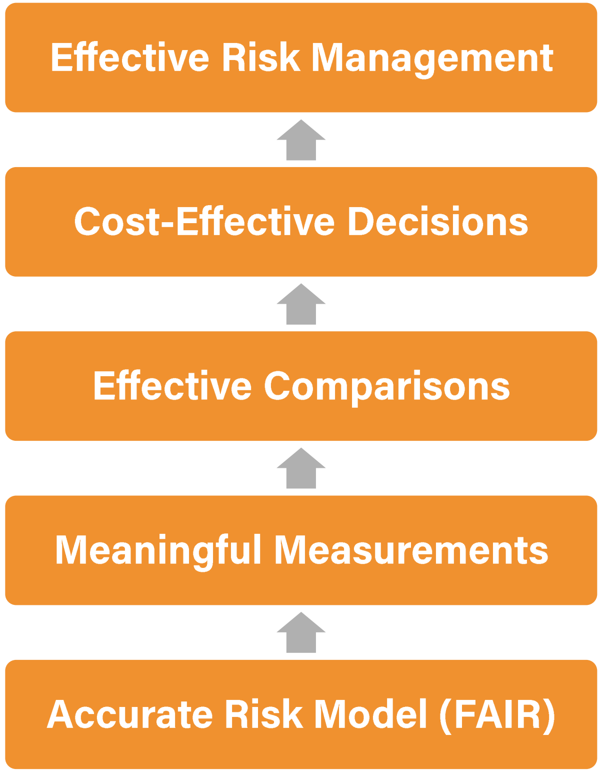
John A. Wheeler, Gartner's influential global research leader for risk management technology solutions and services, is just out with a new blog post **introducing the concept of "techquilibrium"**, defined as "the balance point where the enterprise has the right mix of traditional and digital capabilities to power the business model needed to compete most effectively in an

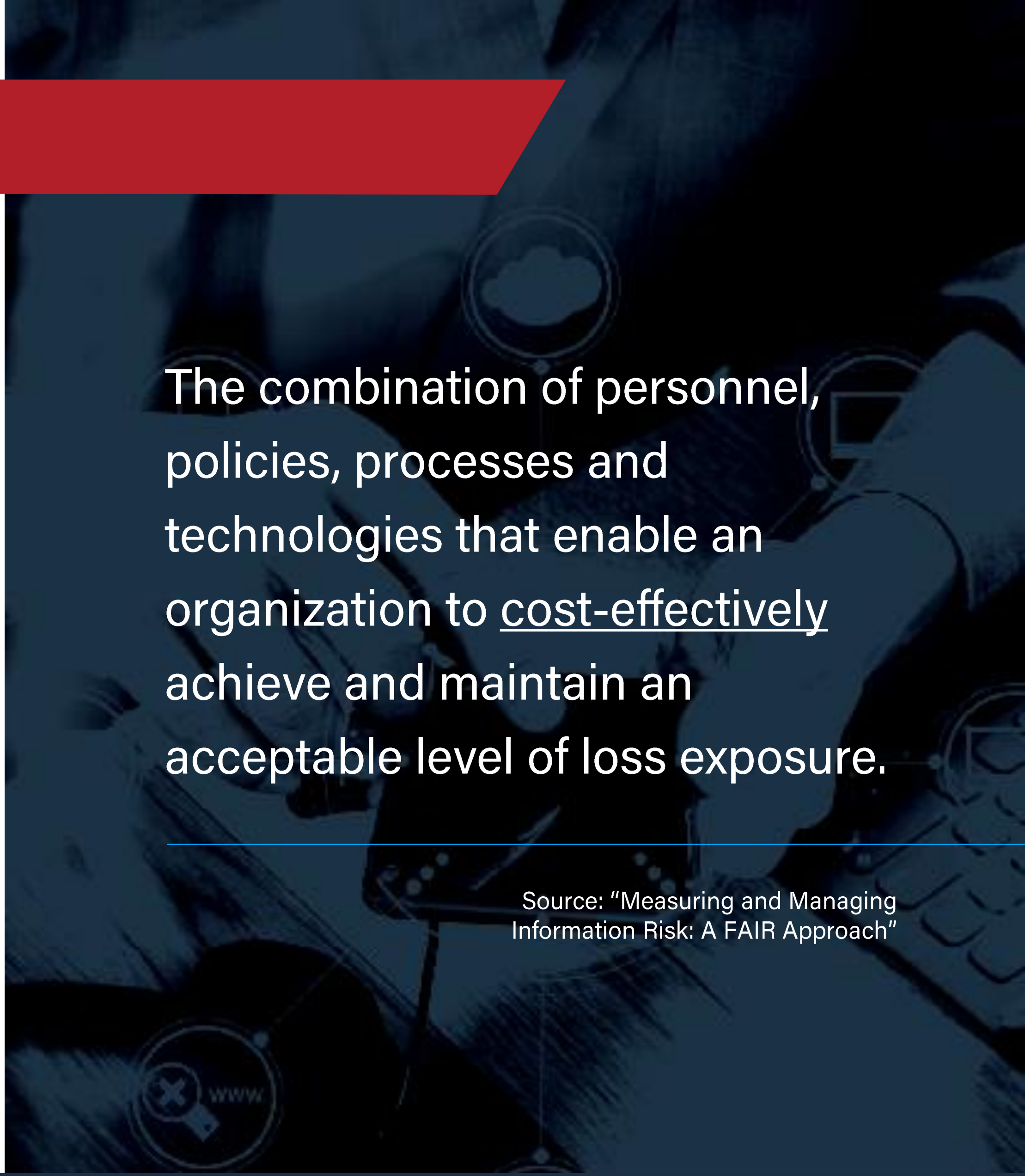
https://www.fairinstitute.org/blog/gartners-john-wheeler-many-organizations-using-irm-and-fair-to-achieve-techquilibrium

"This new state of techquilibrium demands an understanding of both the quantitative and qualitative elements of digital risk."

"Many organizations are now utilizing IRM and FAIR to create risk treatment plans for potential data breach events as they optimize their business" – and beyond the tactical level to the strategic to "develop a successful case for digital transformation."

EFFECTIVE RISK MANAGEMENT





The combination of personnel, policies, processes and technologies that enable an organization to <u>cost-effectively</u> achieve and maintain an acceptable level of loss exposure.

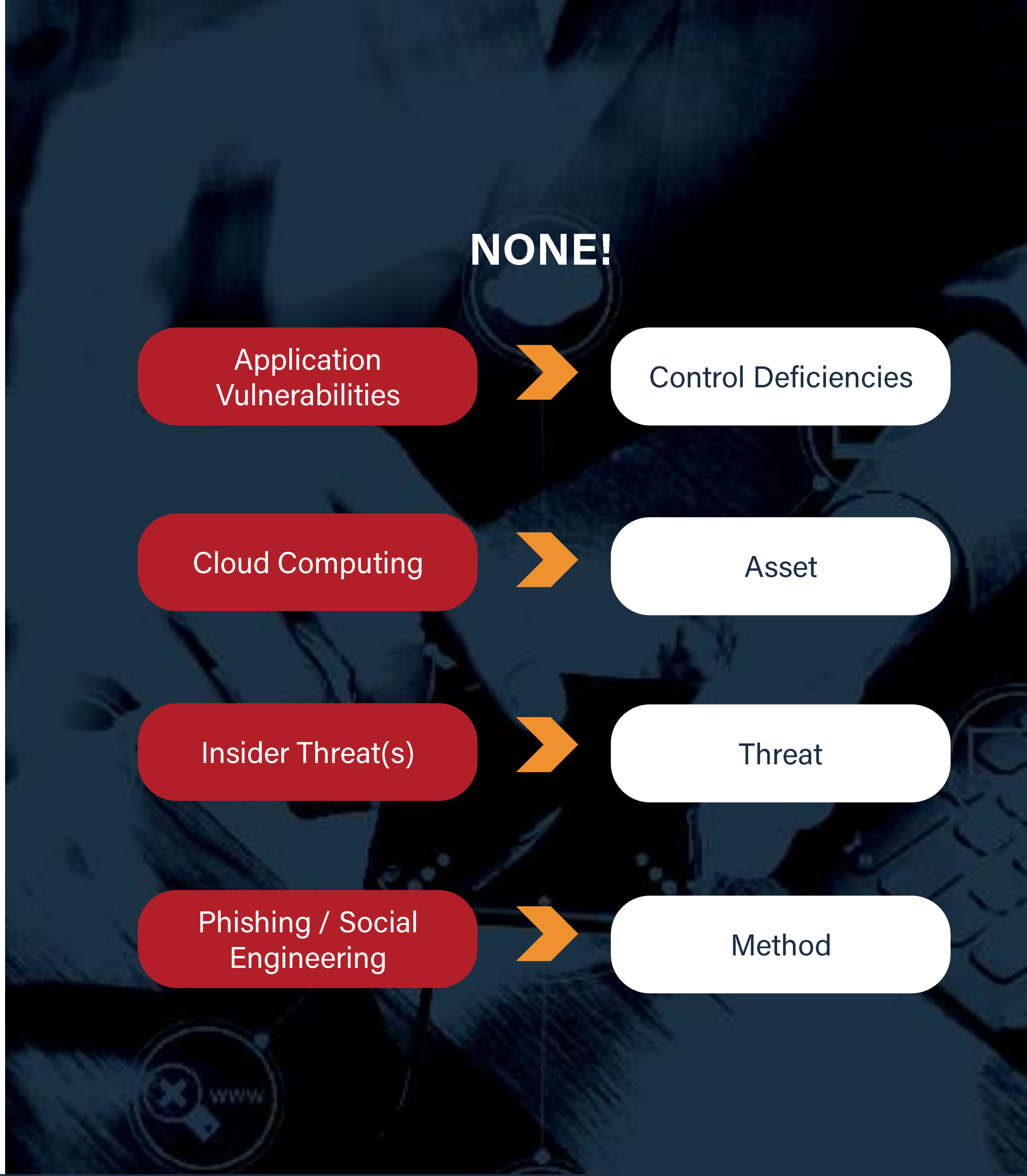
Source: “Measuring and Managing Information Risk: A FAIR Approach”

RISK MODELS MATTER

Which Of These Are **Risks?**

- Point of Sale Attacks
- Cloud Computing
- Insider Threat(s)
- Cyber Criminals
- Application Vulnerabilities
- Hacktivists
- Phishing / Social Engineering
- Third-party Risk
- Mobile Malware
- Business Continuity

Typical Top 10 Technology Risk List



NONE!

Application Vulnerabilities → Control Deficiencies

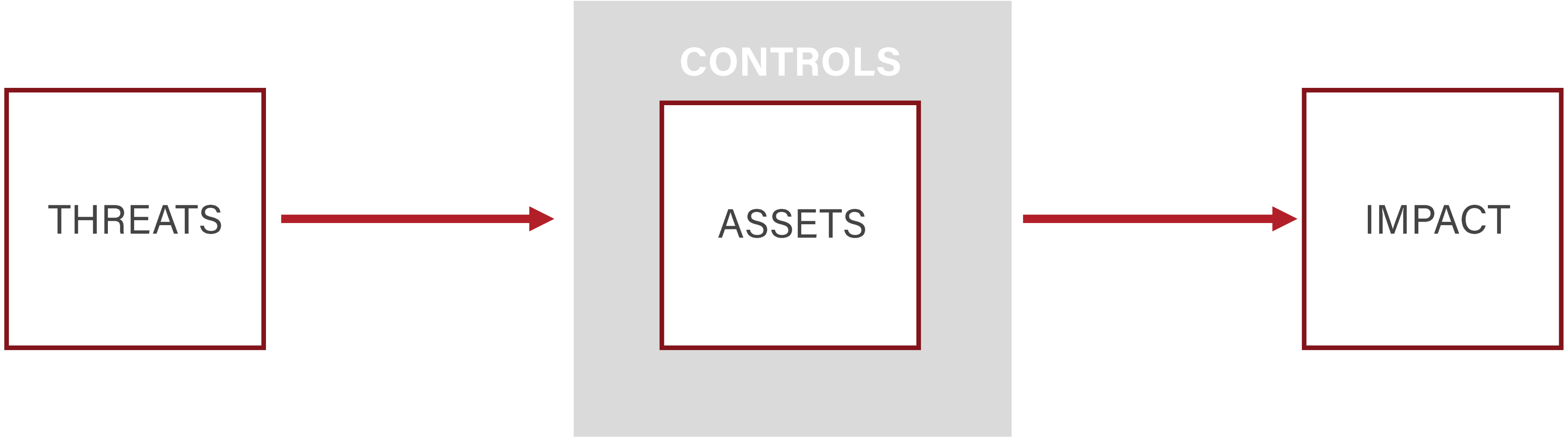
Cloud Computing → Asset

Insider Threat(s) → Threat

Phishing / Social Engineering → Method

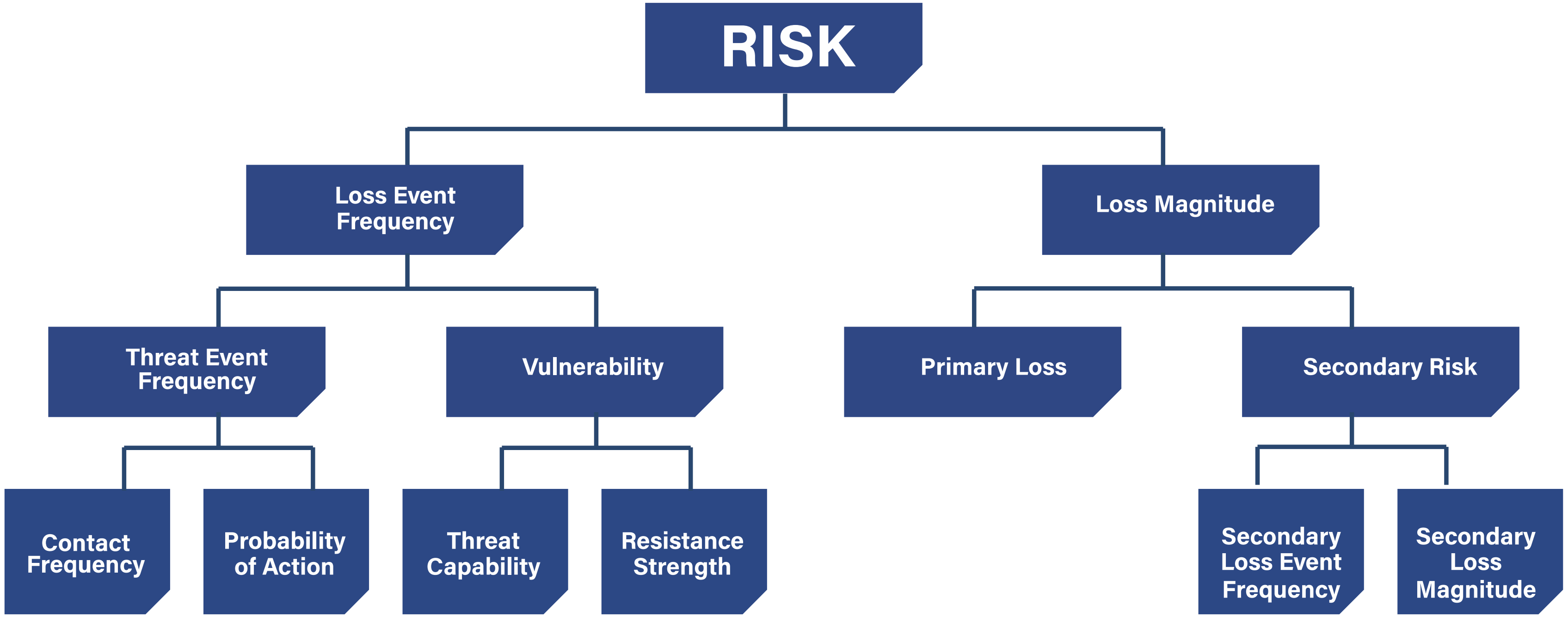
FAIR: A STANDARD RISK SCOPING MODEL

WE CAN ONLY ASSESS THE RISK OF LOSS EVENTS



RISK (LOSS EXPOSURE) SCENARIO

FAIR: A STANDARD RISK ANALYTICS MODEL



- RISK
  - Loss Event Frequency
    - Threat Event Frequency
      - Contact Frequency
      - Probability of Action
    - Vulnerability
      - Threat Capability
      - Resistance Strength
  - Loss Magnitude
    - Primary Loss
    - Secondary Risk
      - Secondary Loss Event Frequency
      - Secondary Loss Magnitude

Accredited as an Industry Standard by

THE Open GROUP

Complementary to Risk Frameworks

ISO 27001 Information Security Management Certified

NIST

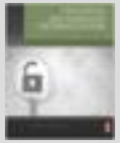
Supported by a Fast Growing Community

FAIR INSTITUTE

Wide Industry Adoption 30% Fortune 1000

FORTUNE 1000

FAIR Book Inducted in Cybersecurity Canon

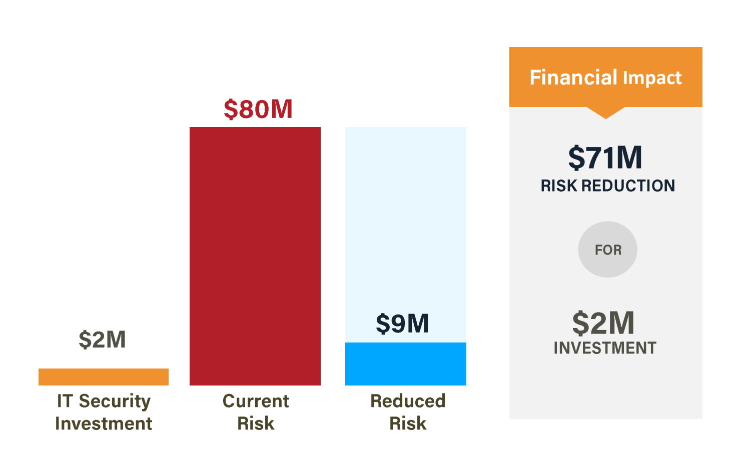


FAIR INSTITUTE RiskLens®

MULTIPLE DIMENSIONS OF ROI

USE CASES	ROI
Understand Loss Exposure	Preserve Value
Prioritize Risk Mitigations	Maximize Risk Reduction
Assess ROI of Security Initiatives	Optimize Cybersecurity Investments
Meet Cyber Regulations	Pass Compliance Audit
Optimize Cyber Insurance Coverage	Facilitate Risk Transfer

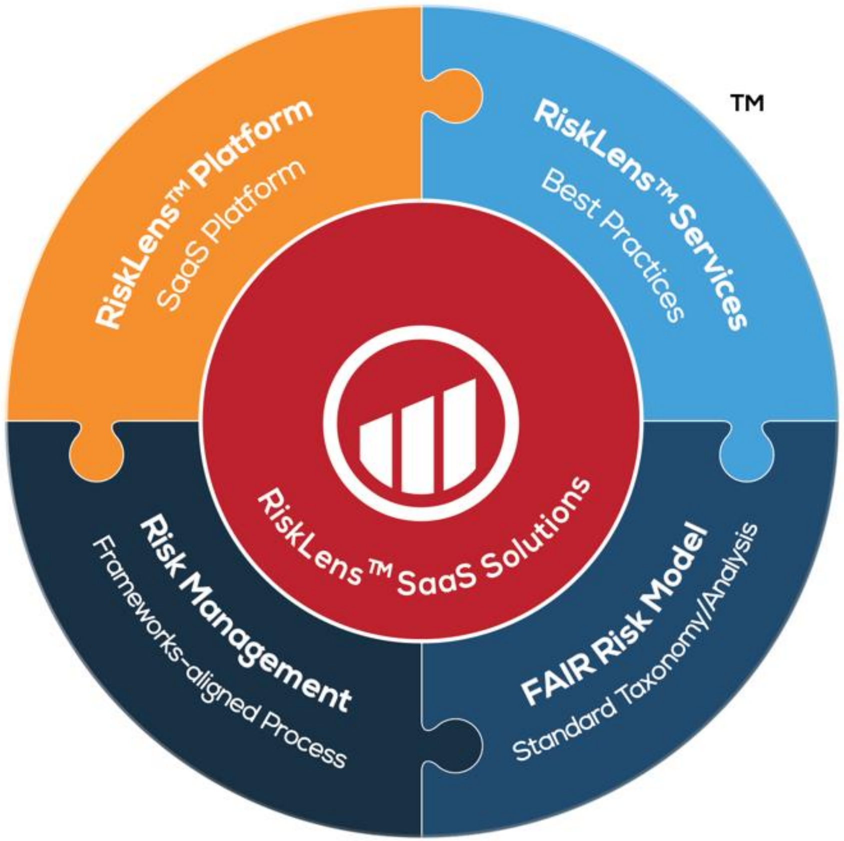
DRIVING SMARTER DECISIONS THAT ENHANCE BUSINESS RESILIENCE



RISKLENS EXTENDS FAIR FOR ENTERPRISE ADOPTION

RiskLens - author of FAIR, Technical Advisor of the FAIR Institute, expert solutions provider to the Fortune 1000

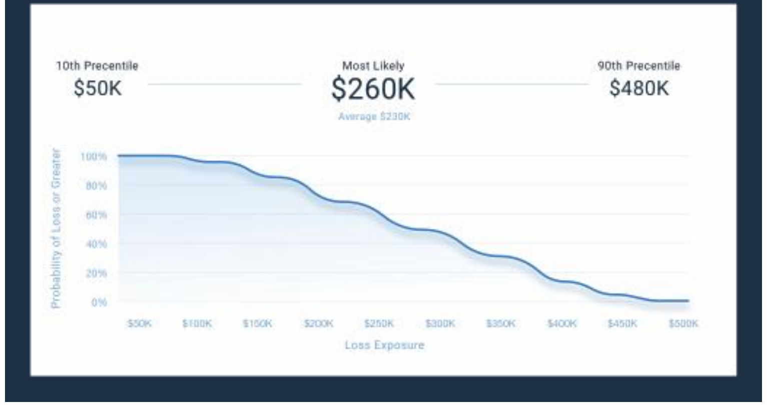
Standardized the best practices for enterprise adoption of FAIR into a suite of SaaS Solutions based on the **RiskLens FAIR Enterprise Model™ (RF-EM™)**



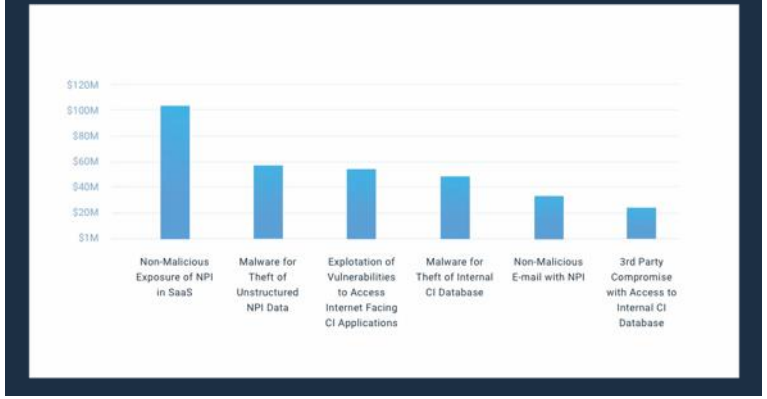
The RiskLens FAIR Enterprise Model™ (RF-EM™) Components

DRIVE BETTER COMMUNICATION & DECISION MAKING

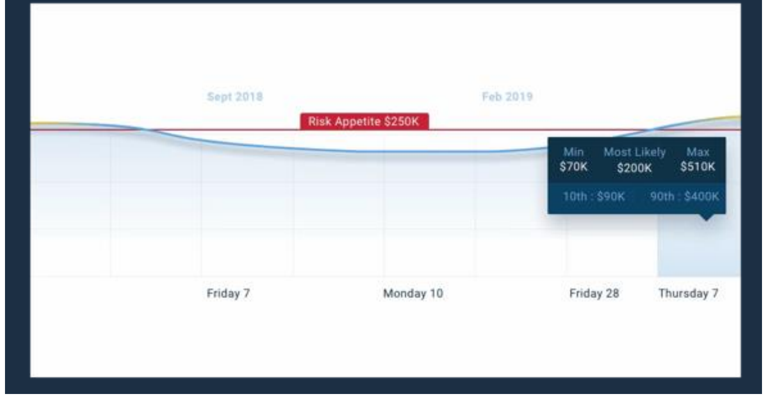
HOW MUCH RISK DO WE HAVE?



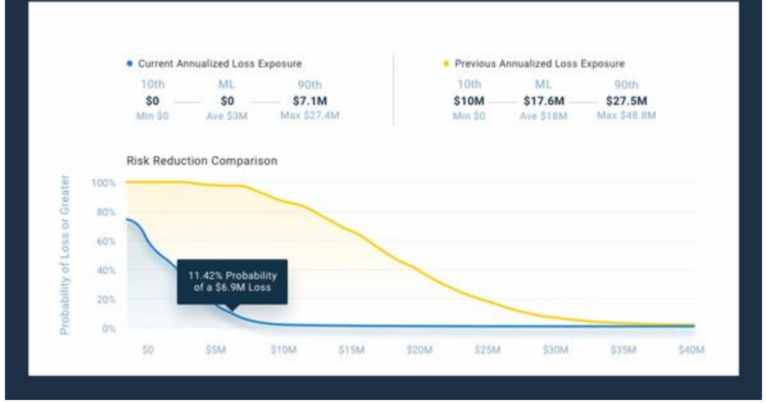
WHAT ARE OUR TOP RISKS?



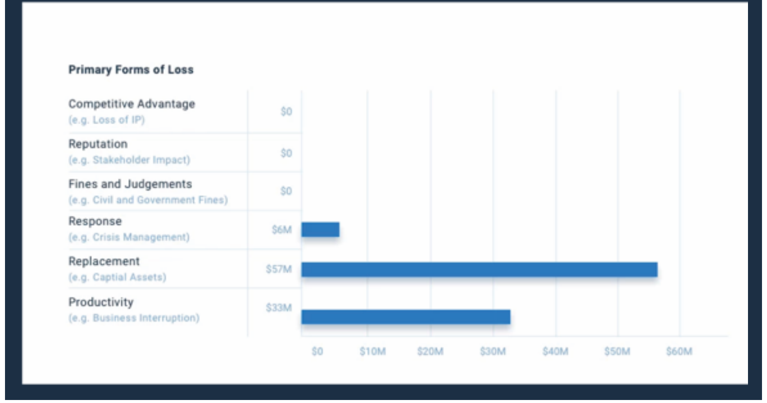
HOW IS RISK TRENDING VS APPETITE?



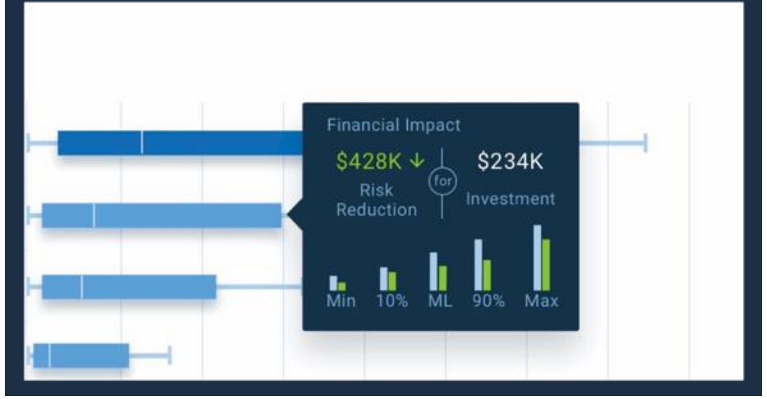
HAVE WE REDUCED RISK?



WHAT TYPES OF LOSS CAN WE EXPECT?

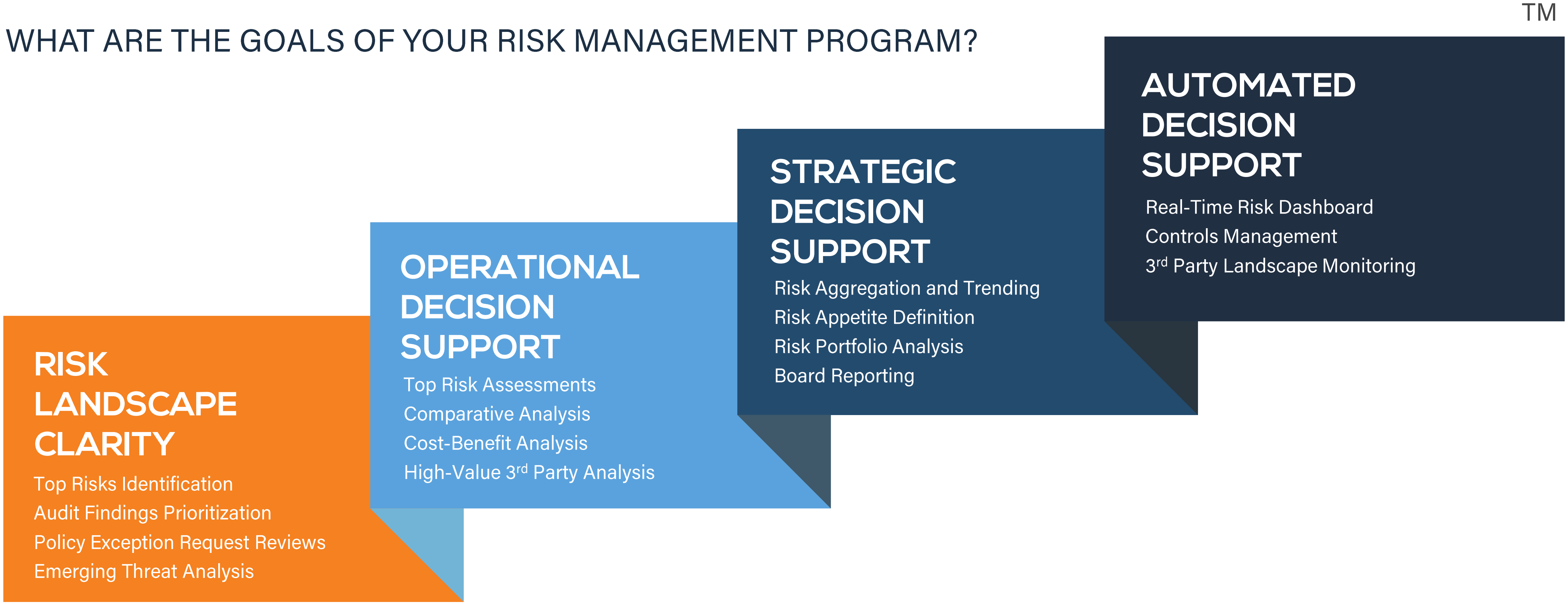


WHAT IS THE COST-BENEFIT OF THIS PROJECT?



RISK MANAGEMENT PROGRAM MATURITY

WHAT ARE THE GOALS OF YOUR RISK MANAGEMENT PROGRAM?



TM

RISK LANDSCAPE CLARITY

Top Risks Identification
Audit Findings Prioritization
Policy Exception Request Reviews
Emerging Threat Analysis

OPERATIONAL DECISION SUPPORT

Top Risk Assessments
Comparative Analysis
Cost-Benefit Analysis
High-Value 3rd Party Analysis

STRATEGIC DECISION SUPPORT

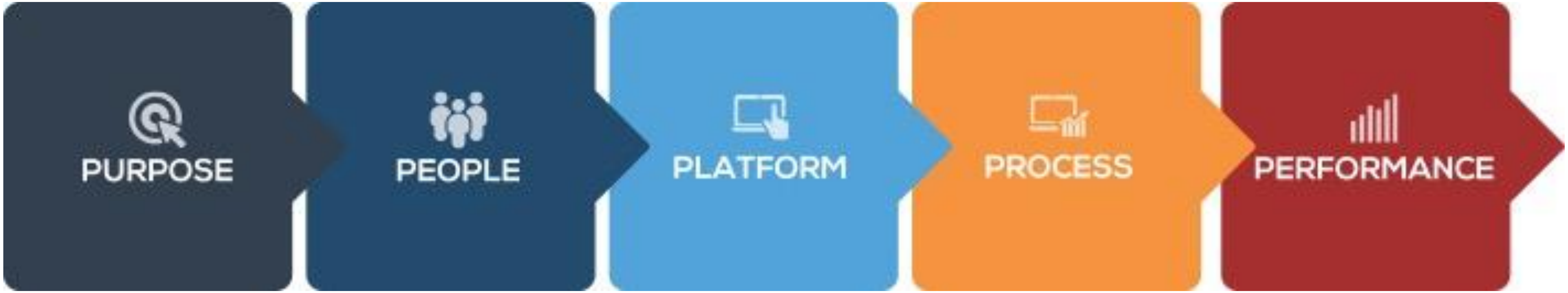
Risk Aggregation and Trending
Risk Appetite Definition
Risk Portfolio Analysis
Board Reporting

AUTOMATED DECISION SUPPORT

Real-Time Risk Dashboard
Controls Management
3rd Party Landscape Monitoring

Source: RiskLens FAIR Enterprise Model^{TM}

QUANTITATIVE RISK MANAGEMENT PROGRAM



PURPOSE	PEOPLE	PLATFORM	PROCESS	PERFORMANCE
PROGRAM GOALS	QUANTITATIVE (FAIR) FUNDAMENTALS	ONBOARDING	CROWN JEWELS & TOP RISKS IDENTIFICATION	RISK APPETITE
ROLES & RESPONSIBILITES	RISK ANALYST TRAINING	CONFIGURATION	TOP QUANTITATIVE RISK ASSESSMENTS	MONITORING & REPORTING
DEPENDENCIES	ORIENTATION & AWARENESS	DATA LIBRARIES	RISK ASSESSMENT WORKFLOWS	PROGRAM SUCCESS

Source: RiskLens FAIR Enterprise Model^{TM}

CYBER RISK ECONOMICS IS HERE

Privacy and Computer Security Issues: A State Enforcement Perspective

Gene Fishel

Senior Assistant Attorney General Chief,

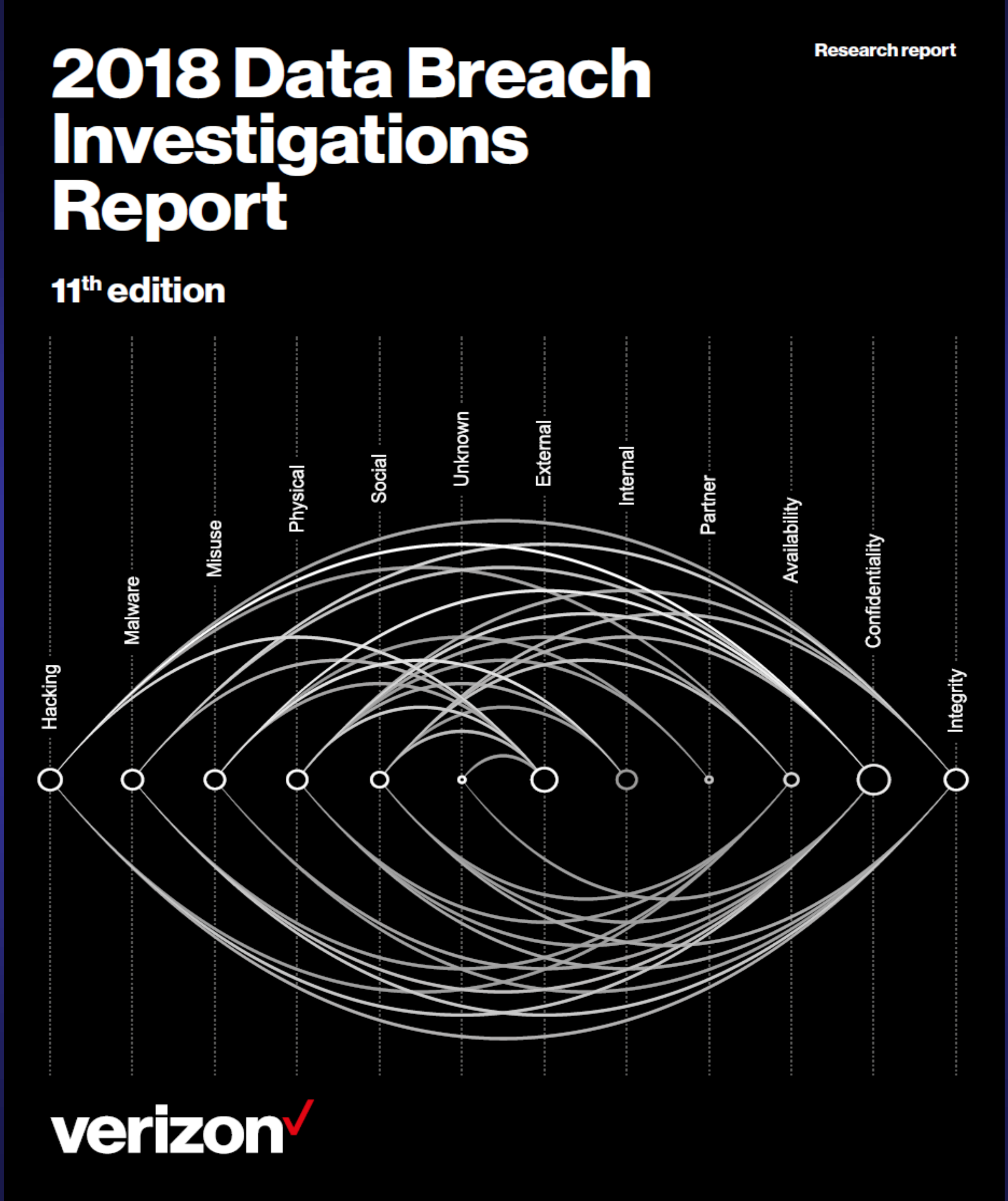
Computer Crime Section

Virginia Attorney General’s Office

Outline

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

Database breaches



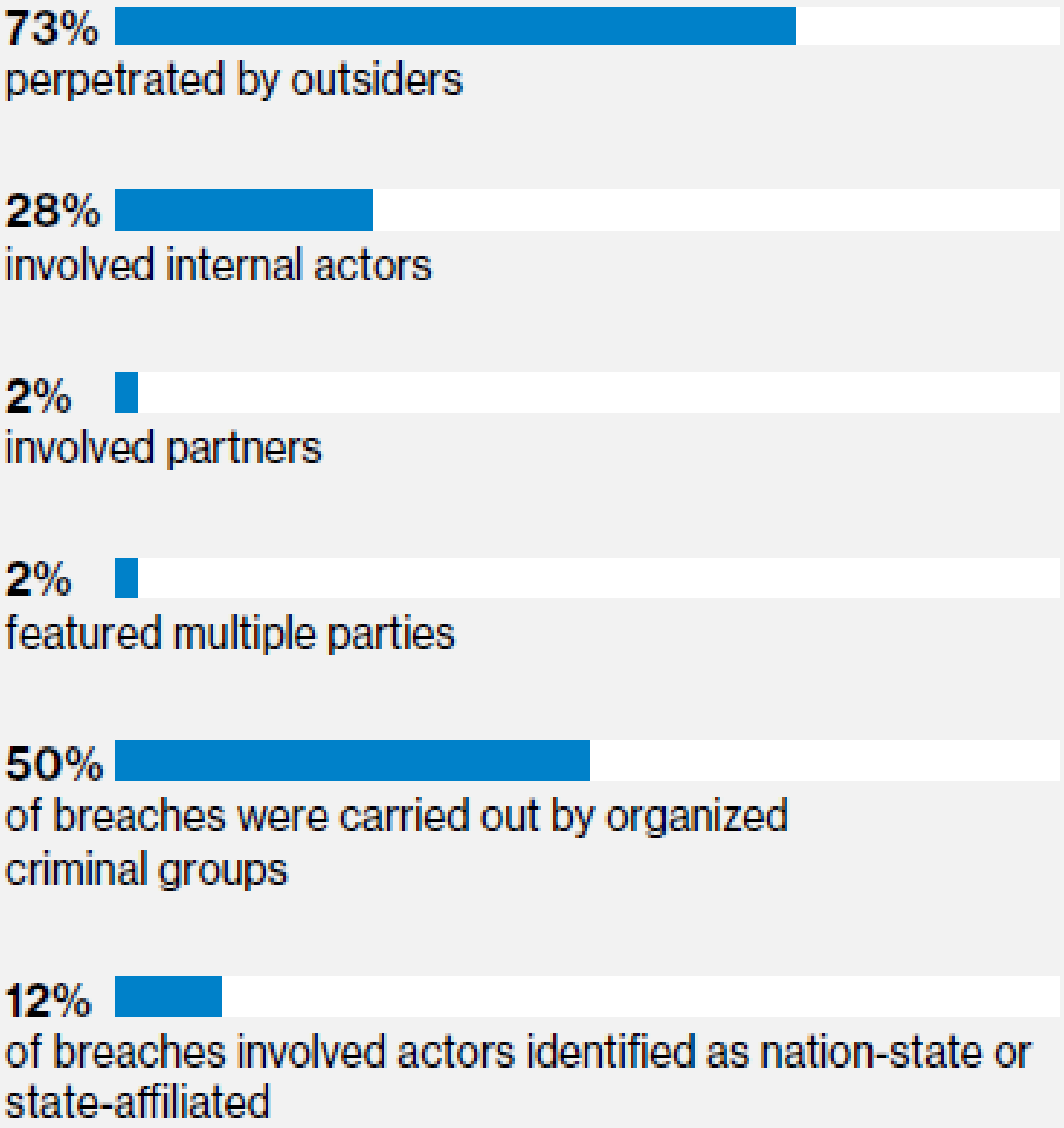
Research report

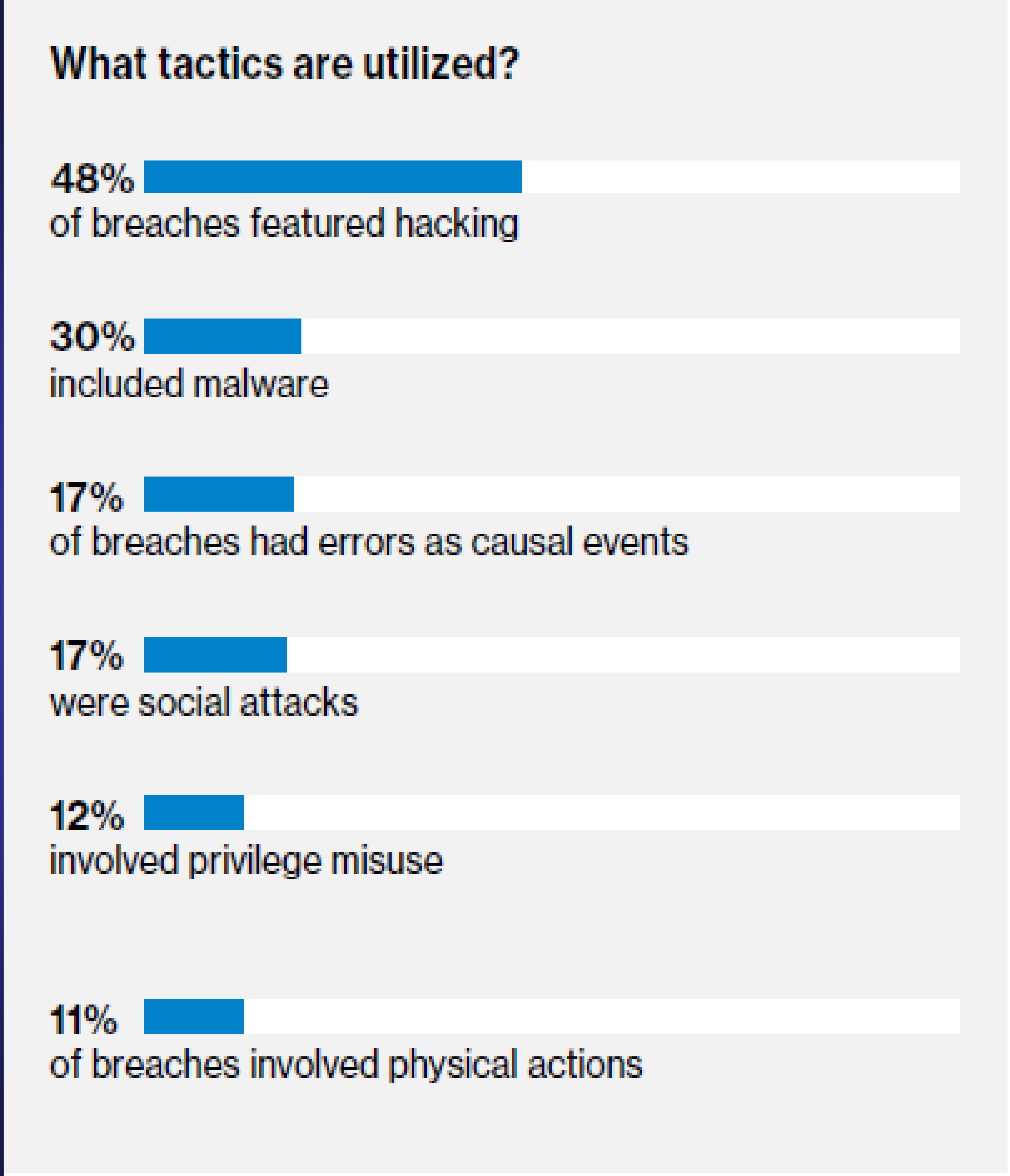
2018 Data Breach Investigations Report

11th edition

verizon

Who's behind the breaches?





What tactics are utilized?

48% of breaches featured hacking

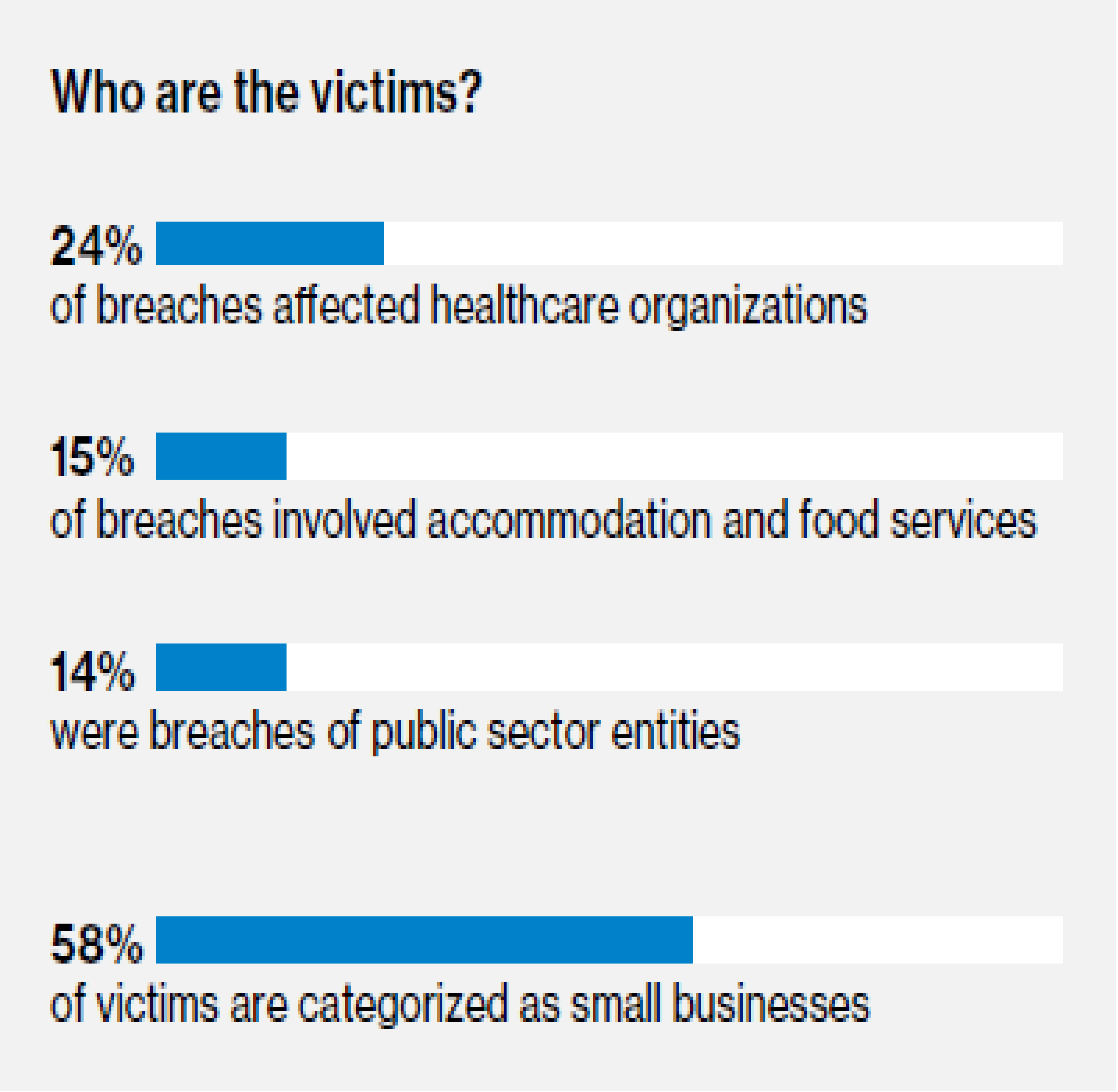
30% included malware

17% of breaches had errors as causal events

17% were social attacks

12% involved privilege misuse

11% of breaches involved physical actions



Who are the victims?

24%
of breaches affected healthcare organizations

15%
of breaches involved accommodation and food services

14%
were breaches of public sector entities

58%
of victims are categorized as small businesses

Database breach laws

- 50 state laws +
- Virginia Code §18.2-186.6
- Pertinent provisions
  - 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 name, SSN, financial acct/credit card numbers along with access code, driver’s license number
  - Tax identification numbers and tax withheld (to counter prevalent payroll breaches / IRS scams)
  - July 1 = 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

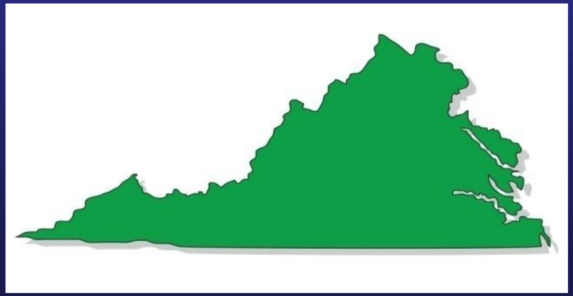
- Pertinent provisions
  - Notice must include:
    - Incident in general terms
    - Type of information accessed
    - The general acts of entity to prevent further unauthorized access
    - Telephone number for affected persons to call
    - Advice directing person to remain vigilant of accounts and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

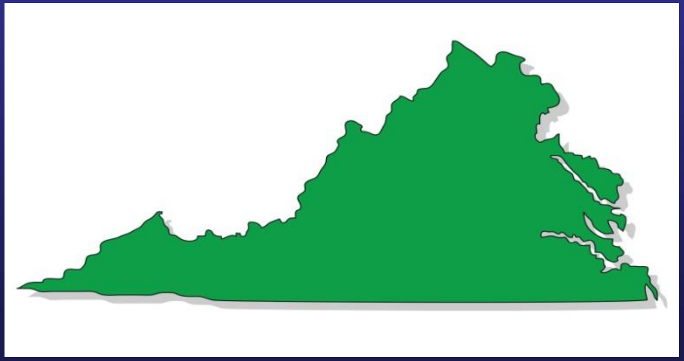
Enforcer's perspective

- 950 database breach notices received in VA in 2019 (767 in 2018)
- Broad cross-section of industry
- Lost equipment, theft, intrusion are most common occurrences
- Small breaches dominate



Enforcer’s perspective

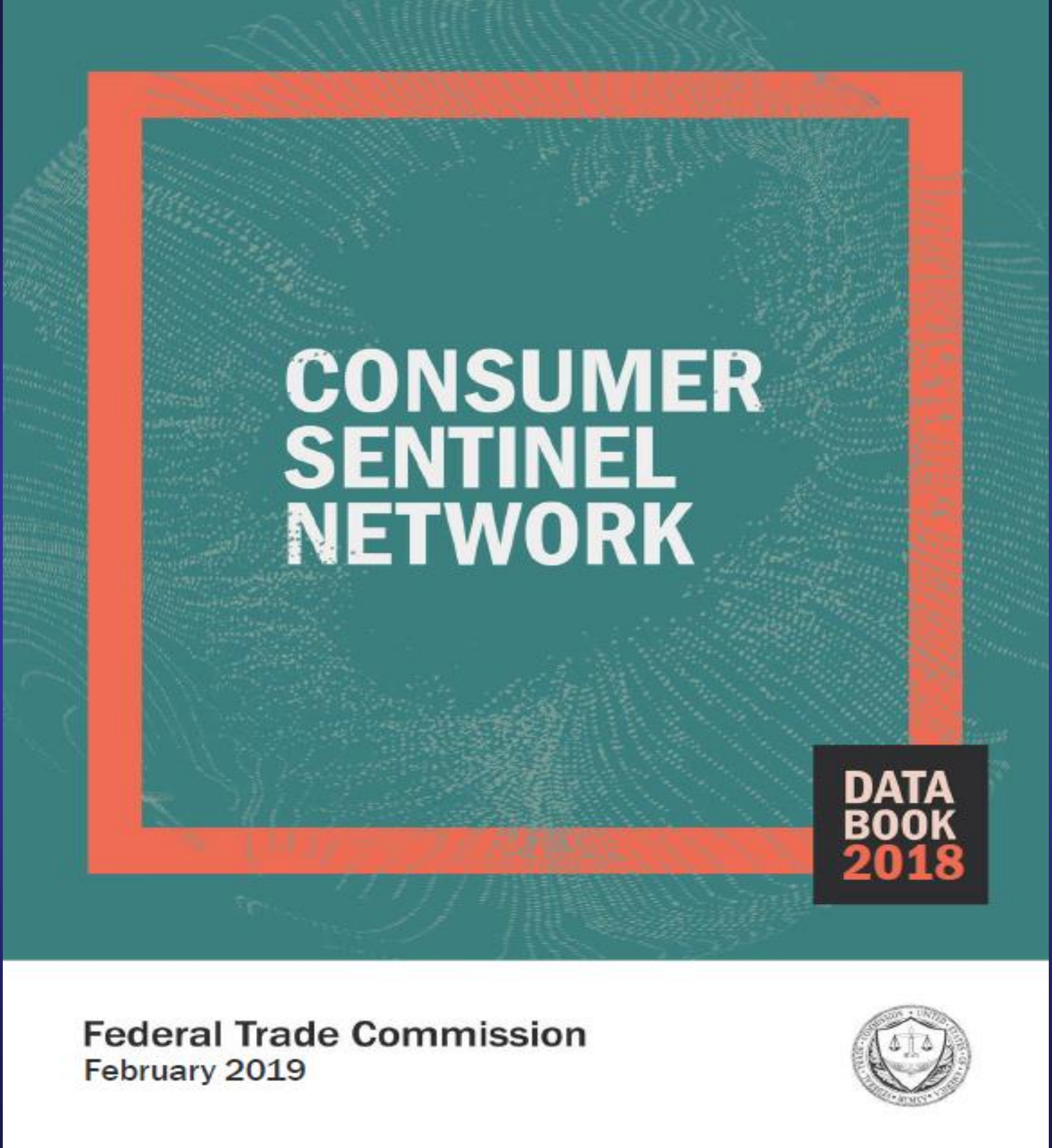
- From one resident to over 1 million residents affected in a single breach
- Work with your attorneys
- Contact law enforcement
- Work with our office



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

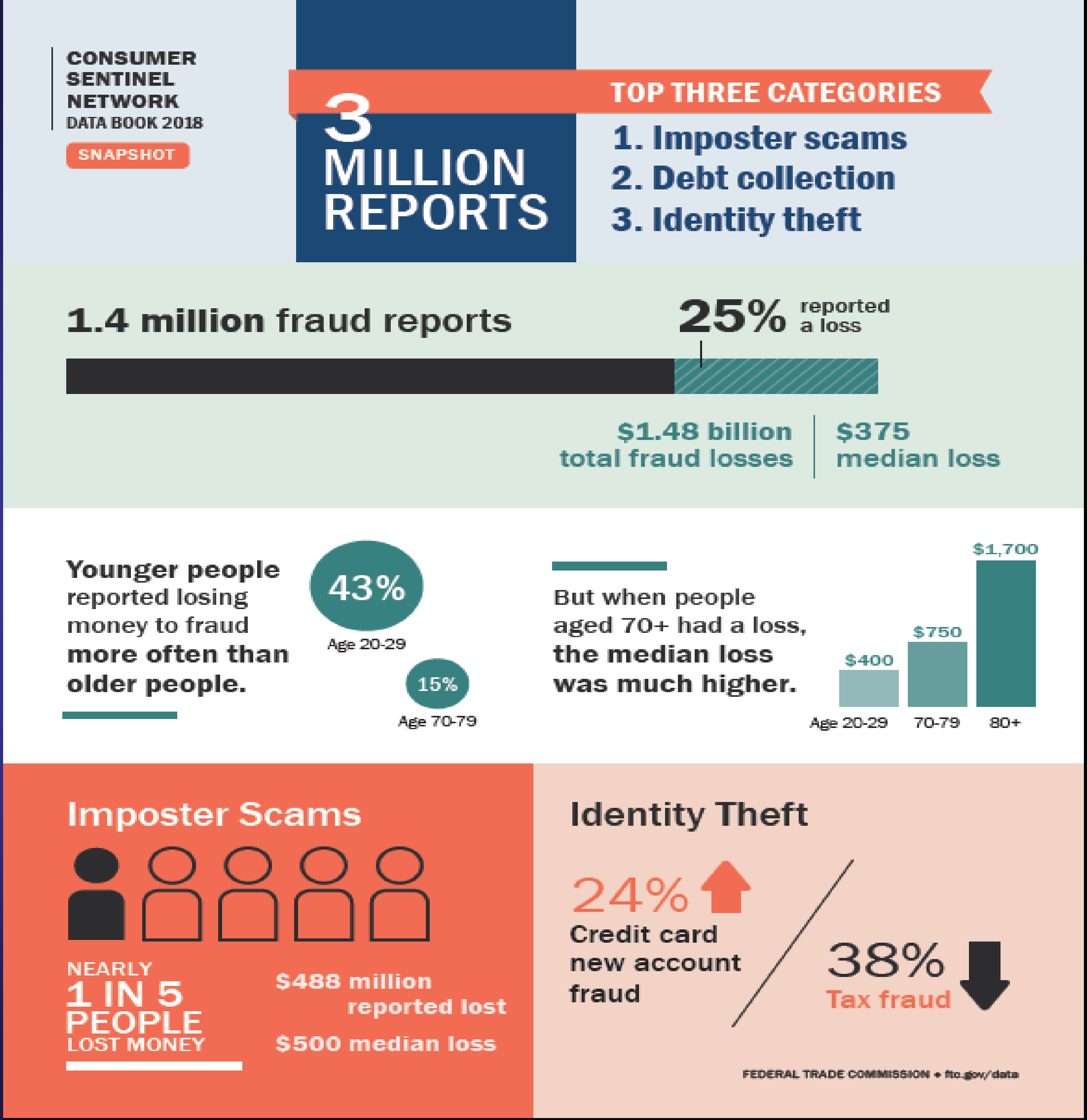
Identity theft



CONSUMER SENTINEL NETWORK

DATA BOOK 2018

Federal Trade Commission
February 2019



CONSUMER SENTINEL NETWORK
DATA BOOK 2018

SNAPSHOT

3 MILLION REPORTS

TOP THREE CATEGORIES

1. Imposter scams
2. Debt collection
3. Identity theft

1.4 million fraud reports

25% reported a loss

$1.48 billion total fraud losses

$375 median loss

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

43%
Age 20-29

15%
Age 70-79

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

Age 20-29	70-79	80+
$400	$750	$1,700

Imposter Scams

NEARLY
1 IN 5
PEOPLE
LOST MONEY

$488 million reported lost

$500 median loss

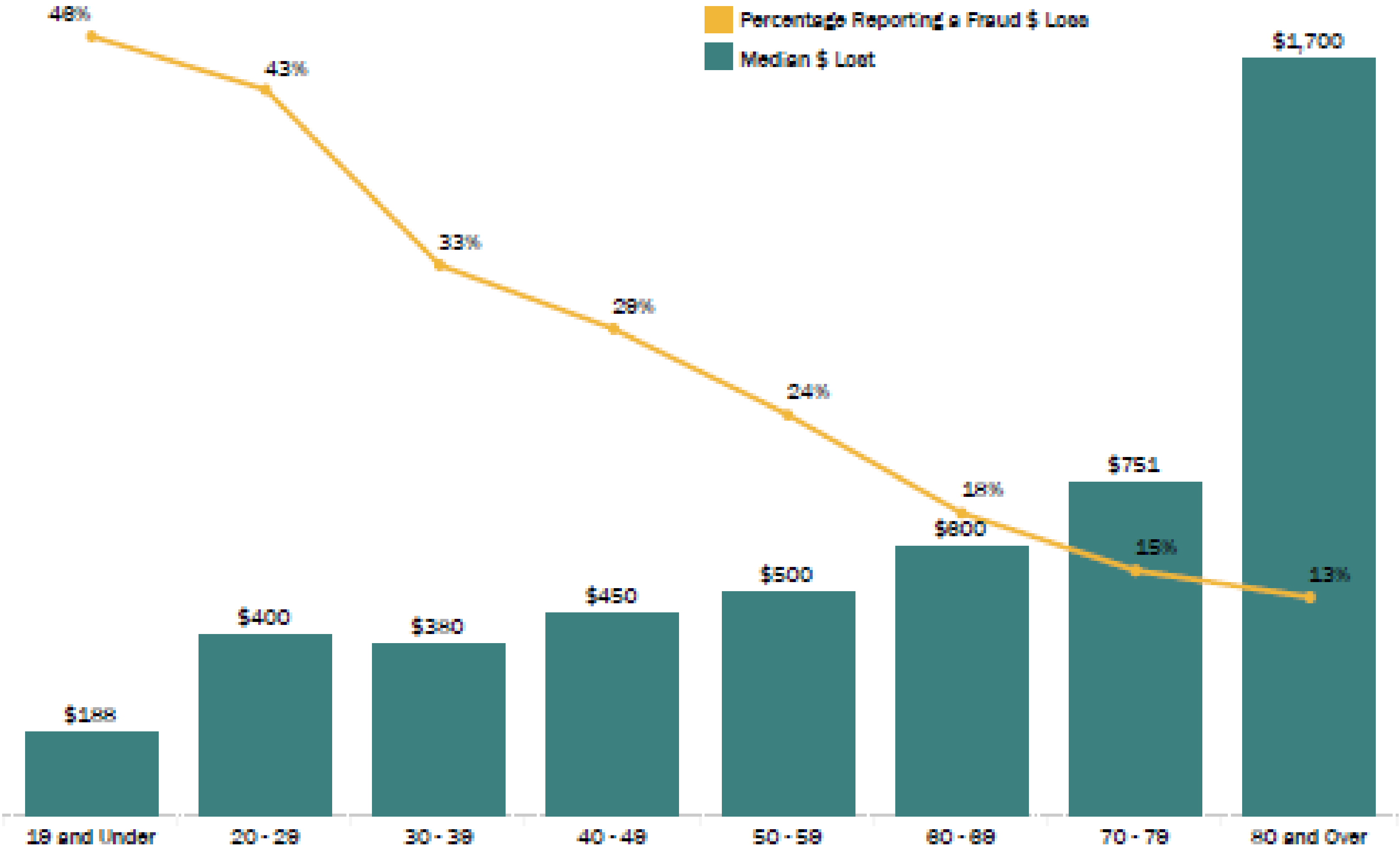
Identity Theft

24%
Credit card new account fraud

38%
Tax fraud

FEDERAL TRADE COMMISSION • ftc.gov/data

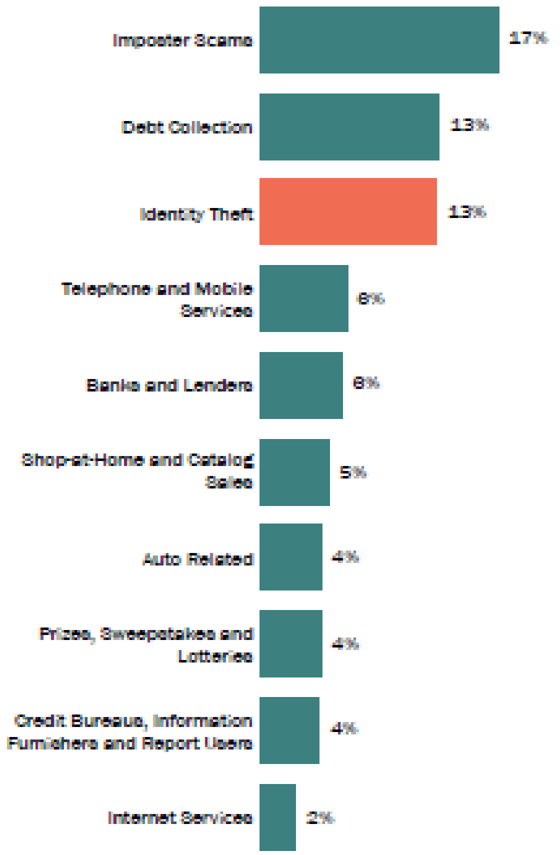
Percentage Reporting a Fraud Loss and Median Loss by Age



Of the 1,427,561 total fraud reports in 2018, 46% included consumer age information.

Virginia

Top Ten Report Categories



Fraud & Other Reports

13th

State Rank
(Reports per 100K Population)

56,135

Total Fraud & Other Reports

Fraud Losses

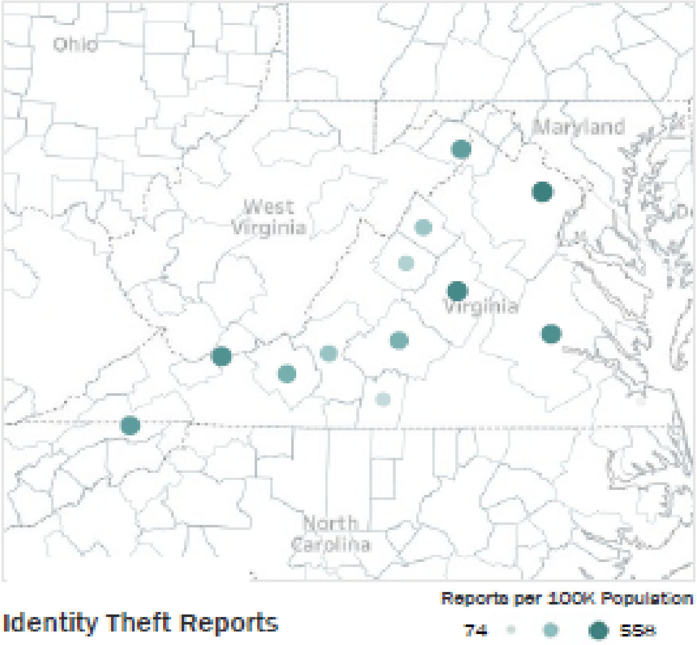
$28.0M

Total Fraud Losses

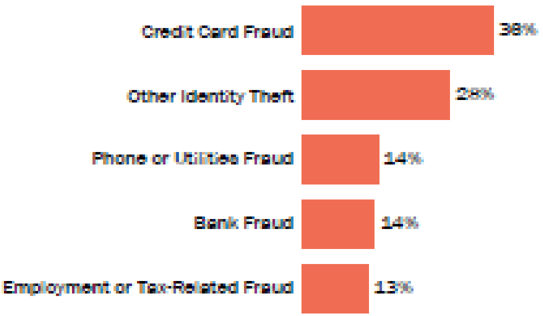
$368

Median Fraud Losses

Fraud & Other Reports by Metropolitan Area



Top Identity Theft Types



Identity Theft Reports

25th

State Rank
(Reports per 100K Population)

8,196

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, one to five years imprisonment
- If 50 or more person's identifying info stolen, one to five years
- One to 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

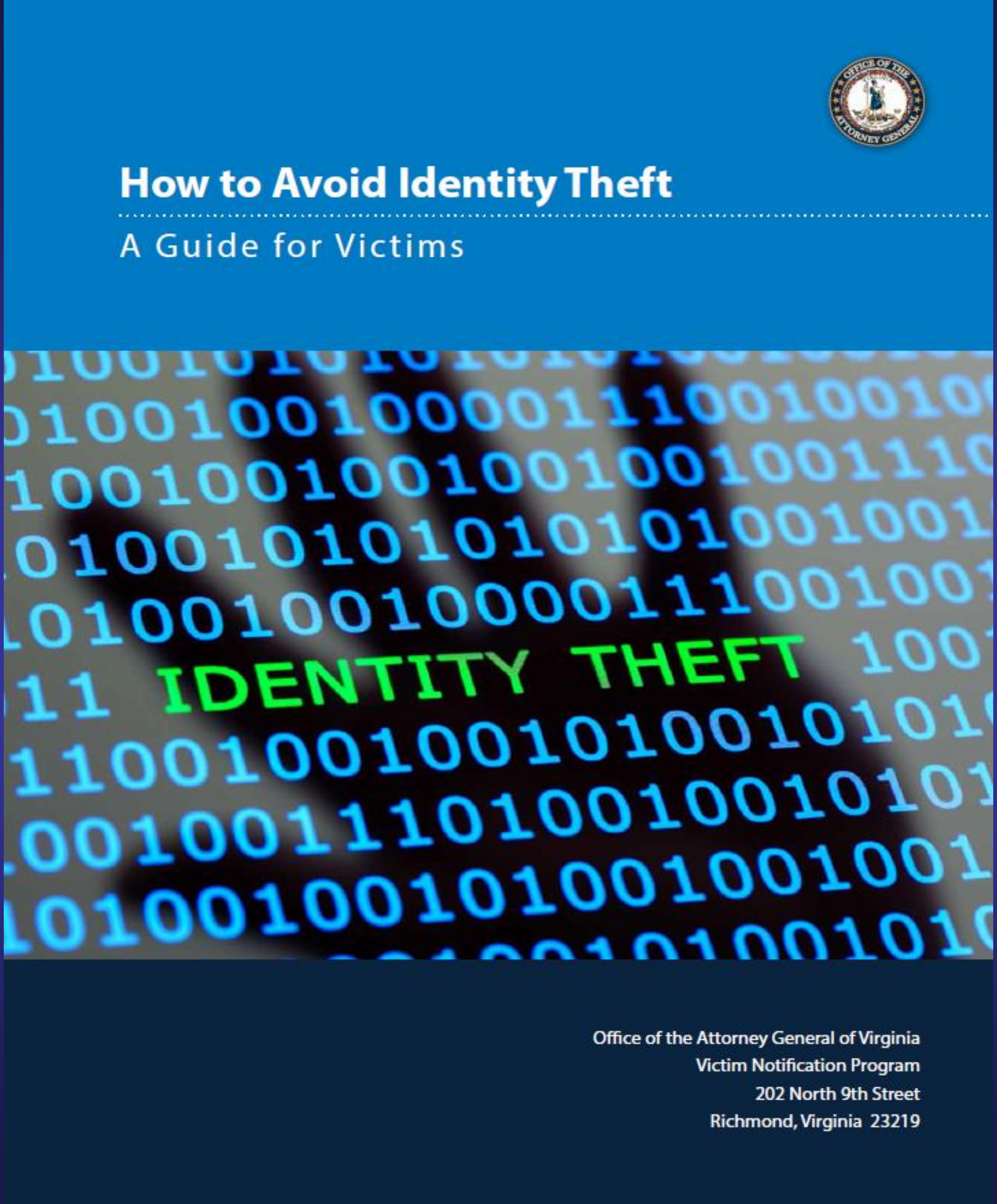
How to spot it:

- 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 and utilities)
- Credit bureaus
- Federal Trade Commission (FTC)
- Local/State law enforcement
- Office of the Attorney General



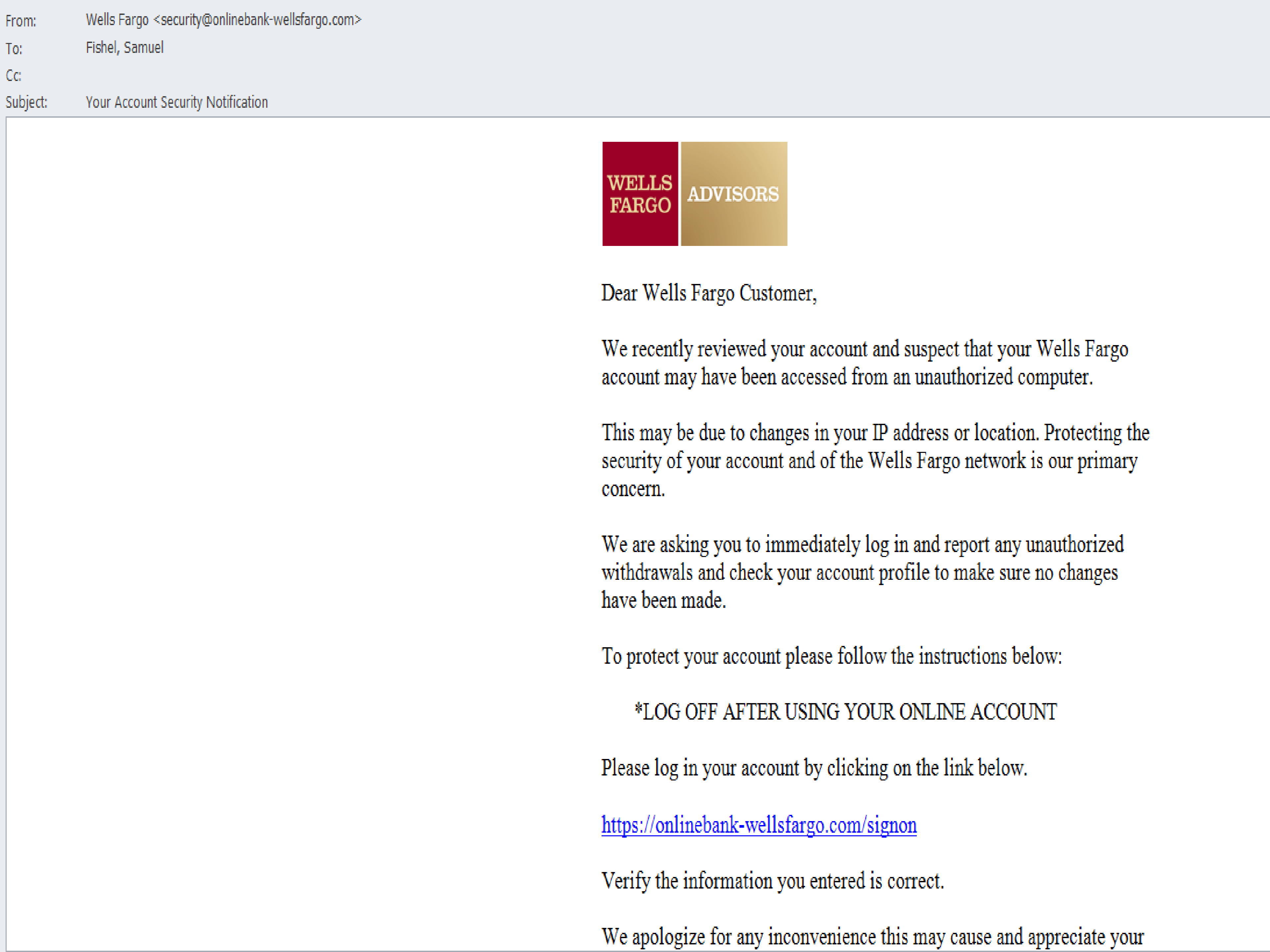
How to Avoid Identity Theft

A Guide for Victims

Office of the Attorney General of Virginia
Victim Notification Program
202 North 9th Street
Richmond, Virginia 23219

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 – one to five years imprisonment
  - B. Distribution of material – one to 10 years
  - C. Uses such information to commit another crime – one to ten years



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

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

Likelihood of clicking based on previous performance

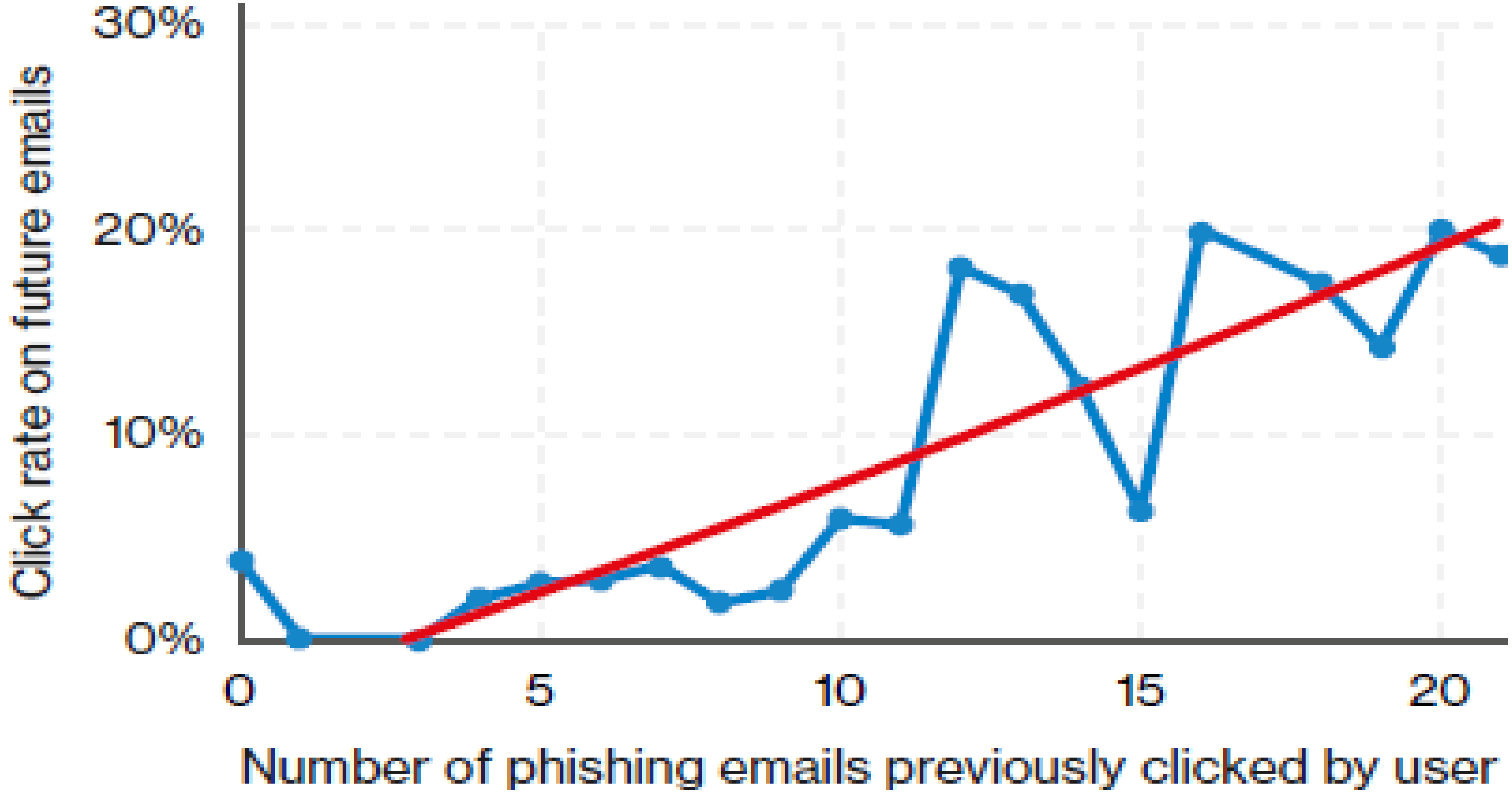


Figure 13. Click rates of users based on historical performance in phishing tests (n=2,771,850)

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, one to five years imprisonment
  - –Installs software on more than five computers, one to five years
  - –Keystroke logger violation, one to five years
  - –Exception for ISPs

Days receiving malware per organization

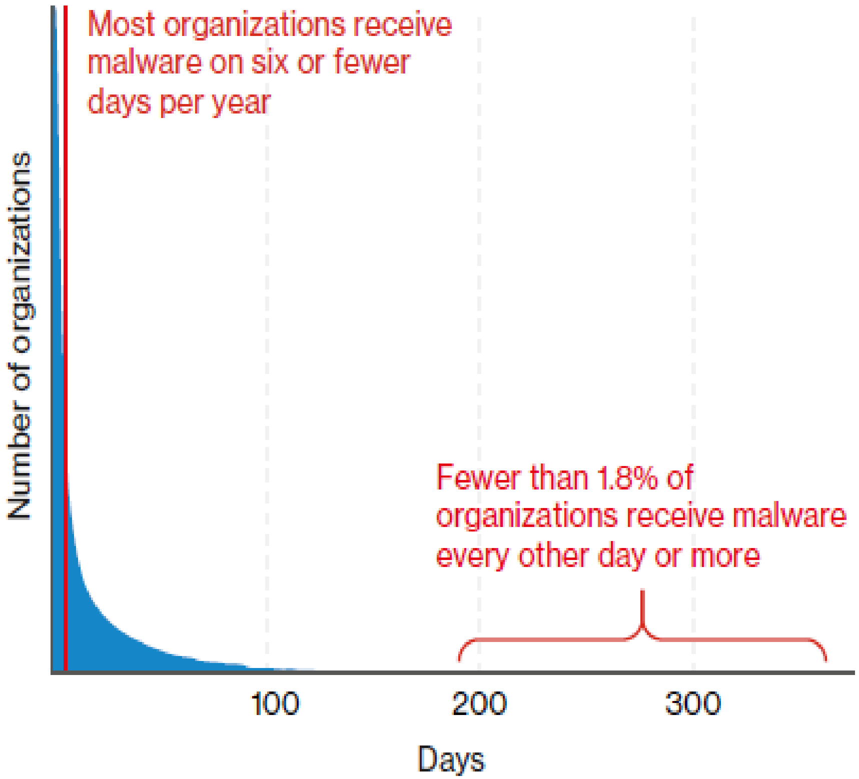


Figure 19. Days receiving malware per organization (n=128,131)

Frequency of malware vectors

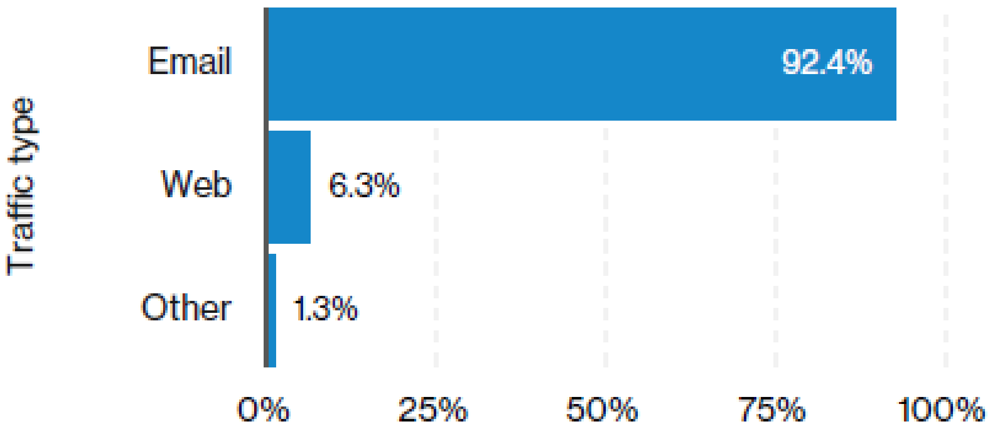


Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

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 – one to 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

Senior Assistant Attorney General

Virginia Attorney General's Office

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 Information Technologies Agency

New Security Services

Bill Stewart
Managed Security Services

CAM and BRM Joint Meeting
Jan. 28, 2020

Endpoint security tool suite: Modernized workstation and server security tools

- On **Jan. 13, 2020,** the approved modernization plan for endpoint network security tools will be deployed to agency devices.
  - Servers will be updated during your regular patching window as to not disrupt normal operations
  - The new security tools will be deployed to agency workstations using the SCCM. The deployment will be completed over several weeks. The proposed schedule will be provided soon.

Endpoint security tool suite: Modernized workstation and server security tools

- **What is provided under the new endpoint security tool suite? ($$- Elective service with additional cost)**
  - Modernized version of existing services
    - Desktop antivirus/firewall/host intrusion prevention
    - Server antivirus/firewall
    - Endpoint compliance
    - Application whitelisting (formerly WWLS/ESOSS); $$
    - Drive encryption; $$ in some instances
  - And some future services
    - Enhanced data loss prevention; $$
    - File and folder encryption; $$
    - Server host intrusion prevention

Endpoint security tool suite: Modernized workstation and server security tools

- **How are the new endpoint security tools different from anti-virus?**
  - The endpoint security tools provide a much greater level of threat protection than the previous anti-virus solution. The new security tools provide quicker response to threats, less false positives and a more proactive response.

- **How do the new endpoint security tools impact agency end users?**
  - The endpoint security tools detection and response services will have minimal impact to the end users

Upcoming Events

IS Orientation

March 31, 2020

1 - 3 p.m.

Room 1211

Register @:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10
Presenter: Marlon Cole

Future ISOAG

March 4, 2020 @ CESC 1 – 4 p.m.

Speakers: - Victoria Yan Pillitteri, NIST

Servio F. Medina, Health Information Technology (HIT)

Mark Martens, VITA

Eric Culbertson, ATOS

ISOAG meets the first Wednesday of each month in 2020

COV Information Security Conference
2020 Vision: A future of Innovation

2020 Security conference registration and call for papers

Registration for the 2020 Commonwealth of Virginia (COV) Information Security Conference is now open. The 2020 conference will be held April 16 and 17 at the Altria Theater in Richmond. The call for papers has been issued and the conference committee is now accepting submissions through February 21.

Registration Fee: $175

Conference and registration information can be found on the link below.

https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/

Send your call for papers questions to: isconferencecfp@vita.virginia.gov

For all other conference questions: covsecurityconference@vita.virginia.gov

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk