CFMA Rocky Mountain

Fraud - The Nexus of Insiders, Outsiders and Cyber

Wi-Fi Network Login

Network:Hyatt-meeting

Password: Digitek_Solutions

#CFMARM2019

Agenda

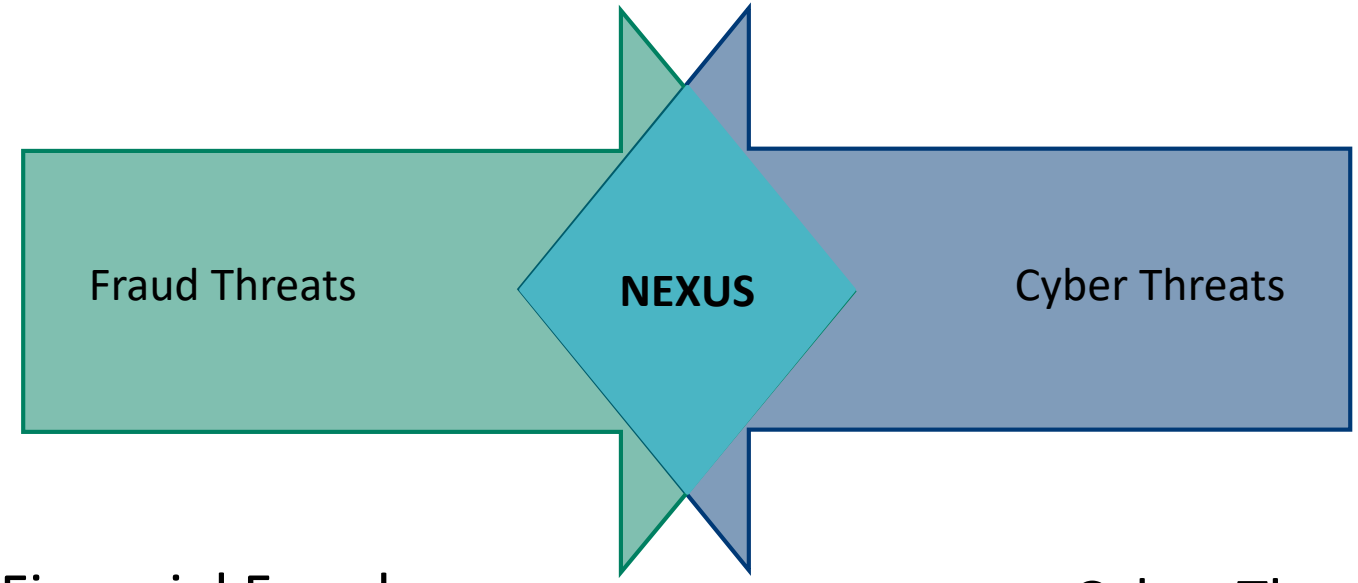
- Introductions
- Overview
- By the Numbers
- Common Threads
- What We Can Do
- Key Activities

Introductions

- Rob Rudloff, CISSP-ISSMP, PMP – Partner
- Beth Womersley, CPA, CRMA – Partner

What Nexus?

Overview



- Financial Fraud
- Corruption
- Asset Misappropriation
- Financial Statement Fraud

- Cyber Threats
- Dishonest Vendors
- Cyber Criminals
- Theft of IP

2,690
real cases of occupational fraud

from

125 countries

in

23 industry categories

$7 BILLION+
IN TOTAL LOSSES

$130,000
MEDIAN LOSS PER CASE

22%
OF CASES CAUSED LOSSES OF
$1 MILLION+

Median duration of a fraud scheme

16
MONTHS

CORRUPTION
was the most common scheme in every global region

ASSET MISAPPROPRIATION SCHEMES
are the most common and least costly

$114,000
median loss

89%
of cases

$800,000
median loss

FINANCIAL STATEMENT FRAUD SCHEMES
are the least common and most costly

10%
of cases

TIPS are by far the most common initial detection method

TIPS 40%

INTERNAL AUDIT 15%

MANAGEMENT REVIEW 13%

EMPLOYEES
provide over half of tips, and nearly 1/3 come from OUTSIDE PARTIES

ORGANIZATIONS WITH HOTLINES
detect fraud by tips more often

46% OF CASES DETECTED BY TIP
HOTLINES

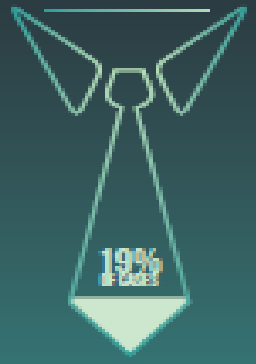
30% OF CASES DETECTED BY TIP
NO HOTLINES

Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

INTERNAL CONTROL WEAKNESSES
WERE RESPONSIBLE FOR NEARLY
HALF OF FRAUDS

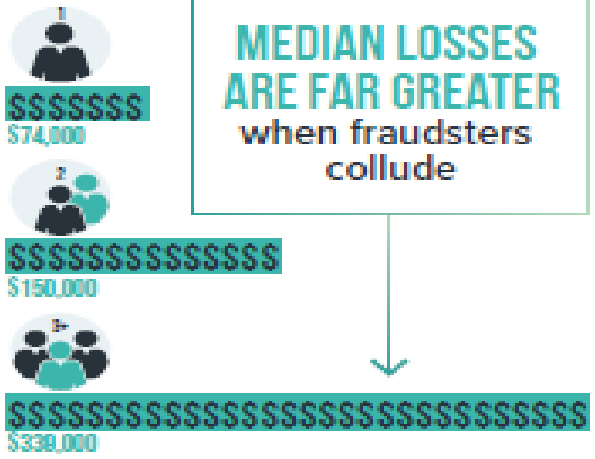
ALL 18 ANTI-FRAUD CONTROLS
ANALYZED WERE ASSOCIATED
WITH LOWER FRAUD LOSSES
AND QUICKER DETECTION

Owners/executives accounted for a small percentage of cases

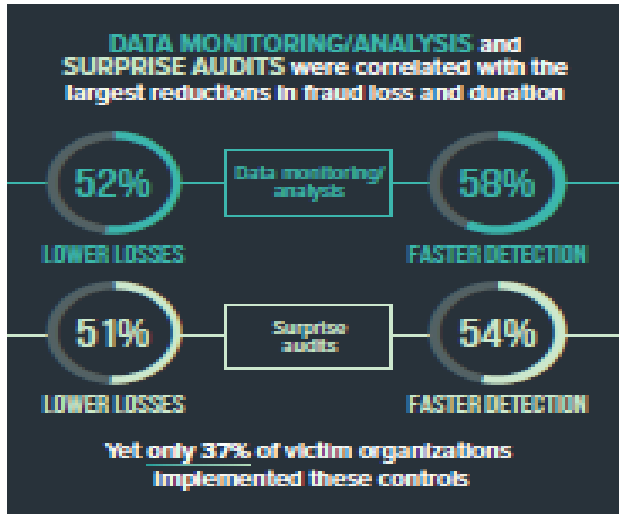


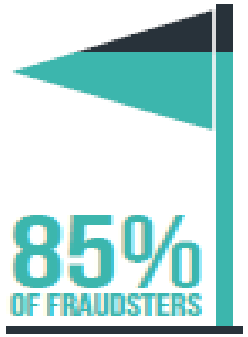
but caused a median loss of
$850,000

LOSSES CAUSED BY MEN WERE 75% LARGER
than losses caused by women



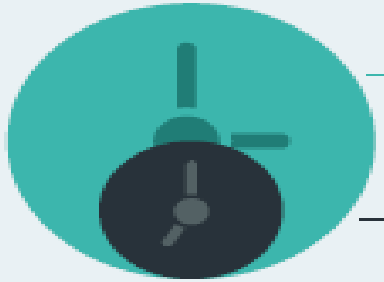
MEDIAN LOSSES ARE FAR GREATER
when fraudsters collude





85%
OF FRAUDSTERS
DISPLAYED AT LEAST ONE BEHAVIORAL
RED FLAG OF FRAUD

FRAUDSTERS WHO HAD BEEN WITH THEIR COMPANY LONGER
STOLE TWICE AS MUCH



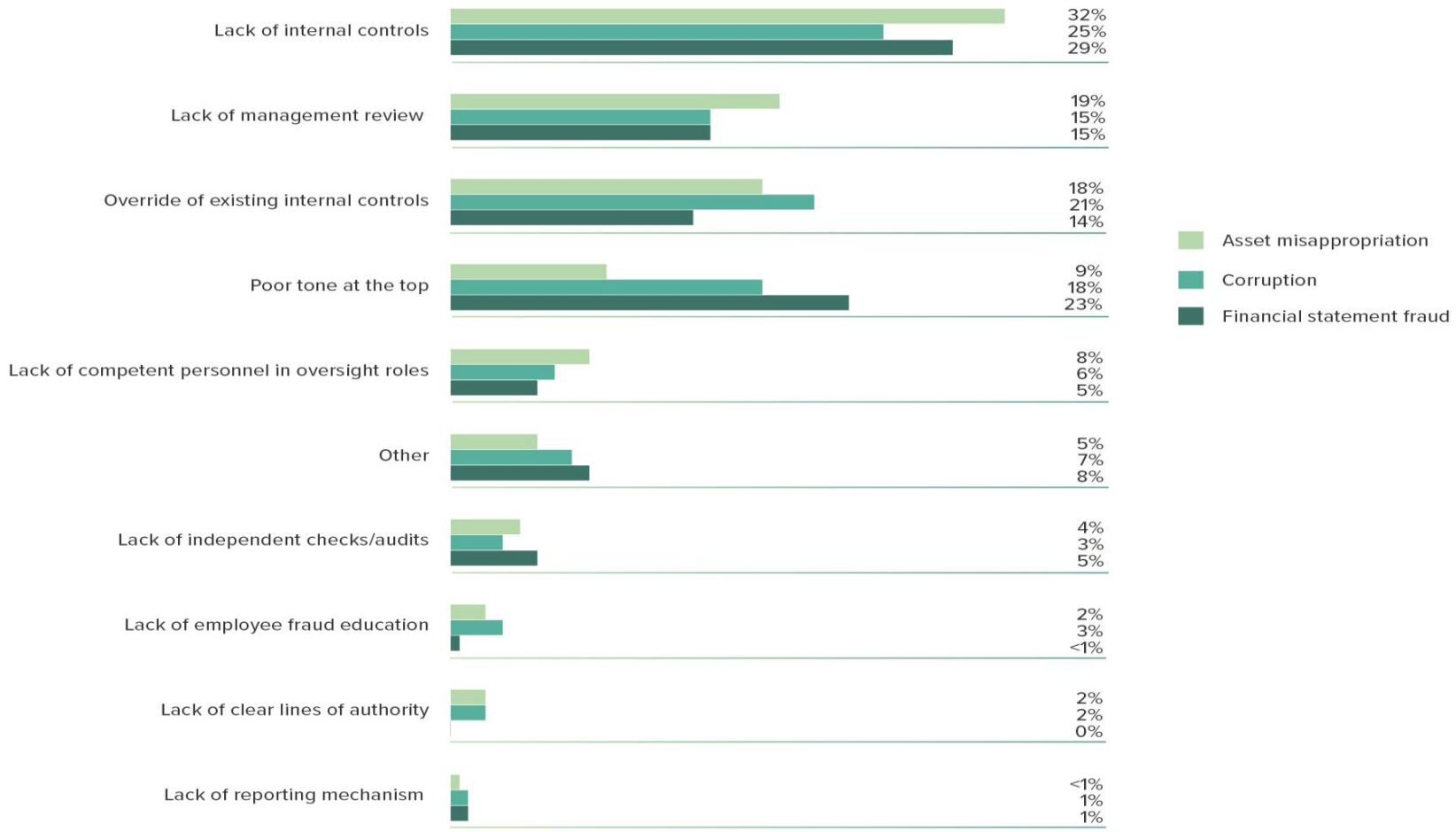
MORE THAN 5 YEARS' TENURE
$200,000
MEDIAN LOSS

LESS THAN 5 YEARS' TENURE
$100,000
MEDIAN LOSS

Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Internal control

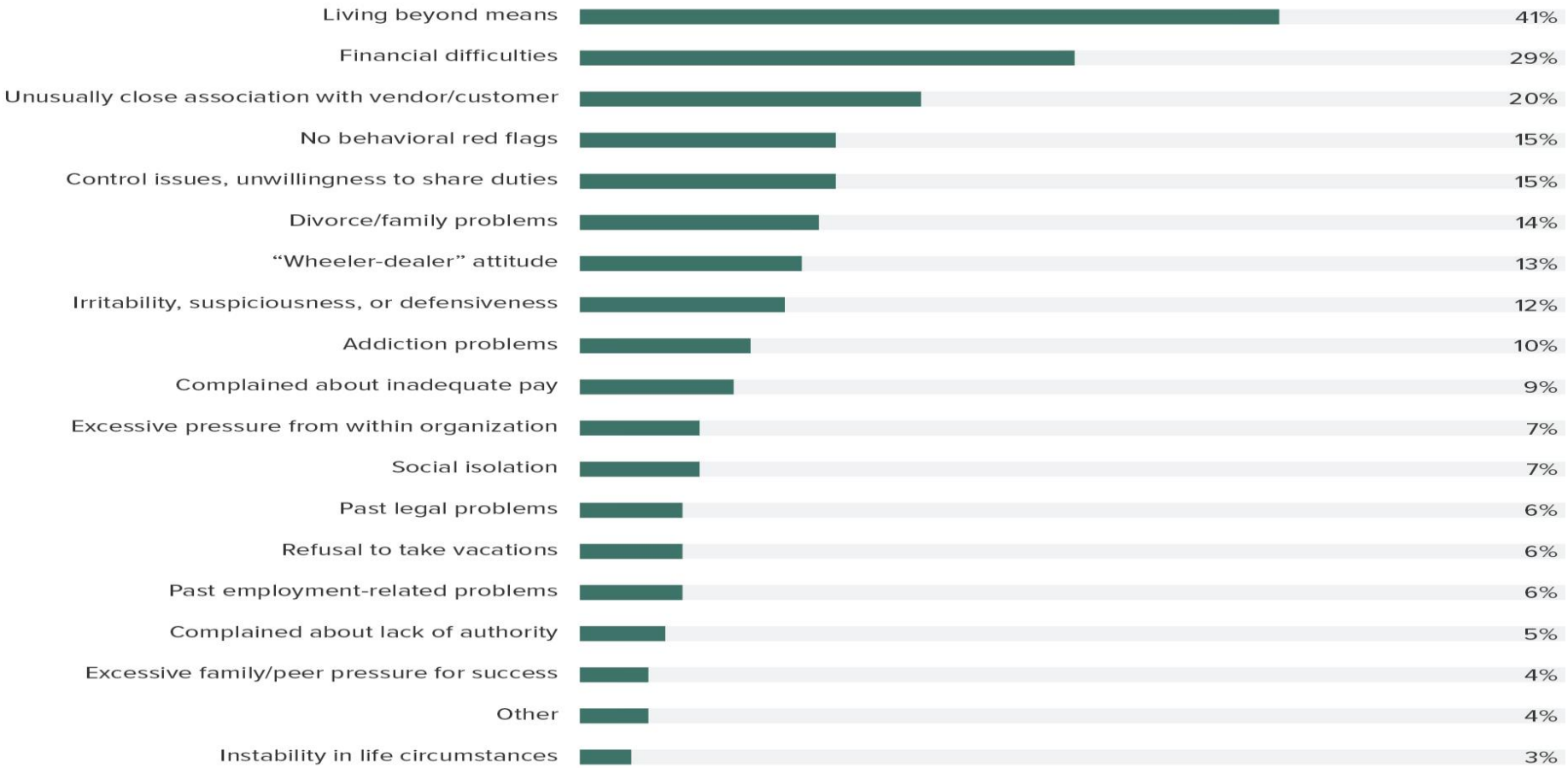
FIG. 23 **How do internal control weaknesses vary by scheme type?**



Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Behavioral Red Flags

FIG. 38 **How often do perpetrators exhibit behavioral red flags?**



Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Common threads – Fraud

- Weak internal controls
- Too much trust
- No segregation of duties
- Poor management oversight
- Poor Communications
- Lack of financial audit
- No background checks
- Lack of independent checks
- Culture

YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

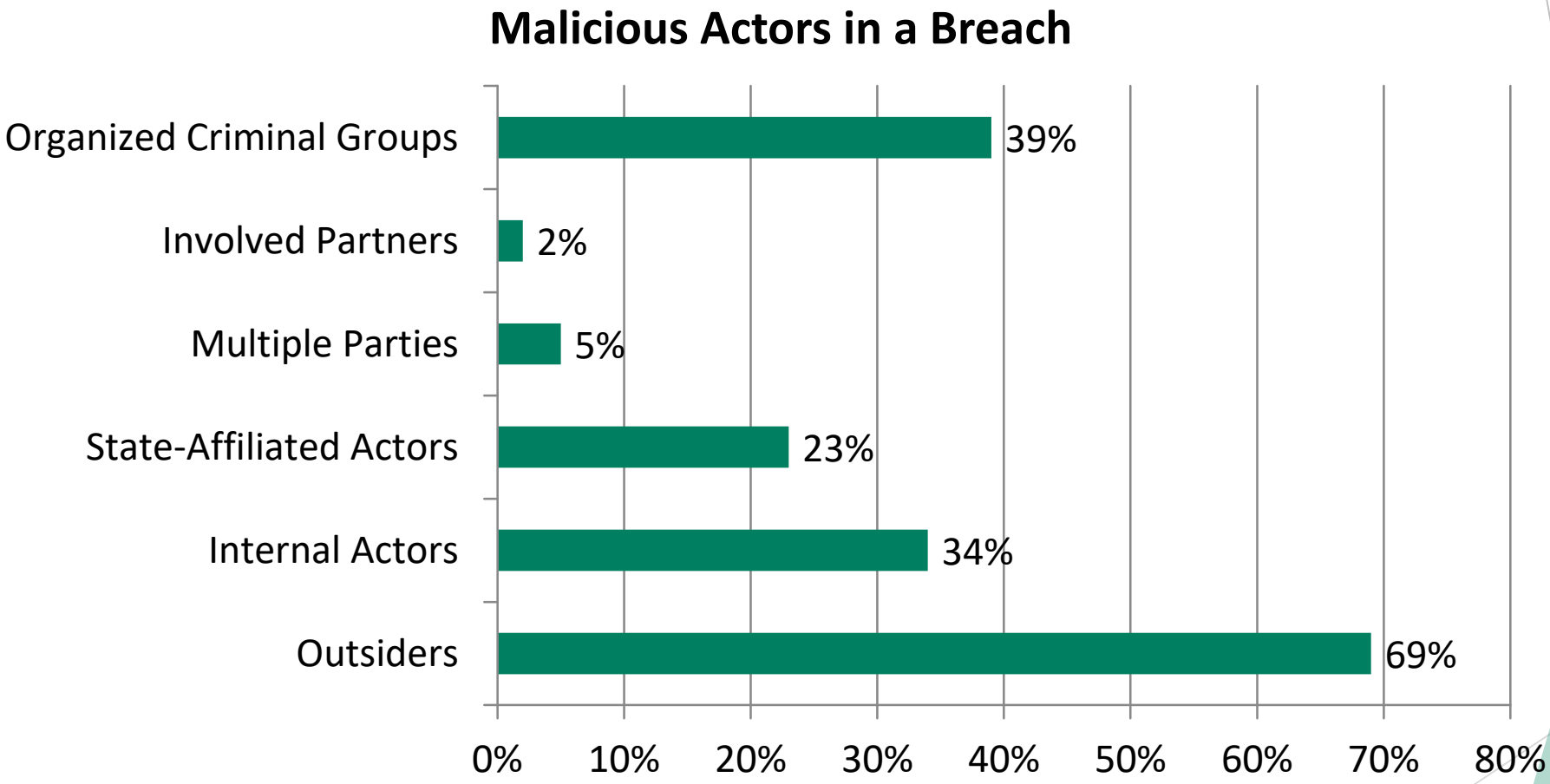
Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

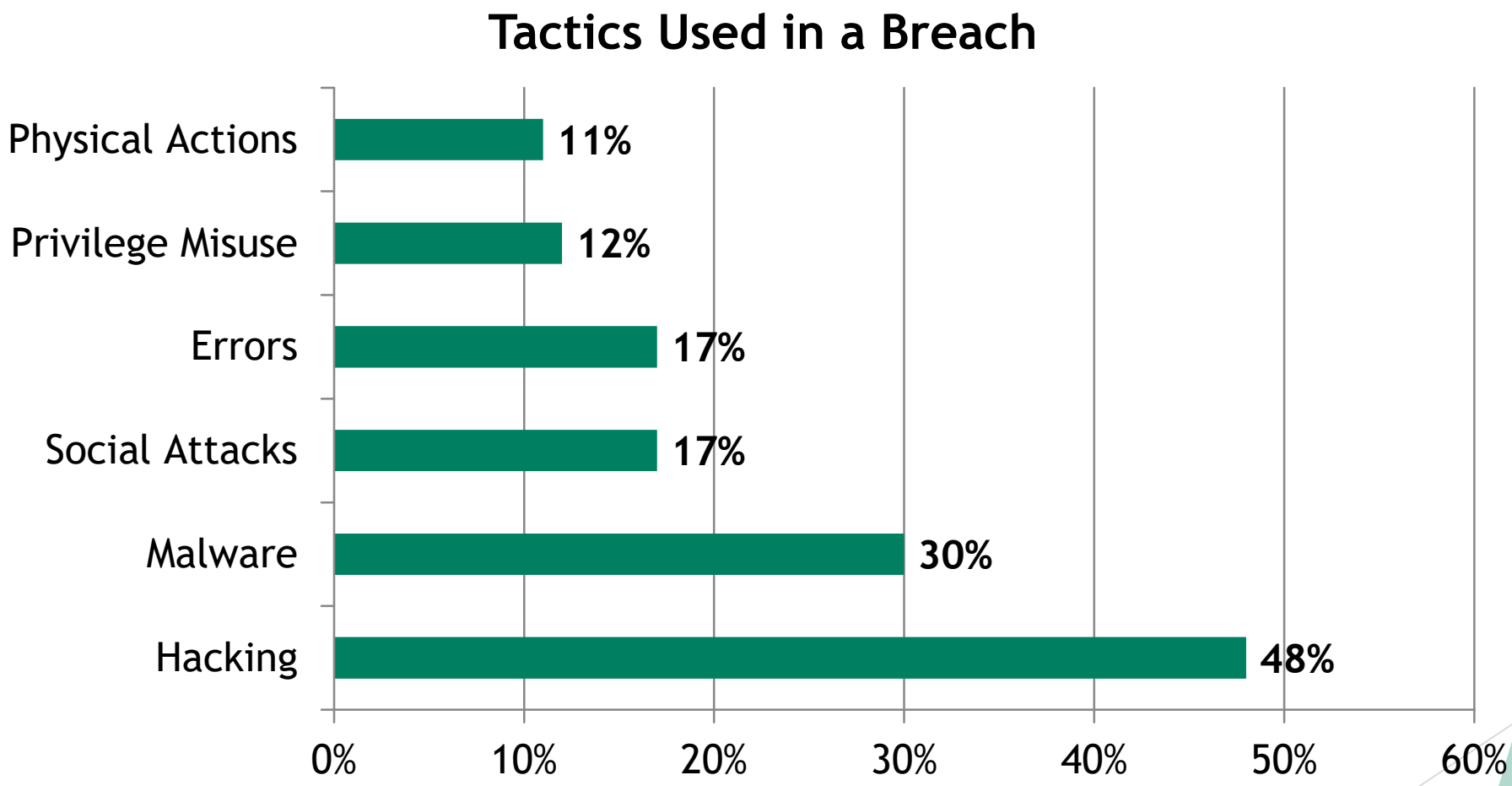
This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Breach Snapshot - Actors



Verizon Enterprise
2019 Data Breach Investigations Report

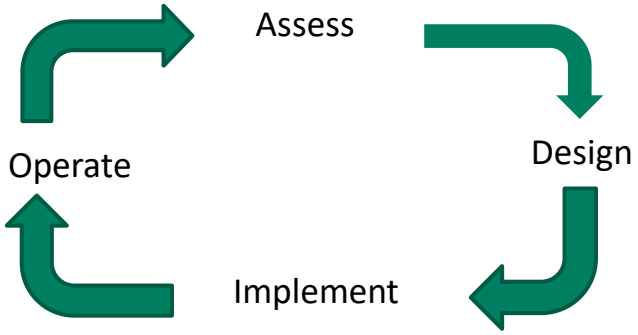
Breach Snapshot – Tactics & Methods



Verizon Enterprise
2019 Data Breach Investigations Report

“Big 3” Issues Now

“Security Hygiene”



Third Parties

People

High Profile Stories from the “Big 3”

Common threads – Cyber

- Weak security posture
- Lack of awareness
- Too much trust
- Poor change control
- Too many privileged account users
- Poor management oversight
- Poor Communications
- Lack of monitoring and reporting
- Lack of independent checks
- Culture

Intersection of Fraud Controls – External, Internal, Cyber

- Segregation of Duties
- Validation and Verification
- Additional Approvals for High Value Actions
- Inspection and Review
- Exception Handling
- Periodic Risk Assessments
- Independent Review

What we can do – Key Areas to Address

- **Training** – Internal Controls and Vigilance

  Policies, processes and awareness

- **Culture** – Reporting & Response

  *I **may** have clicked on something….*

- **Technical Controls** – designed into the process

  Use the capabilities included in your technology.

- **Internal Controls** – use your people & processes

  Processes designed to support proper controls and approvals.

- **Preparation** – risk assessments, planning and controls

Fraud and Risk Assessment

- Risk assessment includes management's assessment of the risks relating to the fraudulent reporting and safeguarding of the entity's assets.
- As part of the risk assessment process, you should identify the various ways that fraudulent reporting can occur, considering:
  - Degree of estimates and judgments in external reporting
  - Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates
  - Geographic regions where the entity does business
  - Incentives that may motivate fraudulent behavior
  - Nature of technology
  - Unusual or complex transactions subject to significant management influence
  - Vulnerability to management override and potential schemes to circumvent existing control activities

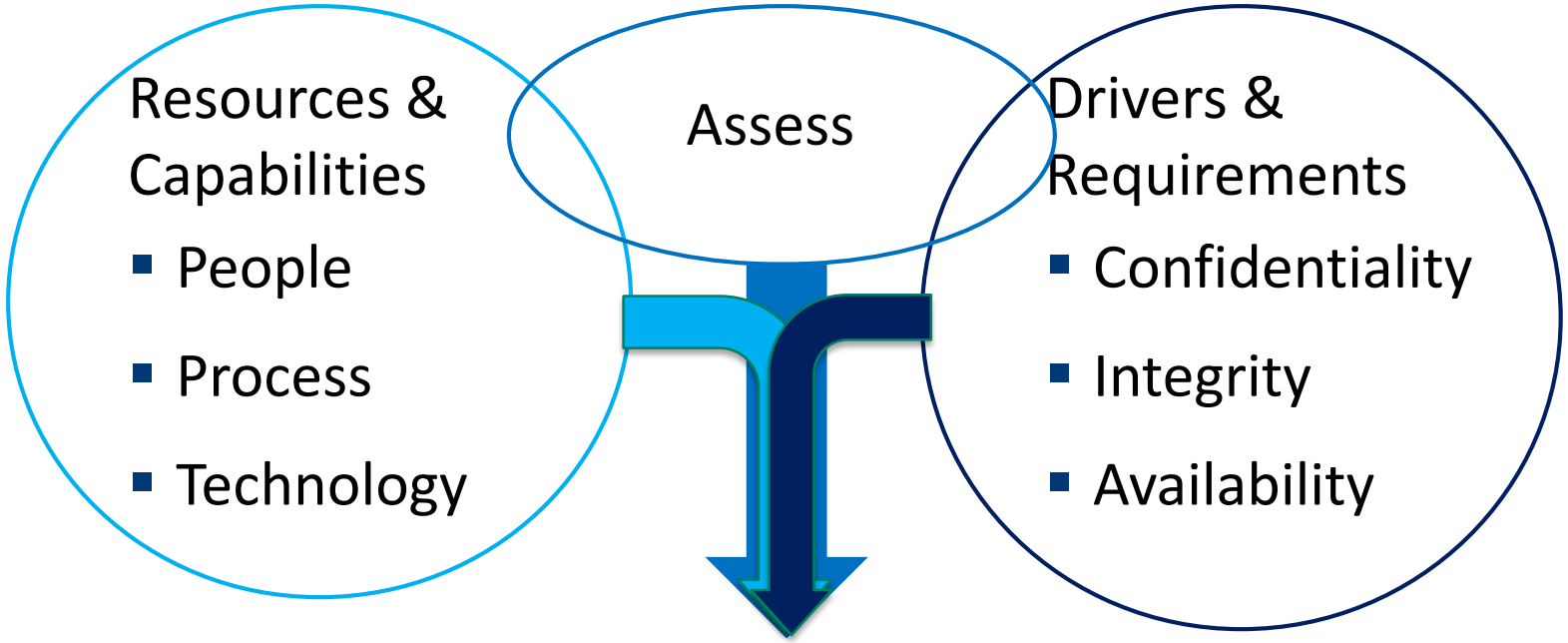
Brainstorming Fraud Risks

- Incentives, pressures, and opportunities
- Risk of management override of controls
- Population of fraud risks
- Fraudulent financial reporting
- Misappropriation of assets
- Corruption
- Information technology
- Regulatory and legal misconduct
- Reputation risk

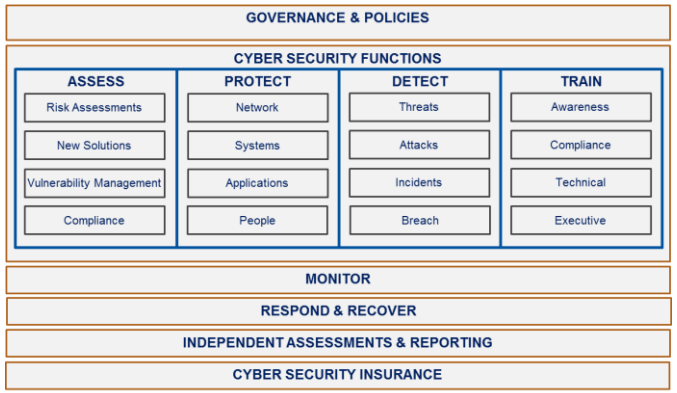
Brainstorming Controls - People

- Anti-fraud training
- Evaluating compensation and advancement programs
- Mandatory vacations
- Conflicts of interests
- Hotlines
- Conducting exit interviews
- Background checks

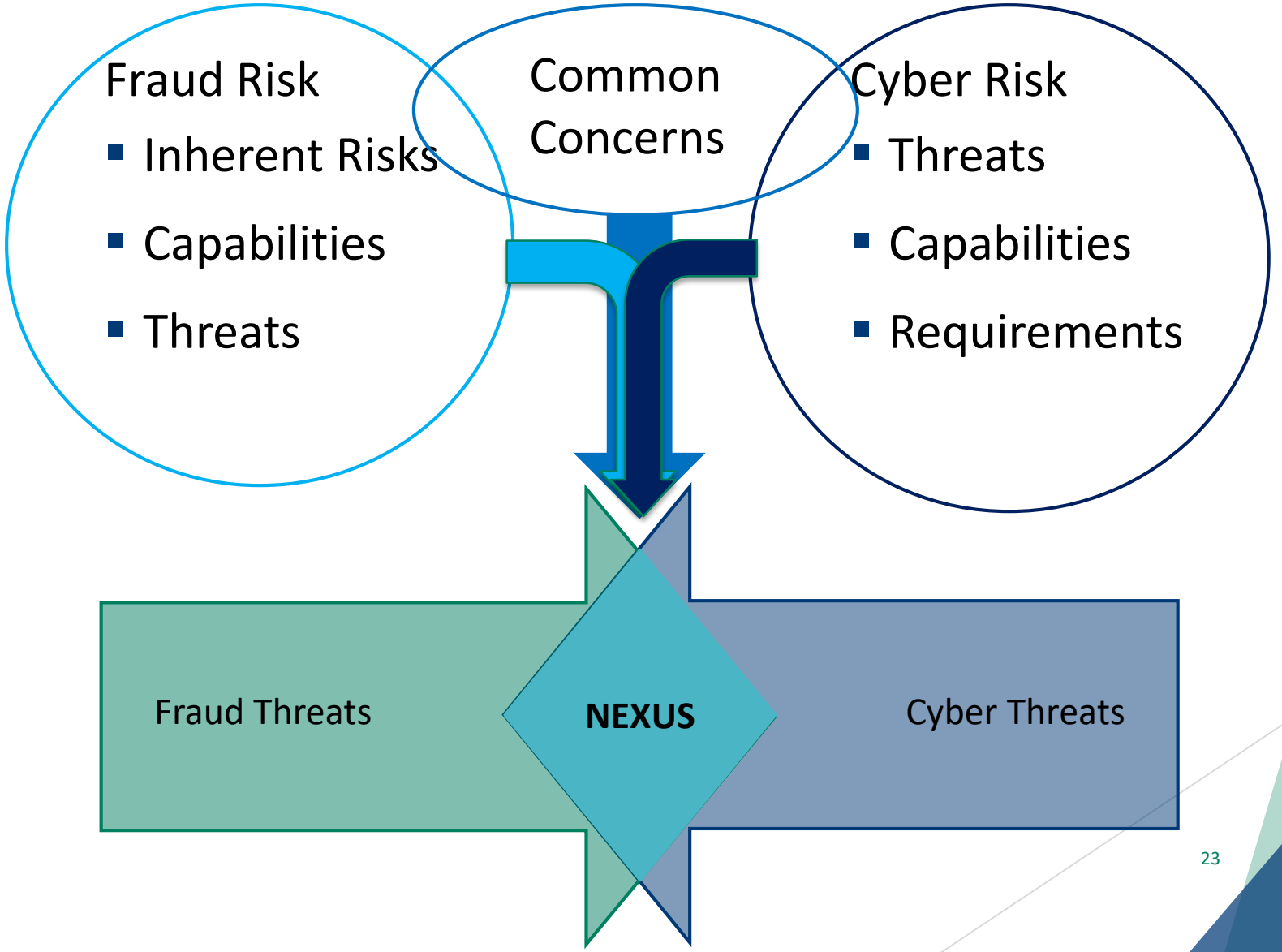
What we can do – Design Better Security



Cyber Security Program



What we can do – Applied to the Nexus



Key Activities to Reduce Fraud Risk

- **Identify** fraud risks
- **Assess** likelihood and significance of fraud risks
- **Respond** to fraud risks
- **Modify** processes and procedures
- **Integrate** people, process and technology controls

Questions

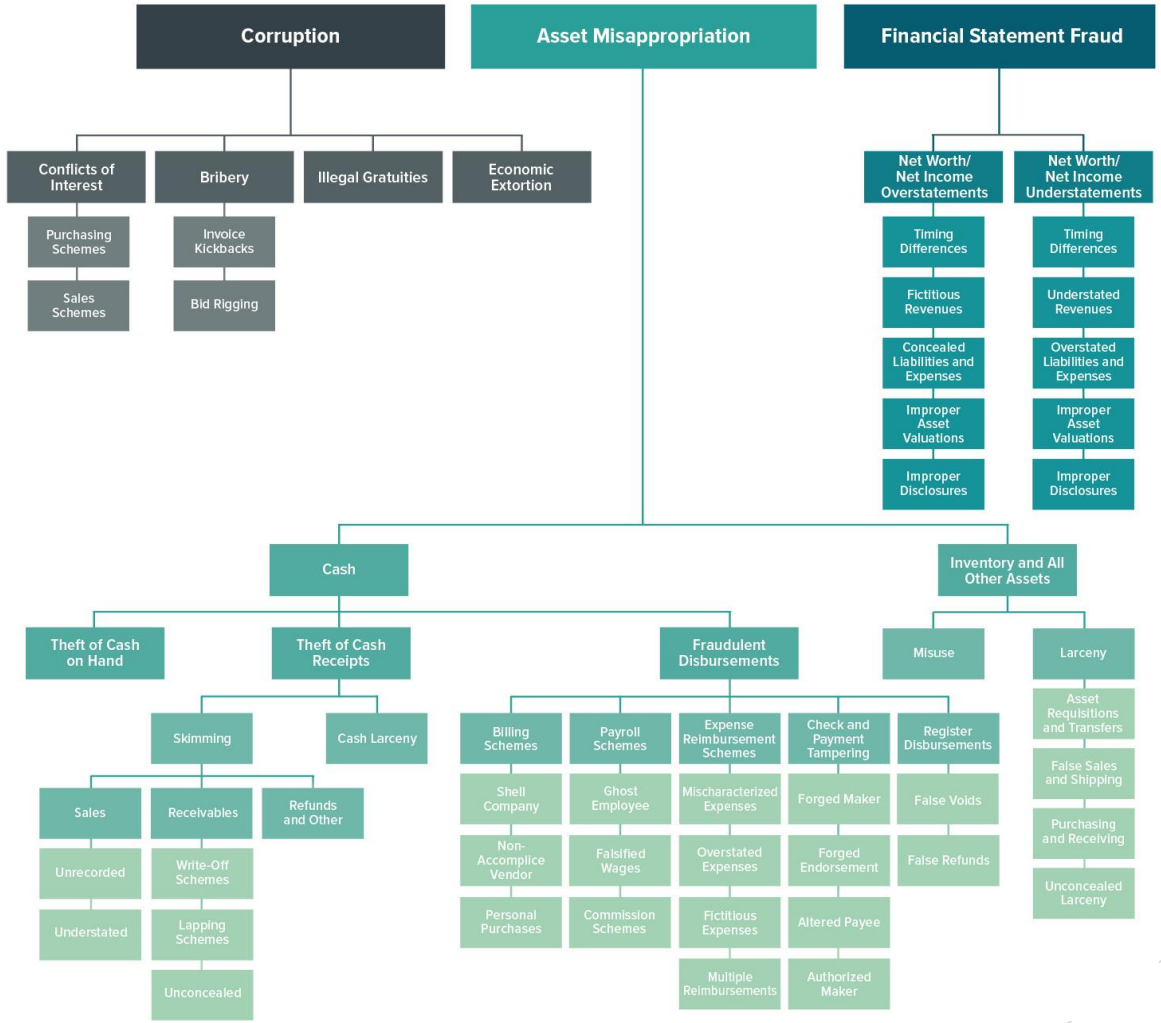
Beth Womersley, CPA, CRMA
Internal Audit Services
RubinBrown LLP
720.209.5986
Beth.Womersley@rubinbrown.com

Rob Rudloff, CISSP-ISSMP, PMP
Cyber Security Services
RubinBrown LLP
303.590.8770
Rob.Rudloff@rubinbrown.com

END OF PRESENTATION

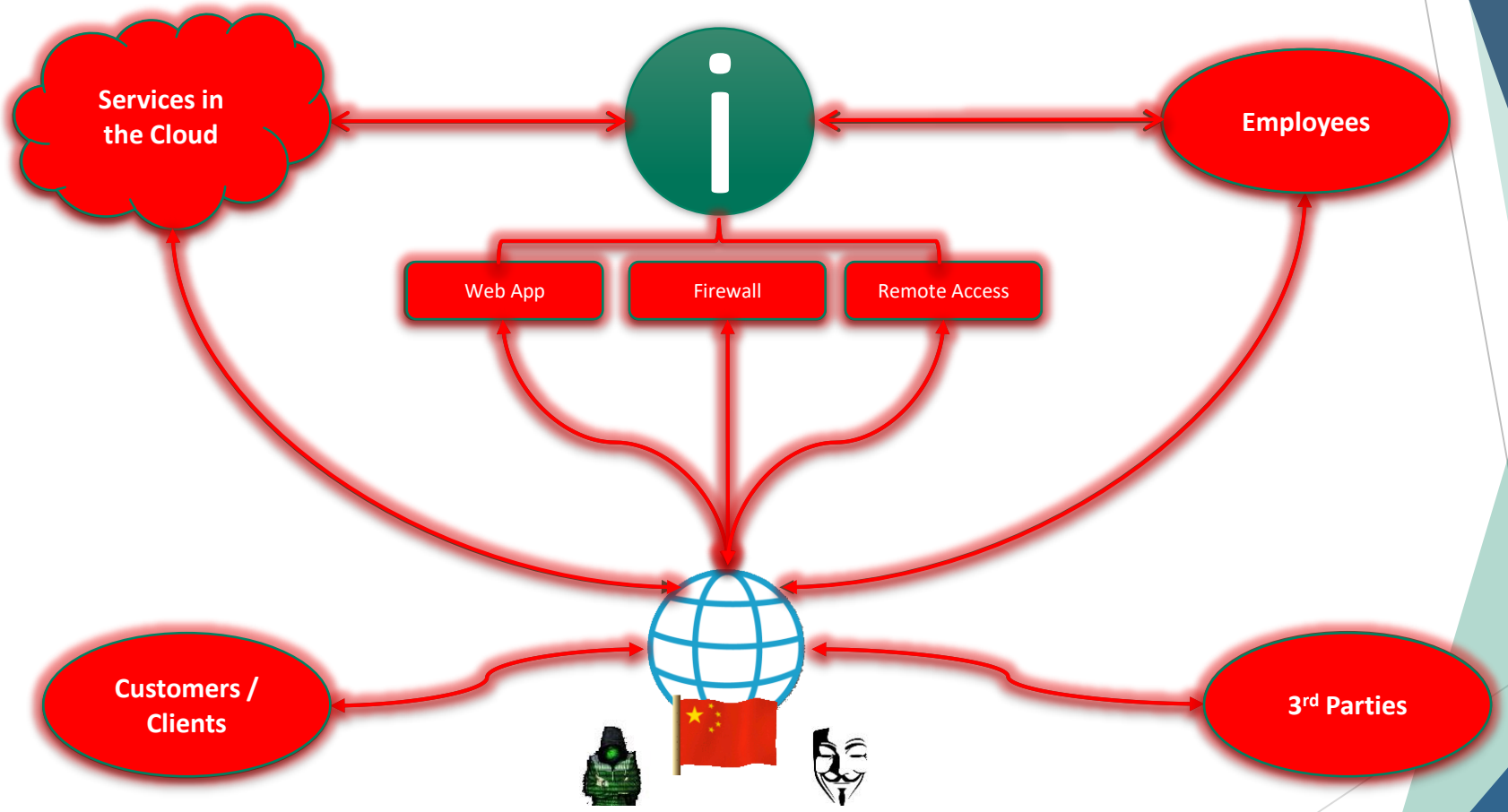
- ONLY REFERENCE SLIDES BEYOND THIS POINT

The “Fraud Tree”



Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Cyber Attacks – Path of Attack



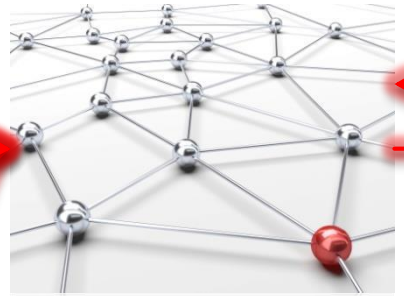
Cyber Attacks – Anatomy of a Breach

Web App

Firewall

Remote Access

Discovery

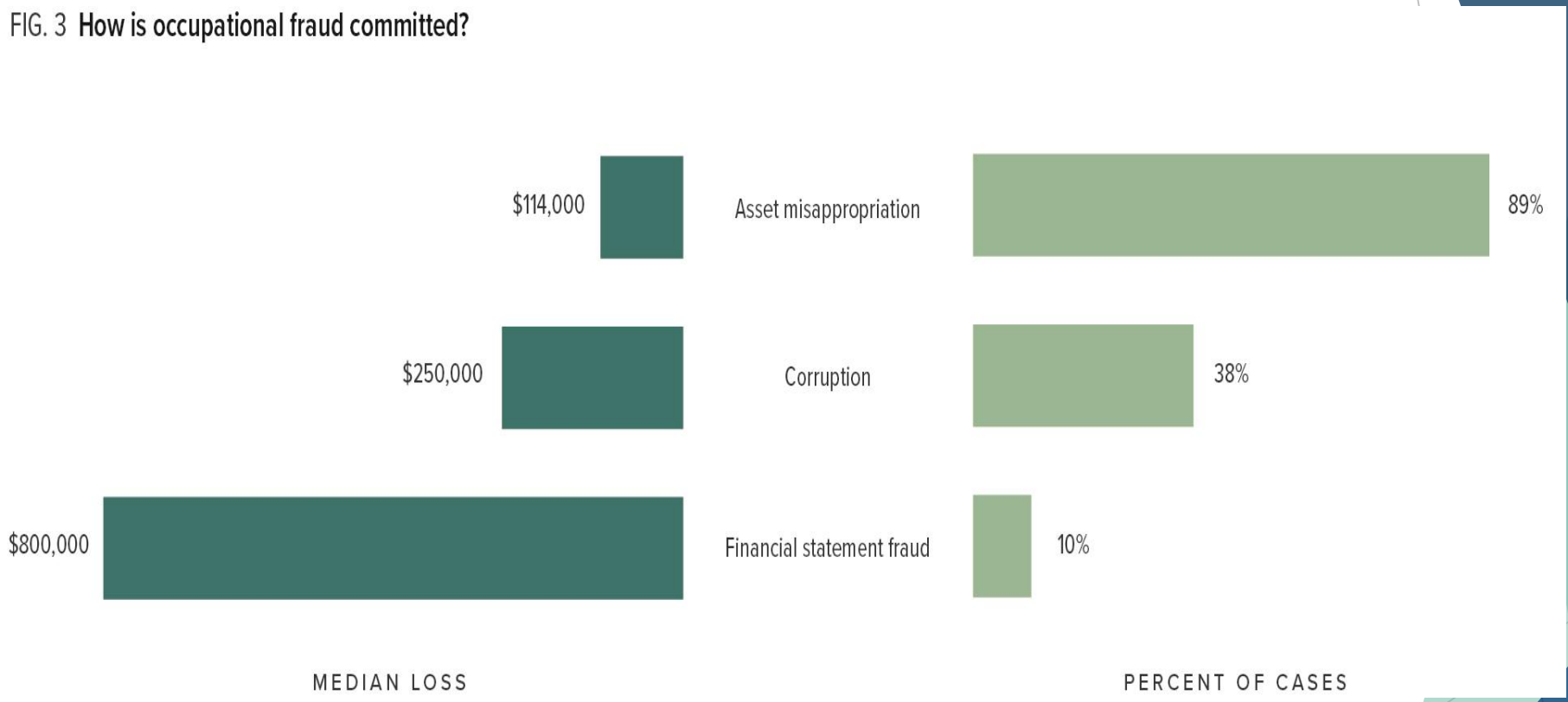


Capture

Internal Attacks

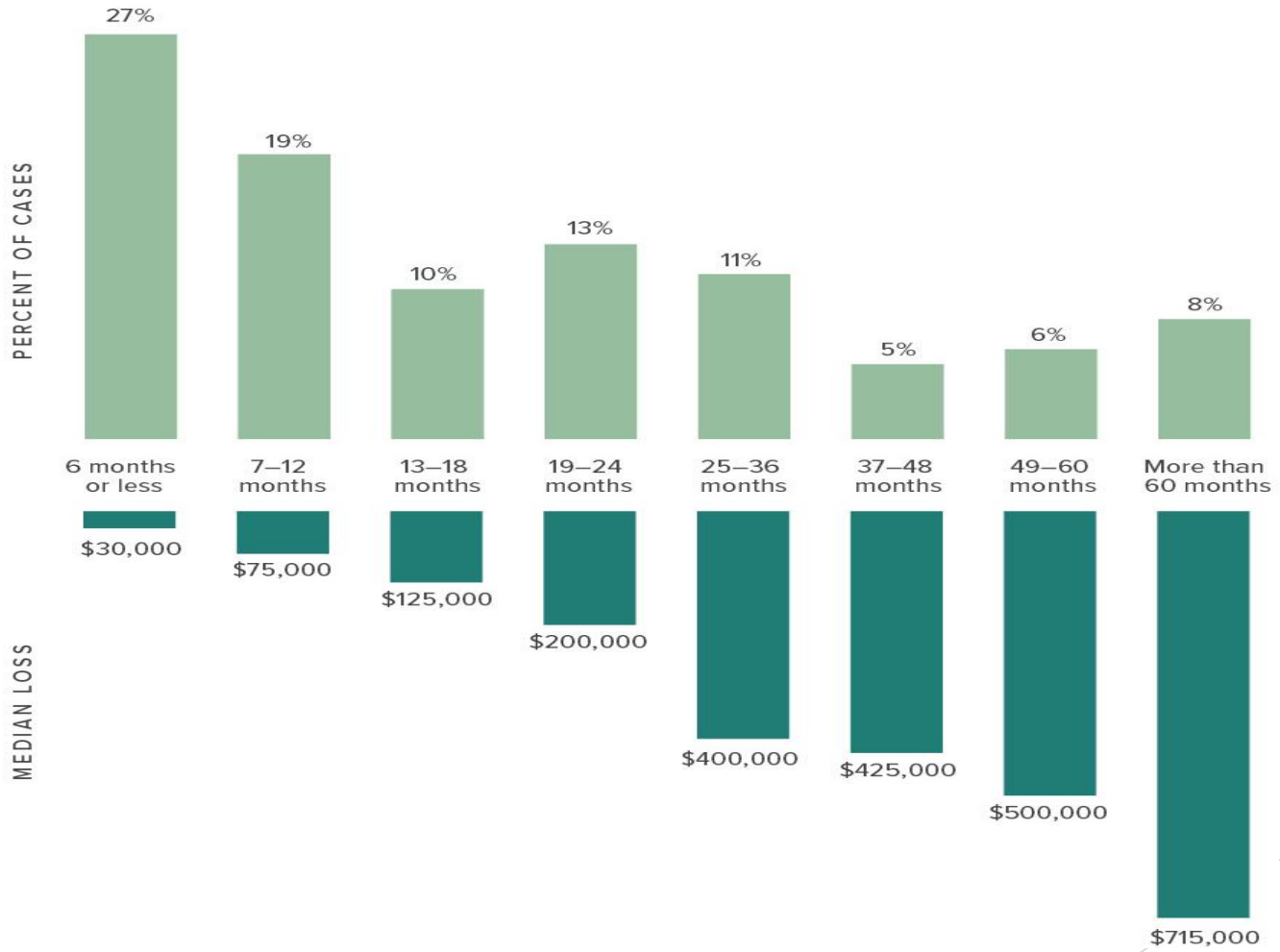
Exfiltration

How Occupational Fraud Is Committed



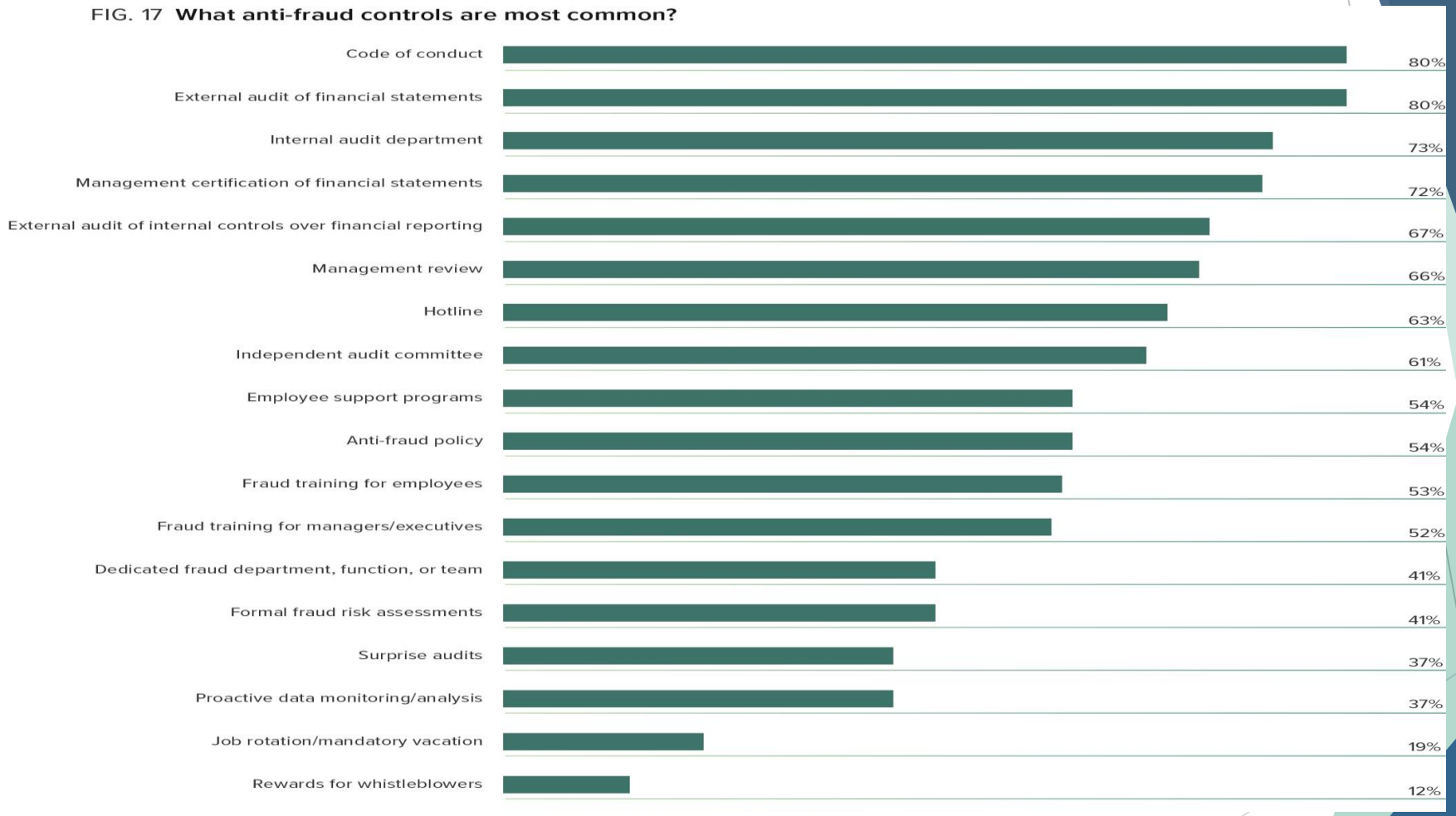
Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Duration of fraud schemes



Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Cited internal controls



Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

The Risk Assessment Team

- Accounting and finance
- Business unit and operations
- Risk management
- Legal and compliance
- Internal audit
- Management

Controls: Cash receipts

- Proper segregation of duties is key:
  - Receiving and recording payments
  - Use of lockbox
  - Daily deposits
  - “For deposit only” accounts
  - Bonded employees
  - Compare deposits to cash receipts journal

Controls: Cash disbursements

- Check writing and signing considerations
- ACH and Wire Transfer Approval Requirements
- Check requisitions and other support
- Vendor master files

Controls: The bank statement

- Reconciliation should be independent from cash receipts and cash disbursements functions
- Review of bank statement – Receipt of bank statement should be independent from person reconciling
- Review of cancelled checks
- Review of reconciliation

Controls: Other considerations

- Analytical review
- Reporting requirements
- Document policies and procedures
- Officer and Board responsibilities

Effectiveness of Controls

Control	Percent of cases	Control in place	Control not in place	Percent reduction
Code of conduct	80%	$ 110,000	$250,000	56%
Proactive data monitoring/analysis	37%	$ 80,000	$ 165,000	52%
Surprise audits	37%	$ 75,000	$ 152,000	51%
External audit of internal controls over financial reporting	67%	$100,000	$200,000	50%
Management review	66%	$100,000	$200,000	50%
Hotline	63%	$100,000	$200,000	50%
Anti-fraud policy	54%	$100,000	$ 190,000	47%
Internal audit department	73%	$108,000	$200,000	46%
Management certification of financial statements	72%	$109,000	$ 192,000	43%
Fraud training for employees	53%	$100,000	$ 169,000	41%
Formal fraud risk assessments	41%	$100,000	$ 162,000	38%
Employee support programs	54%	$100,000	$ 160,000	38%
Fraud training for managers/executives	52%	$100,000	$ 153,000	35%
Dedicated fraud department, function, or team	41%	$100,000	$ 150,000	33%
External audit of financial statements	80%	$120,000	$ 170,000	29%
Job rotation/mandatory vacation	19%	$100,000	$ 130,000	23%
Independent audit committee	61%	$120,000	$ 150,000	20%
Rewards for whistleblowers	12%	$ 110,000	$ 125,000	12%

Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse, ACFE

Key Takeaways & Action Items

- Get Started!
- Perform a Cyber Security Assessment
  - Identify Threats, Vulnerabilities and Risks
  - Understand Risk Areas to Address them
- Perform Internal Process Reviews
  - Identify and Address Control Issues
  - Identify areas for Process Improvement

Nexus of Fraud and Cyber

- Fake Employees
- Fake Vendors
- Fraud Schemes
- Fake Purchases
- Fake Returns
- Theft
- Skimming
- Payroll
- Billing
- Expense Reimbursement
- Check Tampering
- Register Disbursement

- Vendor Impersonation
- BEC/Wire Fraud
- Fake/Modified invoices
- Redirected Funds
- Fake Delivery
- Theft

Understand Our Environment – Data Flow