# A New Look at Cyber Security

Bryan Fury, MSISM, CISSP, CRISC

bfury@corporateone.coop

614-825-9378

# Agenda

- Incident vs Breach
- Verizon Report
- Industry Comparisons
- Areas of Focus
- Passwords
- Minimum Controls

# Incident vs Breach

- **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.

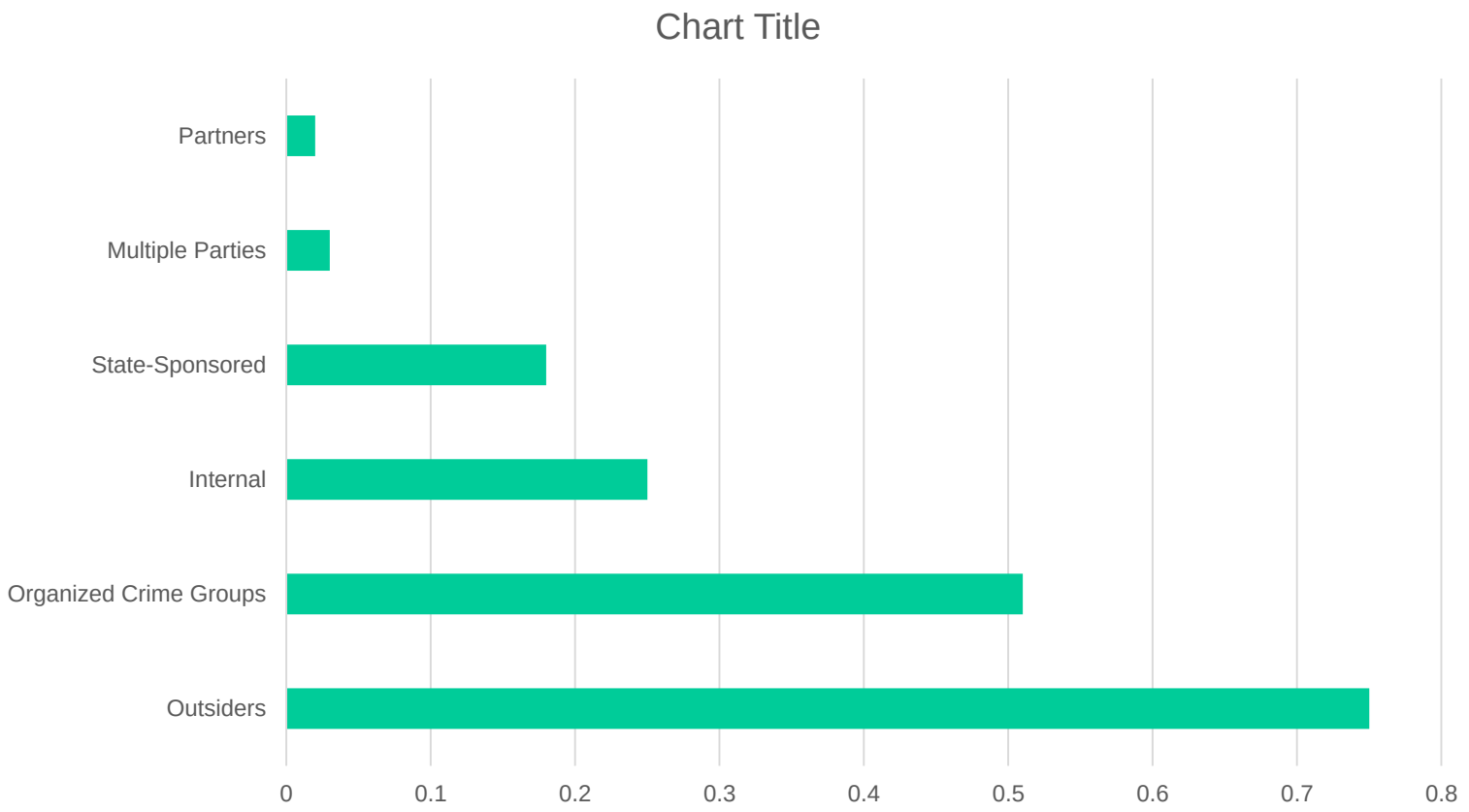
# Verizon Data Breach Report

- In it's 10th Edition
- 100,000+ Incidents
- 1,935 Breaches
  - Down from 2016
- 82 Countries
- Contributors
  - Major Security Companies
  - Large Corporations
  - US-CERT
  - 3-4 Letter Agencies

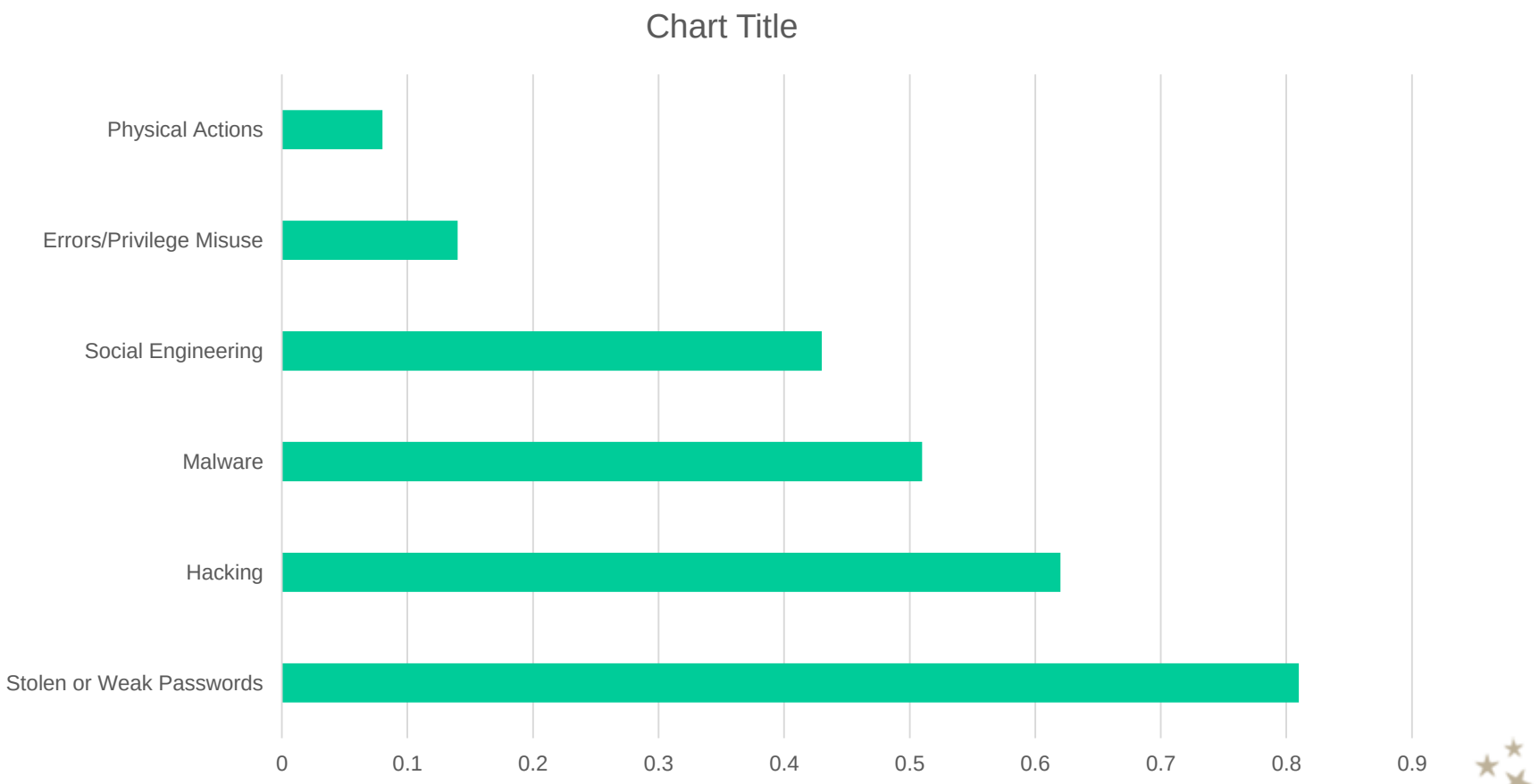
# VERIS

- veriscommunity.net – features information on the framework with examples and enumeration listings
- github.com/vm-risk/VERIS – features the full VERIS schema
- github.com/vm-risk/vcdb – provides access to the database on publicly disclosed breaches.

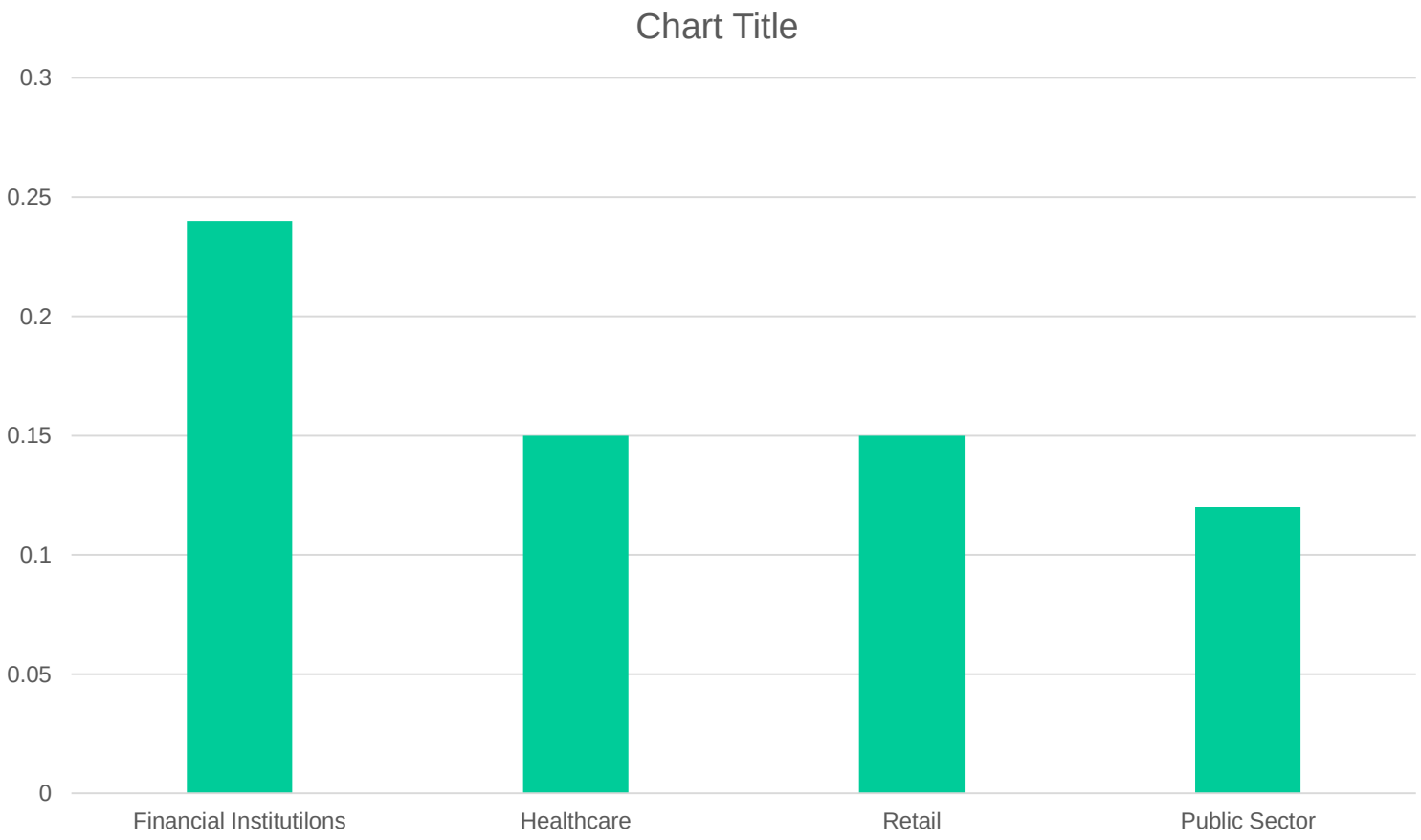
# Who's Behind The Breaches?



# What Tactics Do They Use?

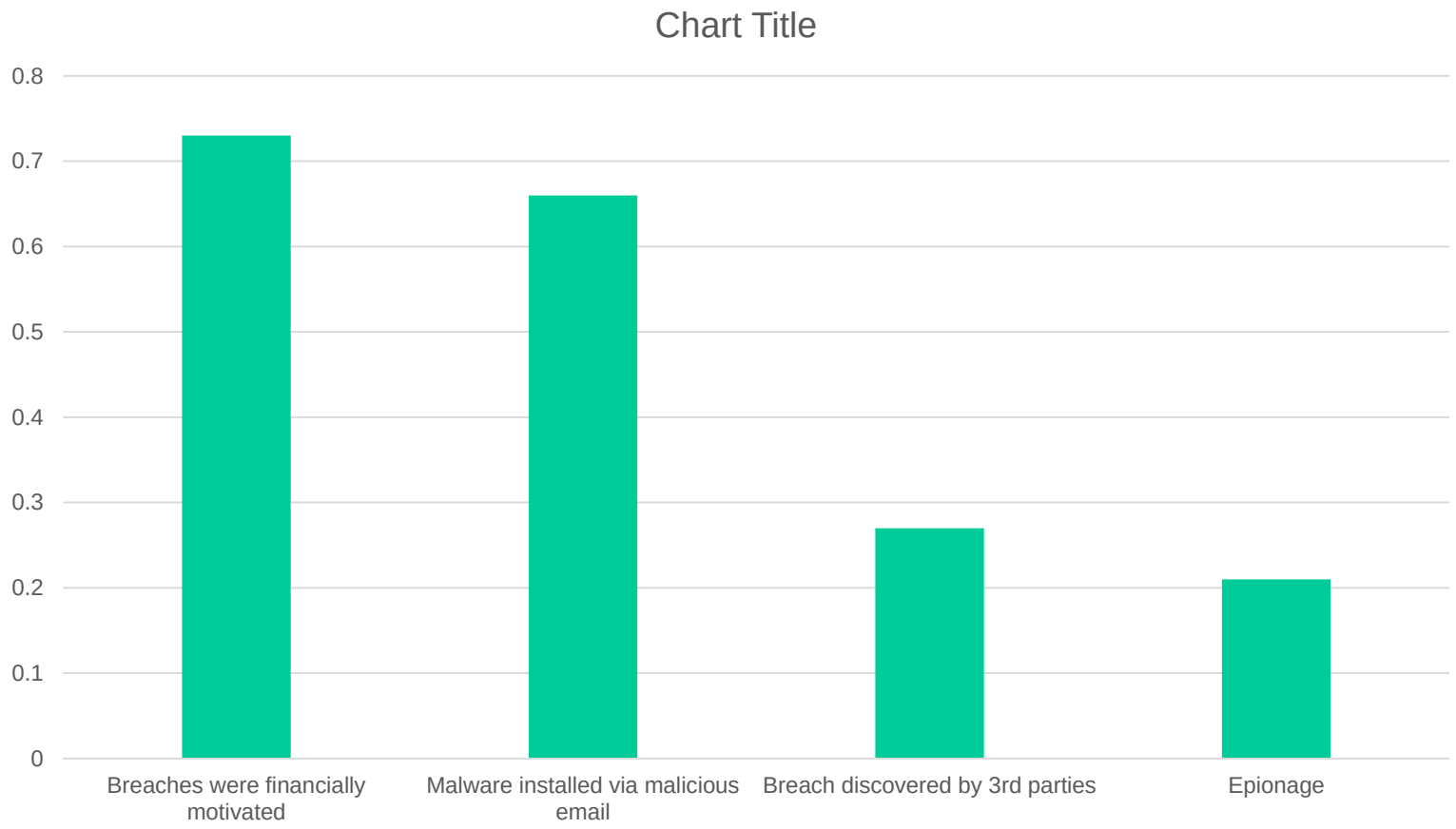


# Who Are The Victims?




CorporateOne FEDERAL CREDIT UNION

# What Else Is Common?



# Are We Fighting An Uphill Battle?

- Antiquated technologies
- Broadening attack surfaces
  - BYOD
  - VPNs
- Educating internal users while defending perimeter
- Not a top priority for most organizations

# We're Losing the Game!

**Compromises**

93% within minutes

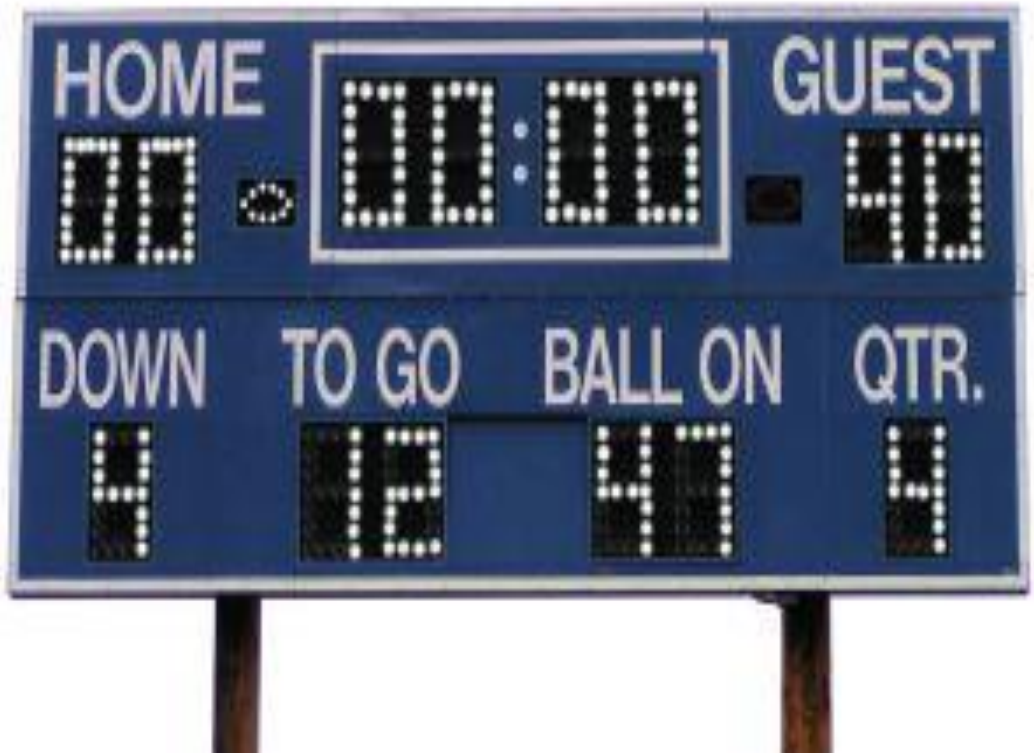
98% within days

**Exfiltration**

98% w/in days

**Discovery**

14% within days



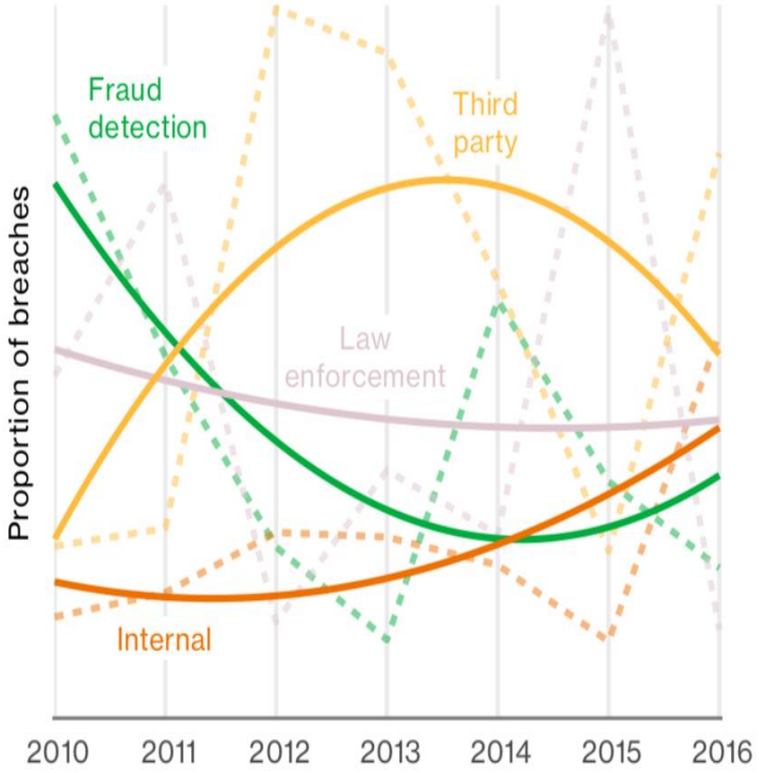
# How are they getting in? Common Attacks

- Exploiting Human Weakness
  - Phishing, Tailgating, Dumpster Diving, Media Dropping
- Attacks Against Unpatched Systems
  - 93% of CVEs exploited more than 1 year after being published
- Web App Attacks
  - Huge spikes in cross-site scripting and SQL injection
- Keystroke Loggers / Packet Sniffers
- Brute Force Attacks (e.g. guessing passwords)
- Viruses/Worms
- Ransomware

# SIM Attacks

- Swapping
  - Social Engineering mobile carrier
- Cloning
  - Ability to order from Amazon
  - 5 to 10 minutes with Target phone
- Intercept SMS & OTP

# Others are finding out before you do...




- Bragging most common form of disclosure.
- Dridex Botnet in 2015
- Internal discovery is trending up

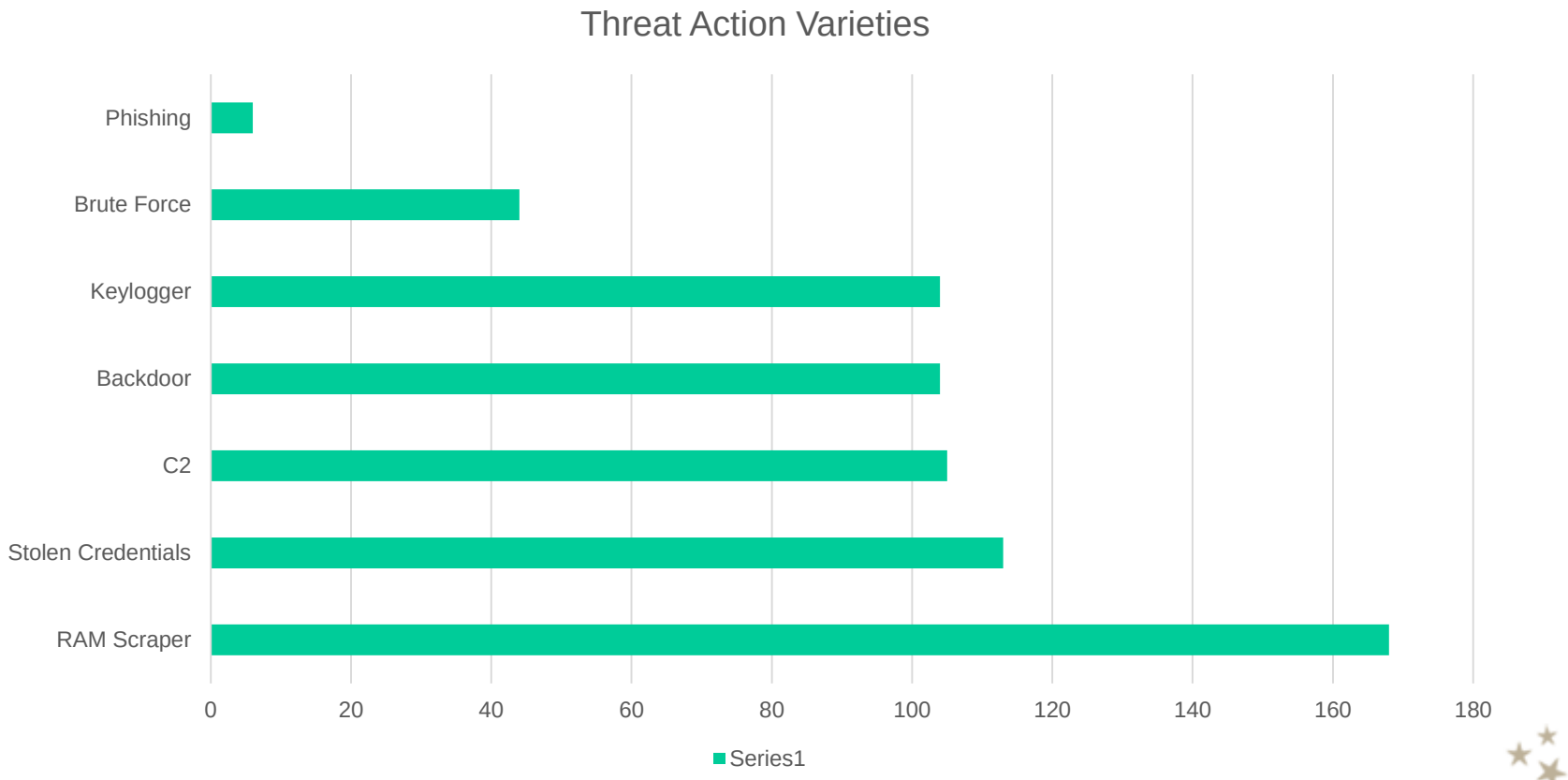
# Accommodation & Food Service

- Frequency
  - 215 Incidents, 201 with data disclosure
- Top 3 patterns
  - PoS Intursion
  - Privilege Misuse
  - Exploiting a Critical Vendor

# Accommodation & Food Service

- Threat Actors
  - 96% External, 4% Internal
- Actor Motives
  - 99% Financial, <1% Grudge
- Data Compromised
  - 99% Payment, 2% Personal, 1% Credentails

# Accommodation & Food Service



# Areas of Focus

- Killing me softly with malware
- Remove this tab before use
- You can’t get there from here
- Don’t be outdated

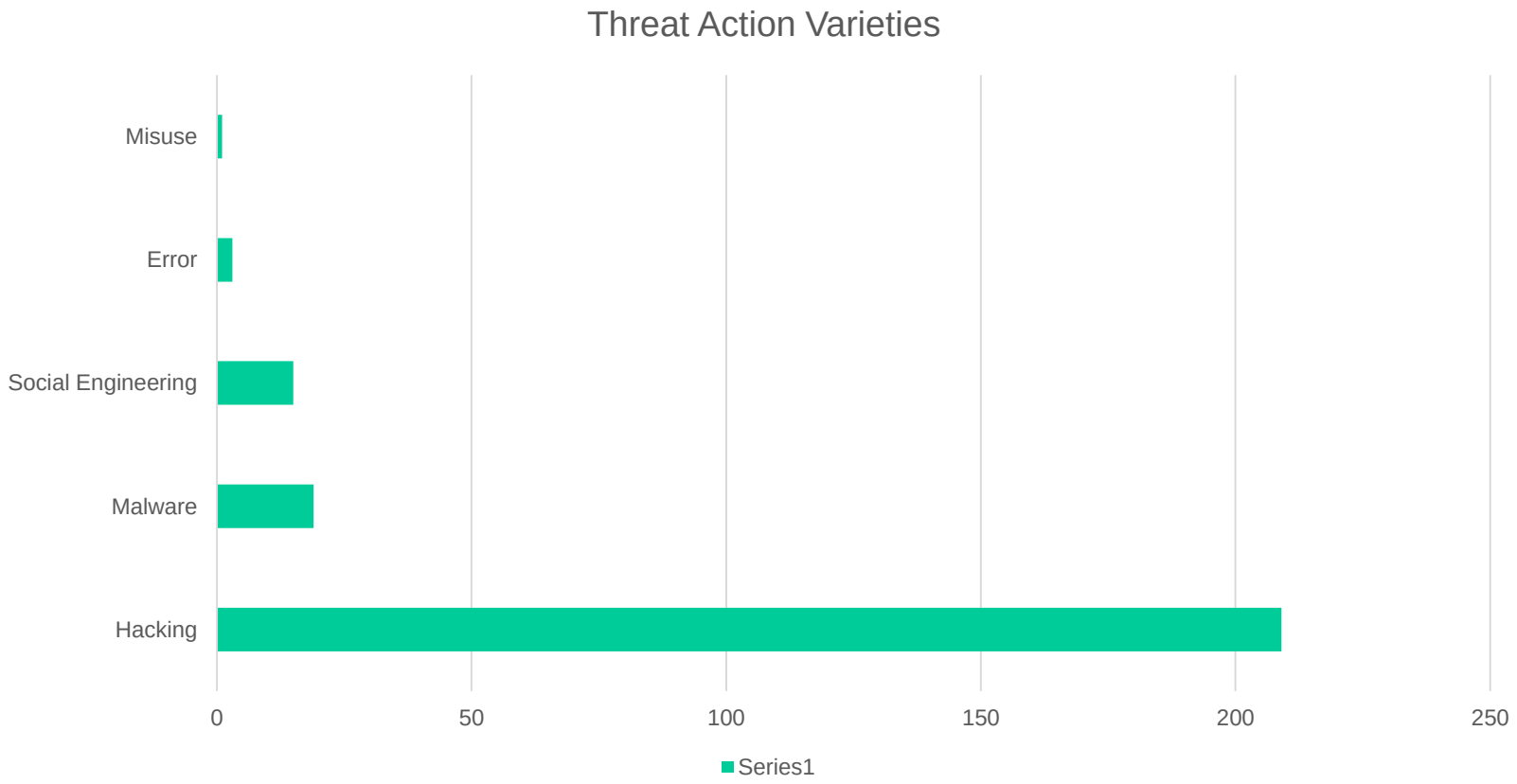
# Retail

- Frequency
  - 326 Incidents, 93 with data disclosure
- Top 3 Patterns
  - Denial of Service
  - Web App Attacks
  - Payment Card Skimming

# Retail

- Threat Actors
  - 92% External, 7% Internal, <1% Partner
- Actor Motives
  - 96% Financial, 2% Espionage, 2% Curiosity
- Data Compromised
  - 57% Payment, 27% Personal, 17% Credentials

# Retail



# Areas of Focus

- What do we want?  When do we want it?  Now!

- No man is an island

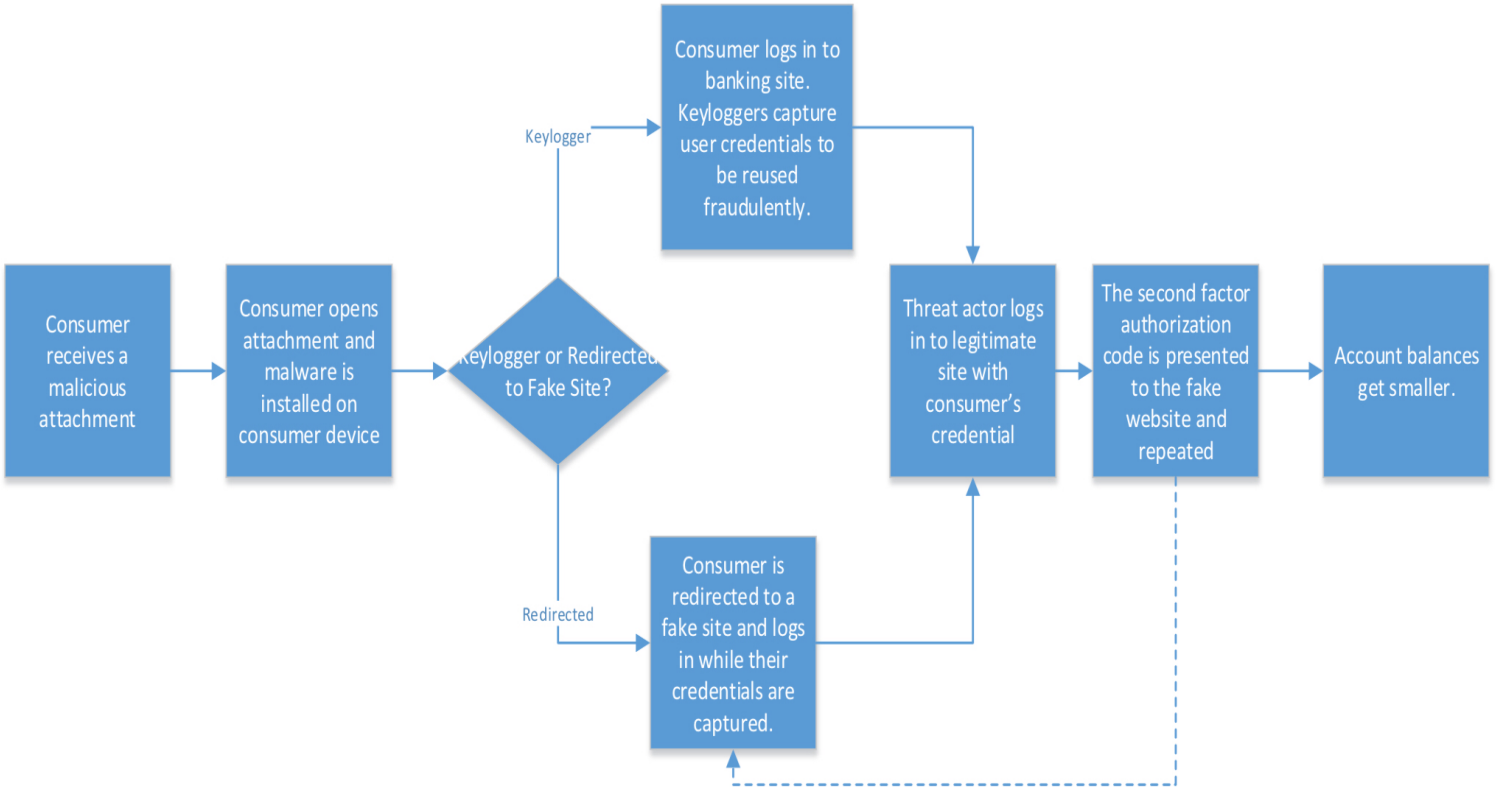
# Financial Institutions

- Frequency
  - 998 Incidents, 471 with data disclosure
- Top 3 Patterns
  - Denial of Service
  - Web App Attacks
  - Payment Card Skimming

# Financial Institutions

- Threat Actors
  - 94% External, 6% Internal, <1% Partner
- Actor Motives
  - 96% Financial, 1% Espionage
- Data Compromised
  - 71% Credentials, 12% Payment, 9% Personal

# Banking Trojan




CorporateOne FEDERAL CREDIT UNION

It's where you belong.

# Areas of Focus

- Taunt them a second time
- Make a new plan
- It’s not that I don’t trust you, but...

# Attack The Humans

- Drivers of human behavior can be leveraged to influence someone
  - Eagerness
  - Curiosity
  - Distraction
  - Uncertainty

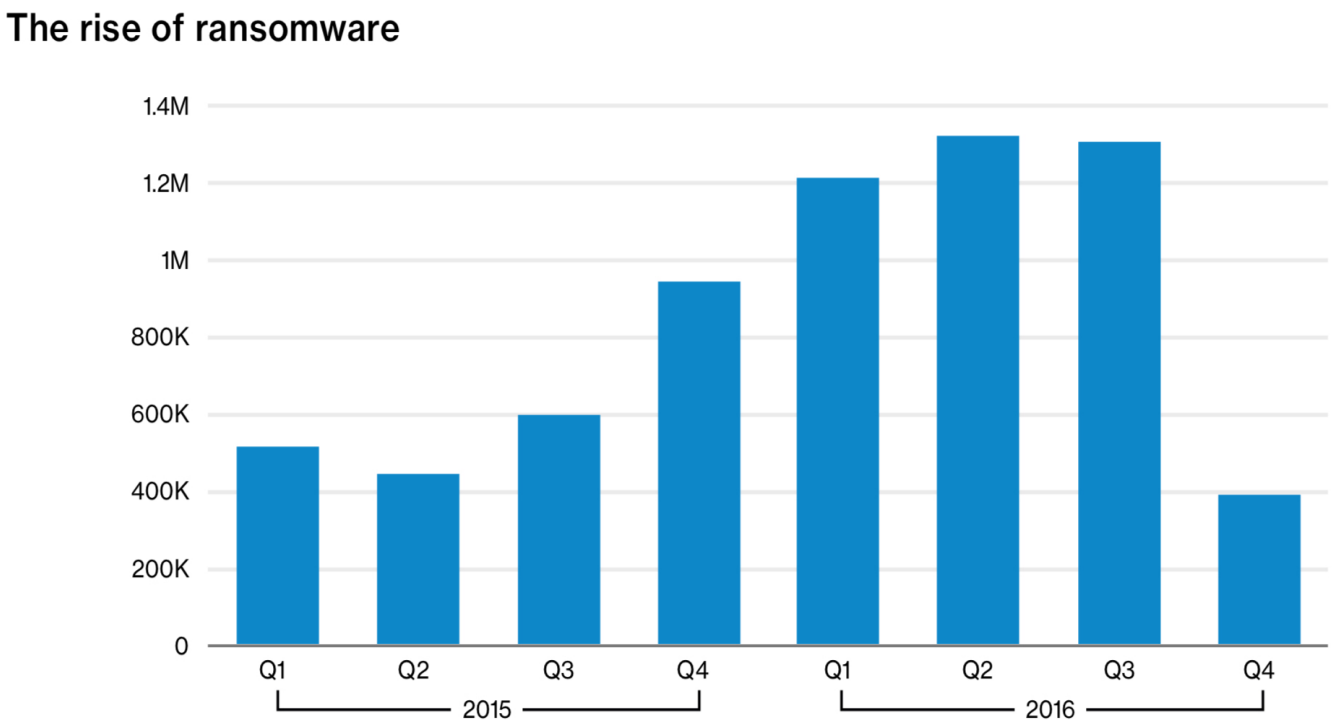
# Attack The Humans

- 98% of breaches & incidents that involve social action contain:
  - Phishing
  - Pretexting

# Phishing by Numbers

- 7.3 million records from 14,000 campaigns
- ~3 million unique users from 2,280 orgs
- 7.3% successfully phished
- 15% of those more than once
- 3% more than twice

# The Rise Of Ransomware




CorporateOne
FEDERAL CREDIT UNION

# Areas Of Focus

- 99% of malware is sent by email or web server
- Block executables at email gateway
- Disable macros by default
- Keep browser patched and updated
- Anti-virus + Anti-malware

# Password

- NIST Special Publicatin 800-63 Appendix A
- Widely Adopted Recommendations for Strong Passwords
  - 8 Character Minimum
  - At least 1 Number
  - At least 1 Special Character
  - Change Every 90 Days

# Passwords

"Much of what I did I now regret.  It just drives people bananas and they don't pick good passwords no matter what you do."

- Bill Burr (2017)

# Passwords

- New NIST 800-63 Recommendations:
  - Favor the User
  - Size Matters
  - No Composition Rules
  - No Password Hints
  - KBA & SMS are Out
  - No More Expiration Without Reason

# Minimum Control Recommendations
## Prevent (P) Detect (D) Respond (R)

- Security Awareness Training & Policies (P/D/R)
- Two-Factor Authentication (P)
- Patch Servers & Workstations Regularly (P)
- Data Encryption Both in Transit & at Rest (P)
- Network Segmentation (P/D/R)
- Vulnerability Scans & Penetration Testing (P/D)
- Anti-Virus & Anit-Malware (P/D)
- Develop an Incident Response Plan (R)
- Manage Vendors (P/D/R)

# Conclusion

- We’re fighting an uphill battle…and losing!
- Most breaches are preventable
  - Stop making it easy on them
- Make Cyber Security a priority
- Basic cyber hygiene

# Contact Information

Bryan Fury

Vice President Enterprise Risk Management

614.825.9378 (O)

614.701.7561 (C)

bfury@corporateone.coop