EMPLOYEE OWNED 2019

Cyber-Security Data Privacy: Part 1

THE CONFERENCE & TRADE SHOW

for **ESOPs**

CyberSecurity – The New Frontier: Part 1

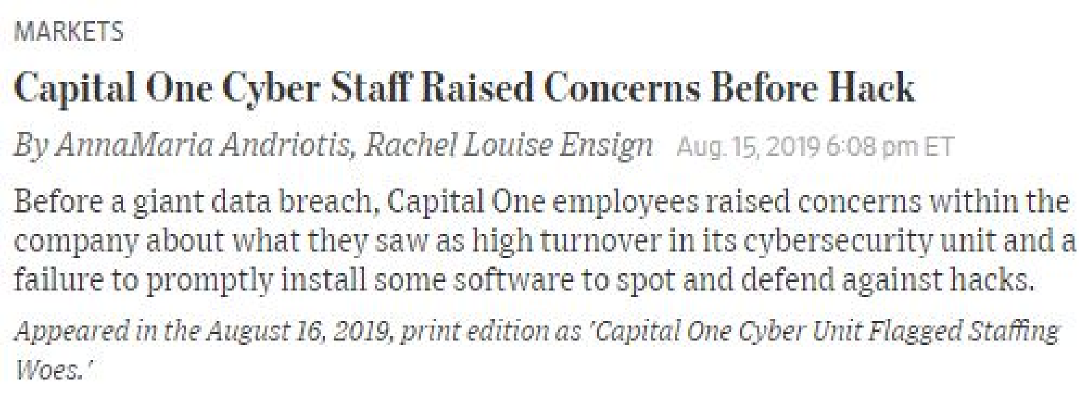
Susan Schaefer
Partner
Winston & Strawn, LLP
sschaefer@Winston.com

Jason Smolanoff
Sr. Managing Director
Kroll, Inc., a division of
Duff+Phelps
jason.smolanoff@kroll.com

Brian Ippensen
President
TI-TRUST, Inc.
brian.Ippensen@ti-trust.com

Why Focus on Cybersecurity?

- Continual and recurring attacks on data and its value
- Recent headlines:



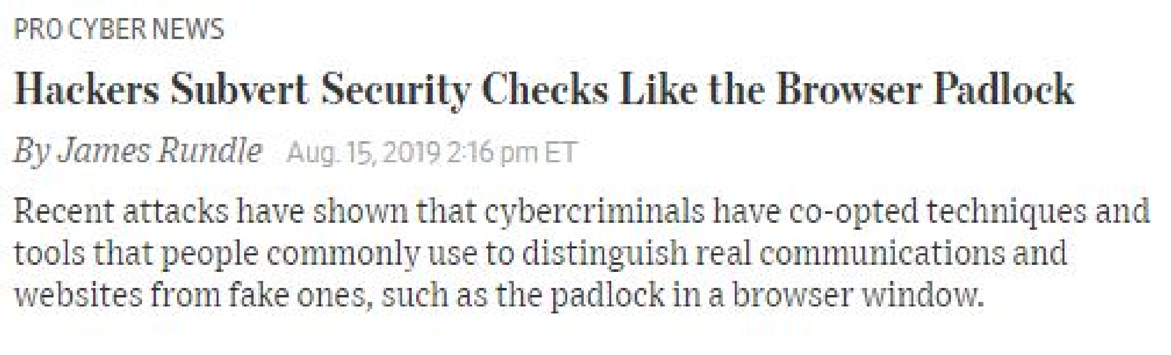
MARKETS

Capital One Cyber Staff Raised Concerns Before Hack

By AnnaMaria Andriotis, Rachel Louise Ensign Aug. 15, 2019 6:08 pm ET

Before a giant data breach, Capital One employees raised concerns within the company about what they saw as high turnover in its cybersecurity unit and a failure to promptly install some software to spot and defend against hacks.

Appeared in the August 16, 2019, print edition as 'Capital One Cyber Unit Flagged Staffing Woes.'



PRO CYBER NEWS

Hackers Subvert Security Checks Like the Browser Padlock

By James Rundle Aug. 15, 2019 2:16 pm ET

Recent attacks have shown that cybercriminals have co-opted techniques and tools that people commonly use to distinguish real communications and websites from fake ones, such as the padlock in a browser window.

Why Focus on Cybersecurity for EB?

- Employee benefit plans face significant cybersecurity threats
- Given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating
- There are numerous interfaces that provide potential entryways for cybercriminals
- A diligent plan fiduciary will take steps to prevent a cyber-breach

Data Available and Risks

- Personally Identifiable Information (PII):

  Social Security Numbers, account balances, current salaries, ages, e-mail addresses, passwords, home addresses, etc.

- Plan data could be used to:
  - Steal information to steal identities
  - Verify information to steal benefits
  - Acquire information to calculate benefits
  - Market additional services
- Public recognition that data has value

Cybersecurity Open Questions

- Is cybersecurity an ERISA fiduciary responsibility?
  - If so, does ERISA preempt state cybersecurity laws?
    - It is not clear that state privacy or cybersecurity statutes would be preempted by ERISA
- Plan sponsors and service providers already take seriously their responsibilities to protect participant data, but where are the lines of responsibilities and accountability in the event of a breach?
- Is data a plan asset?
- Who can grant permission to use participant information for marketing?

Current Government Landscape

- There is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans in the US
- ERISA is silent on data protection in the form of electronic records
- US courts have not yet decided whether managing cybersecurity risk is a fiduciary function
- There is no comprehensive federal scheme that covers all service providers, (not all service providers are subject to GLBA)
- Many service providers that service the retirement market are covered by federal rules based on their industry
  - However, note that these plan service providers often cross several different industries, making standard compliance rules difficult

Current Government Landscape

- Some states have started to create their own laws which typically address breach notifications and private rights of action for any unauthorized disclosures of protected personal information
- Several state attorneys general have been active in enforcing these laws in cyberbreach cases, but a state-by-state framework remains inconsistent in that regard

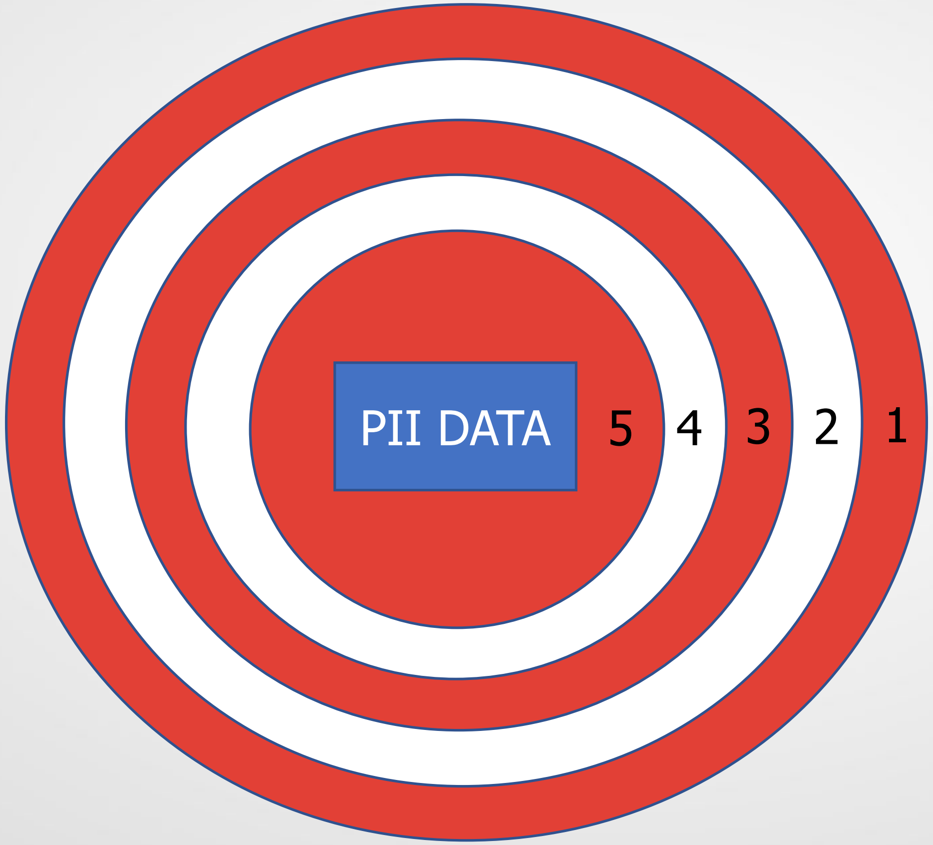
Government Efforts Regarding Cybersecurity

- United States Department of Labor’s Advisory Group
  - In a 2016 report, the ERISA Advisory Council concluded that complete prevention of cybersecurity threats is impossible, but there are steps that can be taken to limit the threat.
  - The ERISA Advisory Council asked the DOL to provide guidance on how to evaluate the cybersecurity risks they face and to require retirement plan sponsors to be familiar with the various security frameworks used to protect data as well as to build a cybersecurity process. The Council would also like the DOL to recommend that sponsors use third-party risk management
  - While ERISA does not mandate a written cybersecurity policy, plan sponsors are required to always act prudently and to document that process, and cybersecurity should be part of that process.

Private and Not-For-Profit Cybersecurity Organizations

- Not unique to employee benefit plans, significant cybersecurity efforts have been, and continue to be, developed to help organizations manage and navigate cyber-risk
- The American Institute of Certified Public Accountants (AICPA)
  - They prepared a Q&A by the EBPAQC to help plan auditors understand cybersecurity risk in employee benefit plans, and to discuss cybersecurity risk, responsibilities, preparedness, and response with plan clients
  - https://www.aicpa.org/content/dam/aicpa/interestareas/employeebenefitplanauditquality/resources/accountingandauditingresourcecenters/downloadabledocuments/cybersecurity-and-ebp-questions-and-answers.pdf
- The SPARK Institute

Cybersecurity in Retirement Industry



WHY YOU NEED TO CARE

Between 27 November and 15 December 2013, more than 40M credit card details and 70M pieces of personal information were stolen from Target, a major US retailer.

Total loss $292M

- Insurance covered less than 30% ($90M)
- $153M awarded in 80 lawsuits
- D&O Suit
- Doesn't include lost revenue
- Reduced sales - took a year to recover

What Constitutes Reasonable Security?

The 20 Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet.

The failure to implement all the Controls that apply to an organization's environment **constitutes a lack of reasonable security**.

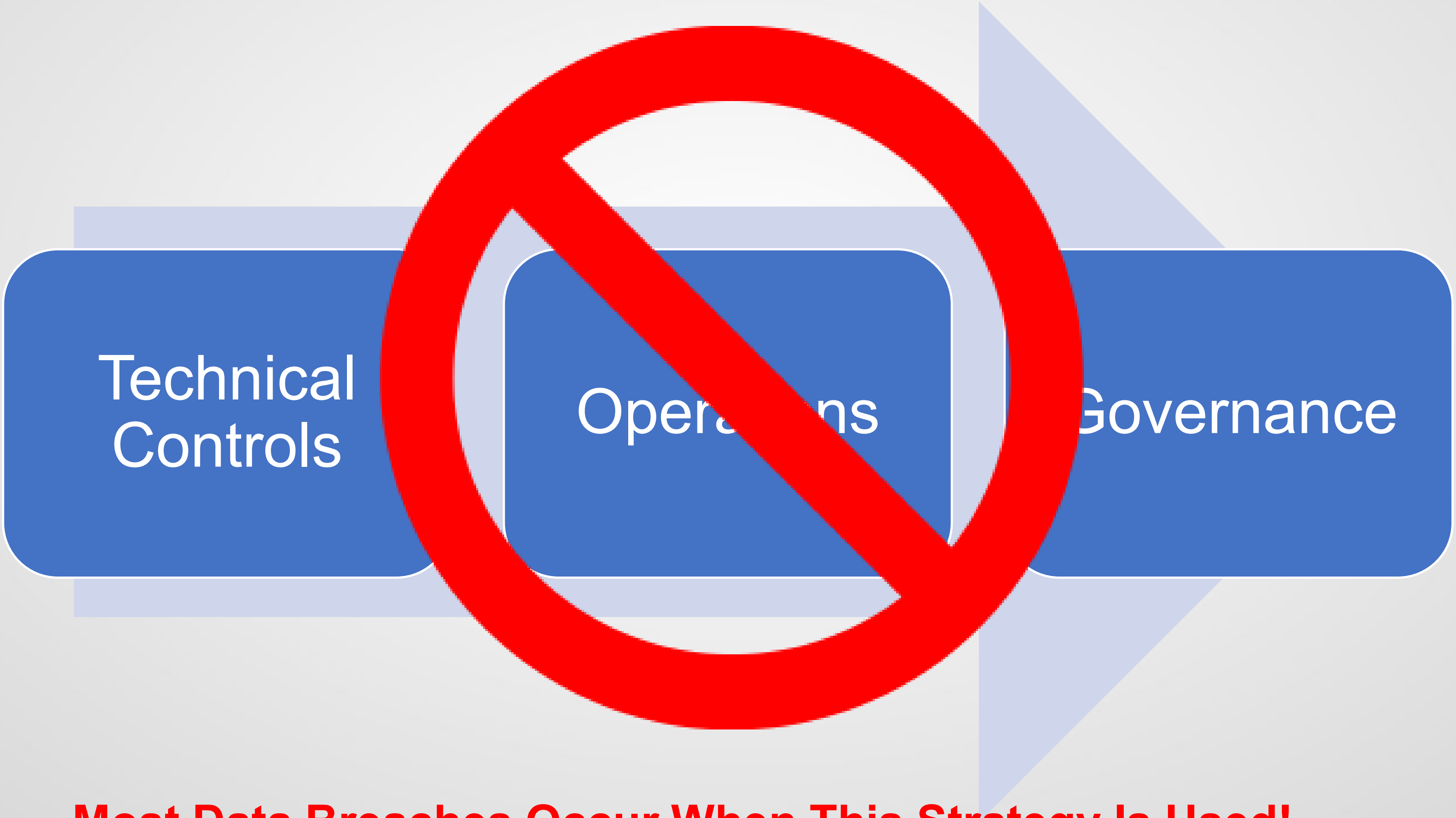
California Data Breach Report (Feb 2016) Attorney Gen. Kamala D. Harris

Most effective strategy to mitigate risk

1. Technical controls
2. Operations
3. Governance

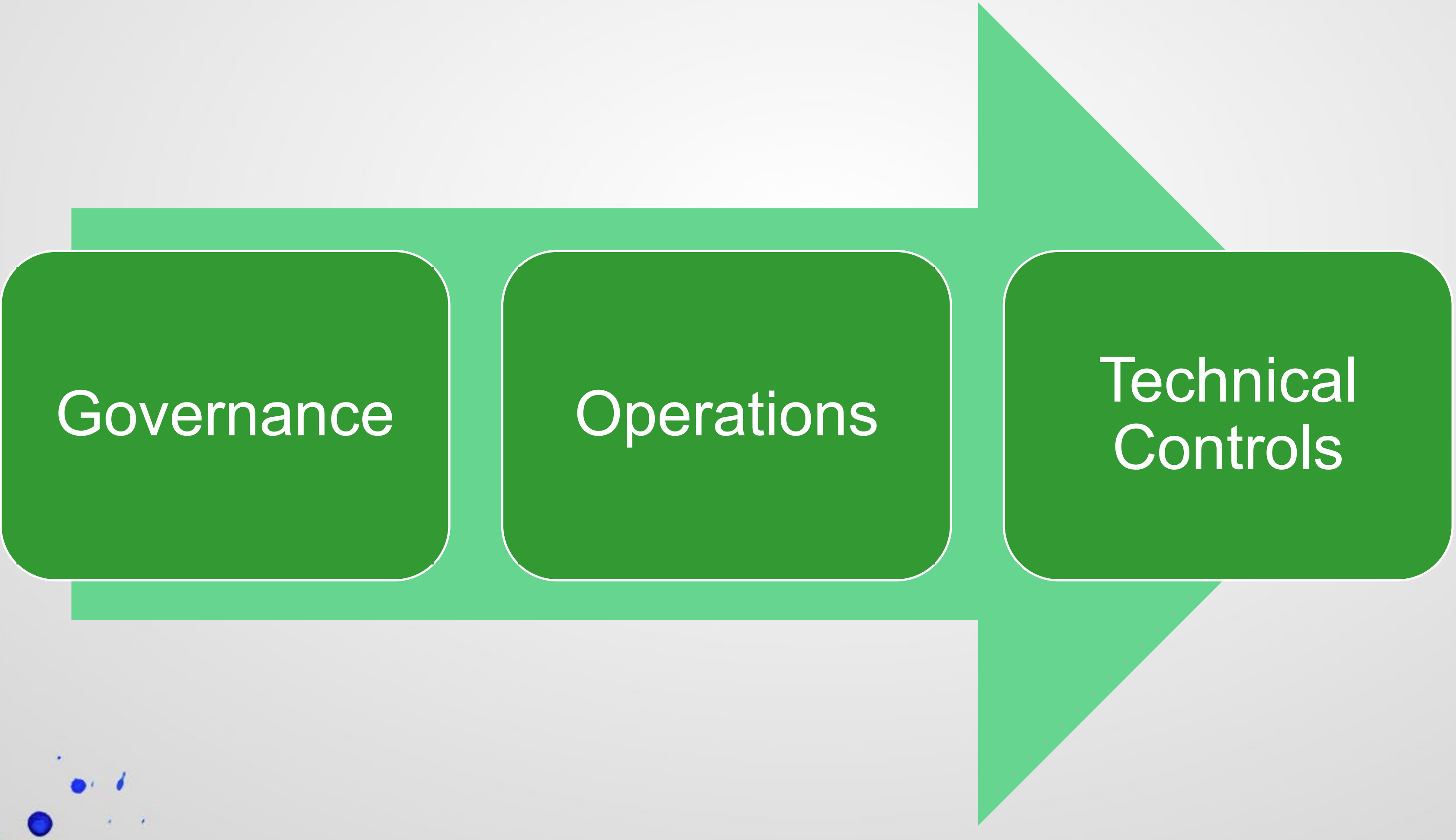
1. Governance
2. Operations
3. Technical controls

Tool Based Strategy?



Most Data Breaches Occur When This Strategy Is Used!

Governance Strategy

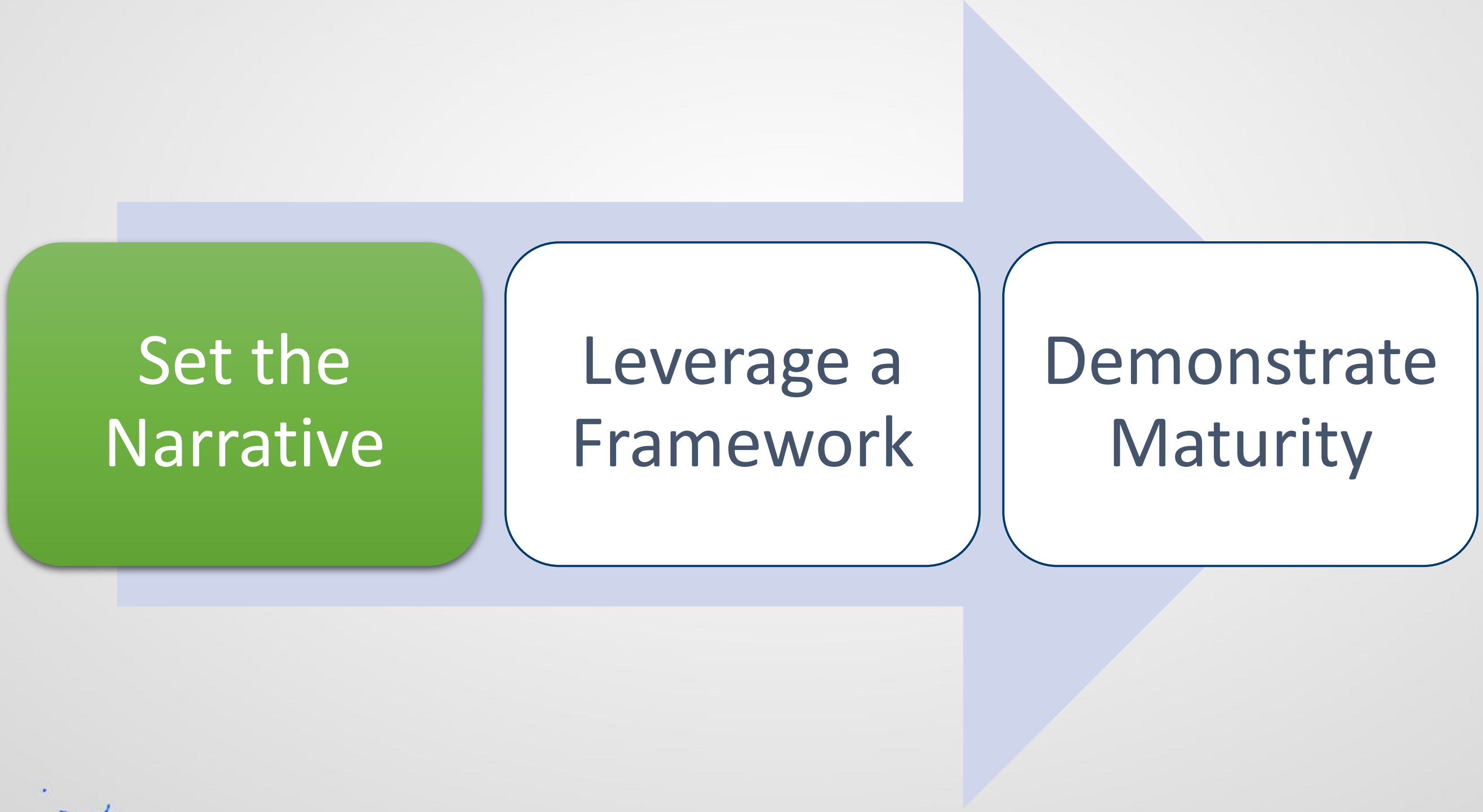


Governance

Operations

Technical Controls

Strategic Components



Set the Narrative

Leverage a Framework

Demonstrate Maturity

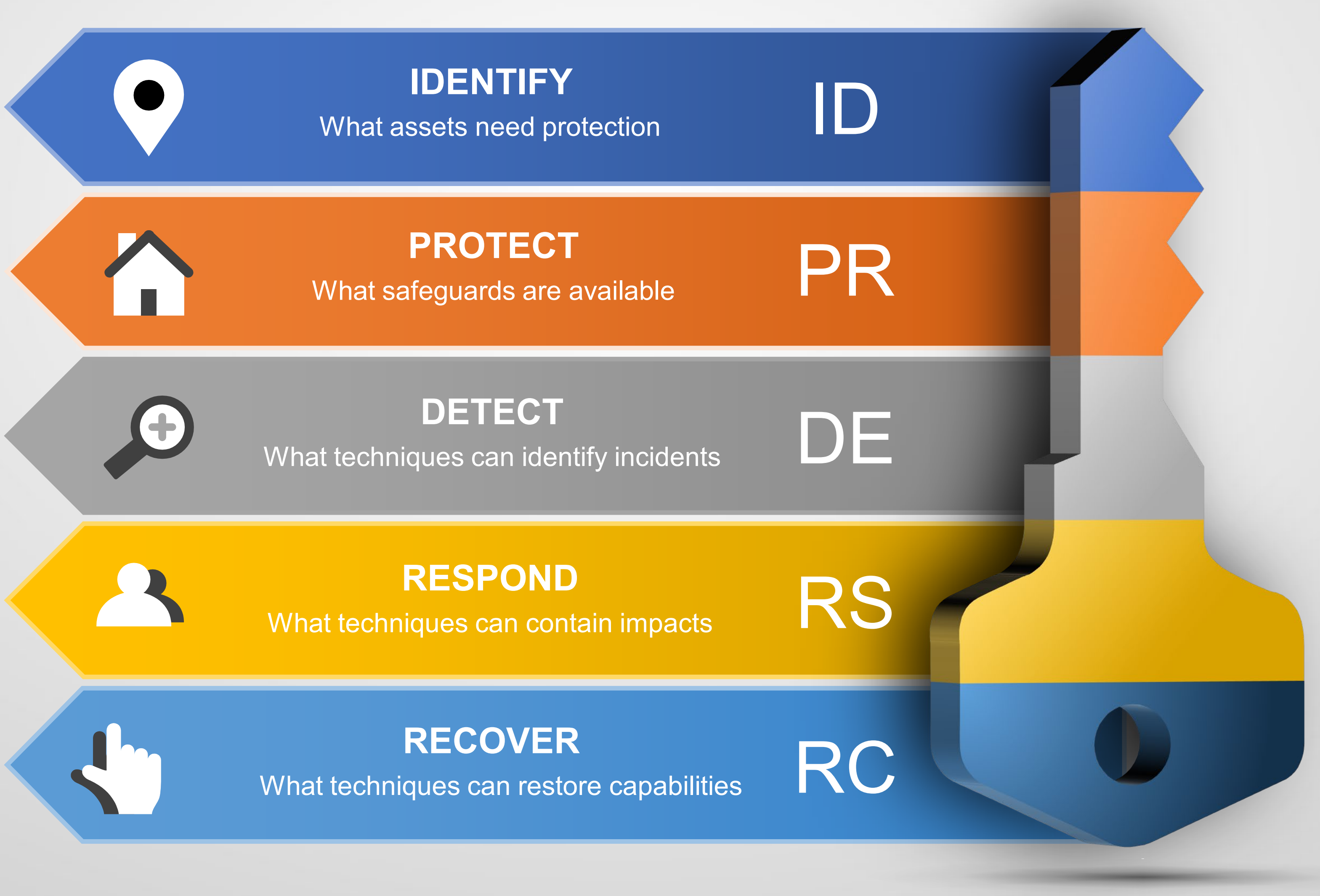
Set the Narrative

- Reasonable Measures Implemented
- Attacker Used Extraordinary Methods
- *<u>Rapidly Detect and Effectively Respond</u>*

What is Your Narrative?

Leverage a Framework

Five concurrent & continuous functions



IDENTIFY ID
What assets need protection

PROTECT PR
What safeguards are available

DETECT DE
What techniques can identify incidents

RESPOND RS
What techniques can contain impacts

RECOVER RC
What techniques can restore capabilities

#EO2019

ESOP™

Framework Core: Functional & Risk-Based

What assets need protection

What safeguards are available?

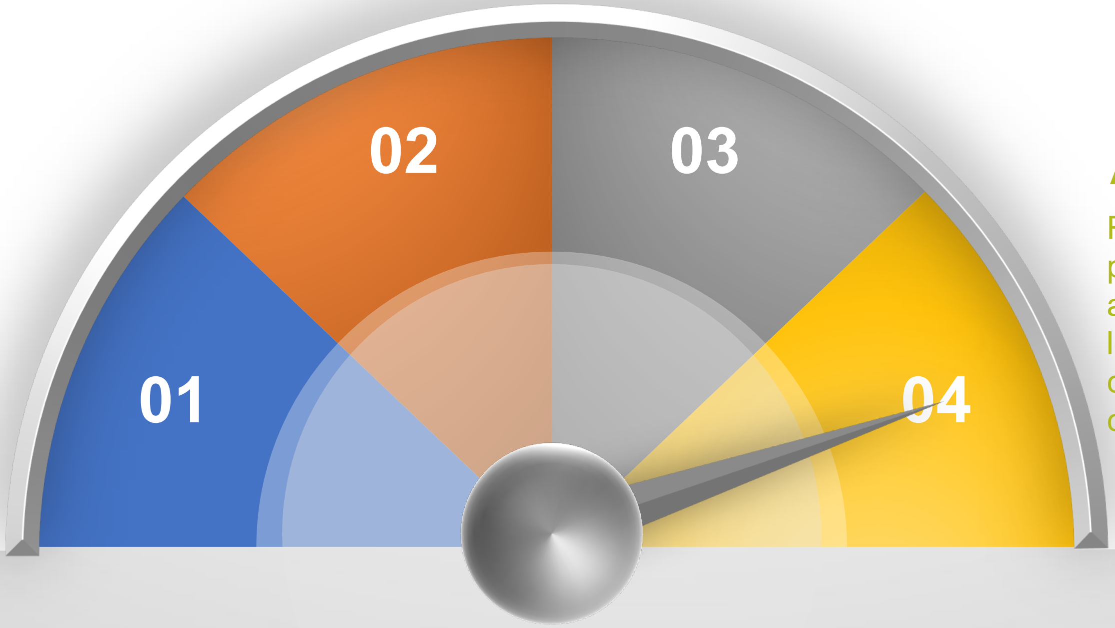
What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

FUNCTION IDENTIFIER	FUNCTION	CATEGORY IDENTIFIER	CATEGORY
ID	IDENTIFY	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	PROTECT	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.PT	Protective Technology
DE	DETECT	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Process
RS	RESPOND	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	RECOVER	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Demonstrate Maturity



PARTIAL

Risk-management is ad hoc, with limited awareness of risks and no collaboration with others

RISK INFORMED

Risk-management processes and program are in place but are not integrated enterprise-wide; collaboration is understood but organization lacks formal capabilities

REPEATABLE

Formal policies for risk-management processes and programs are in place enterprise-wide, with partial external collaboration

ADAPTIVE

Risk-management processes and programs are based on lessons learned and embedded in culture, proactive collaboration

#EO2019

ESOP™

Questions?

Susan Schaefer

Winston & Strawn, Partner

Susan Peters Schaefer advises clients on a wide range of matters that affect employee benefit plans, such as mergers and acquisitions, fiduciary responsibility issues, Employee Retirement Income Security Act (ERISA) controversies, and prohibited transactions. She also represents clients before the Internal Revenue Service and the Department of Labor. She counsels clients such as global manufacturing and service companies, small business, fiduciaries, and financial institutions as well as corporations, individuals, and fiduciaries in a variety of corporate transactions. Susan assists clients with negotiation of employment and non-compete agreements, the development of succession plans, and the implementation of executive compensation plans

sschaefer@winston.com

EMPLOYEE OWNED 2019

ESOP™

Jason Smolanoff

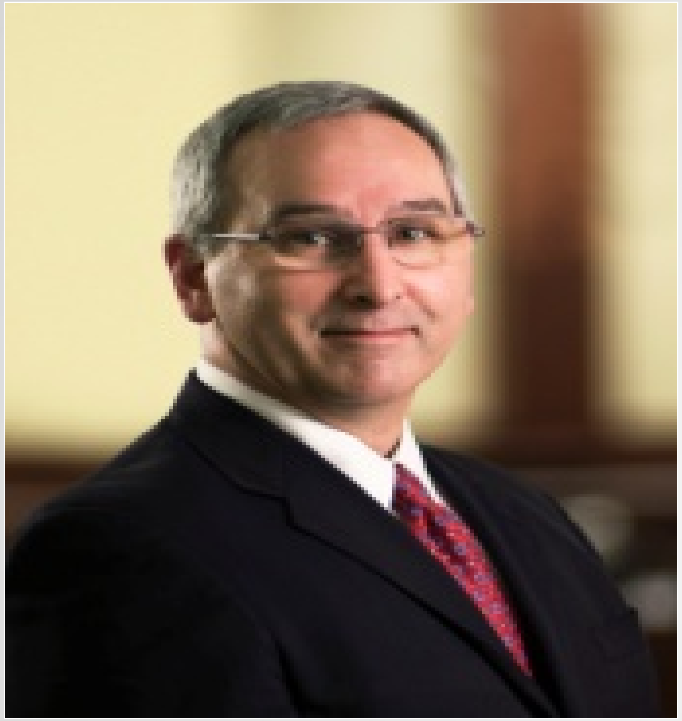
Senior Managing Director and Global Cyber Security Practice Leader

Jason is a Senior Managing Director and the Global Cyber Security Practice Leader for Kroll, a division of Duff & Phelps. He has more than 19 years of federal law enforcement and information security experience and has played a leading role some of the most significant cyber security investigations in history. Jason serves as a Commissioner for the San Manuel Gaming Commission and is also a member of the Loyola Law School's Cybersecurity and Data Privacy Advisory Group.

jason.smolanoff@duffandphelps.com

EMPLOYEE OWNED 2019

ESOP™



Brian Ippensen

TI-TRUST, Inc. President

BS Agricultural Economics, University of Illinois – Champaign. Brian's past work experience includes staff and in-charge for public accounting and audits of banks and retirement plans; cost accounting for edible oil refinery and bean crushing manufacturing; international accountant for foreign export sales; retail banking operations.   Brian currently serves on the Board of Directors and is the Chairperson of the Fiduciary Committee for The ESOP Association. Brian joined TI-TRUST, Inc., in 1997. He was appointed President January 1, 2006 and also serves as board member.

brian.ippensen@ti-trust.com

EMPLOYEE OWNED 2019

ESOP™