EMPLOYEE OWNED 2019

Cyber-Security Data Privacy: Part 2

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

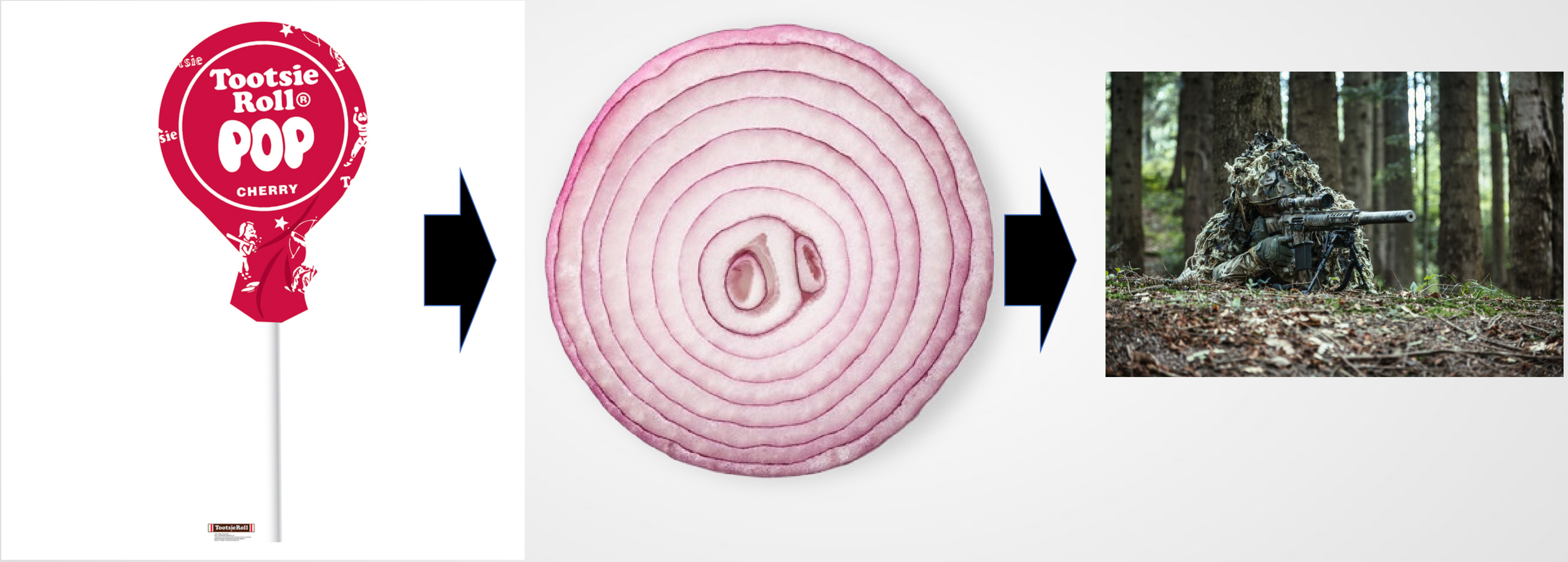
Cyber Resilience: *Building a defensible strategy*

Most effective strategy to mitigate risk- Governance

1. Technical controls
2. Operations
3. Governance

1. Governance
2. Operations
3. Technical controls

Breach Methodologies

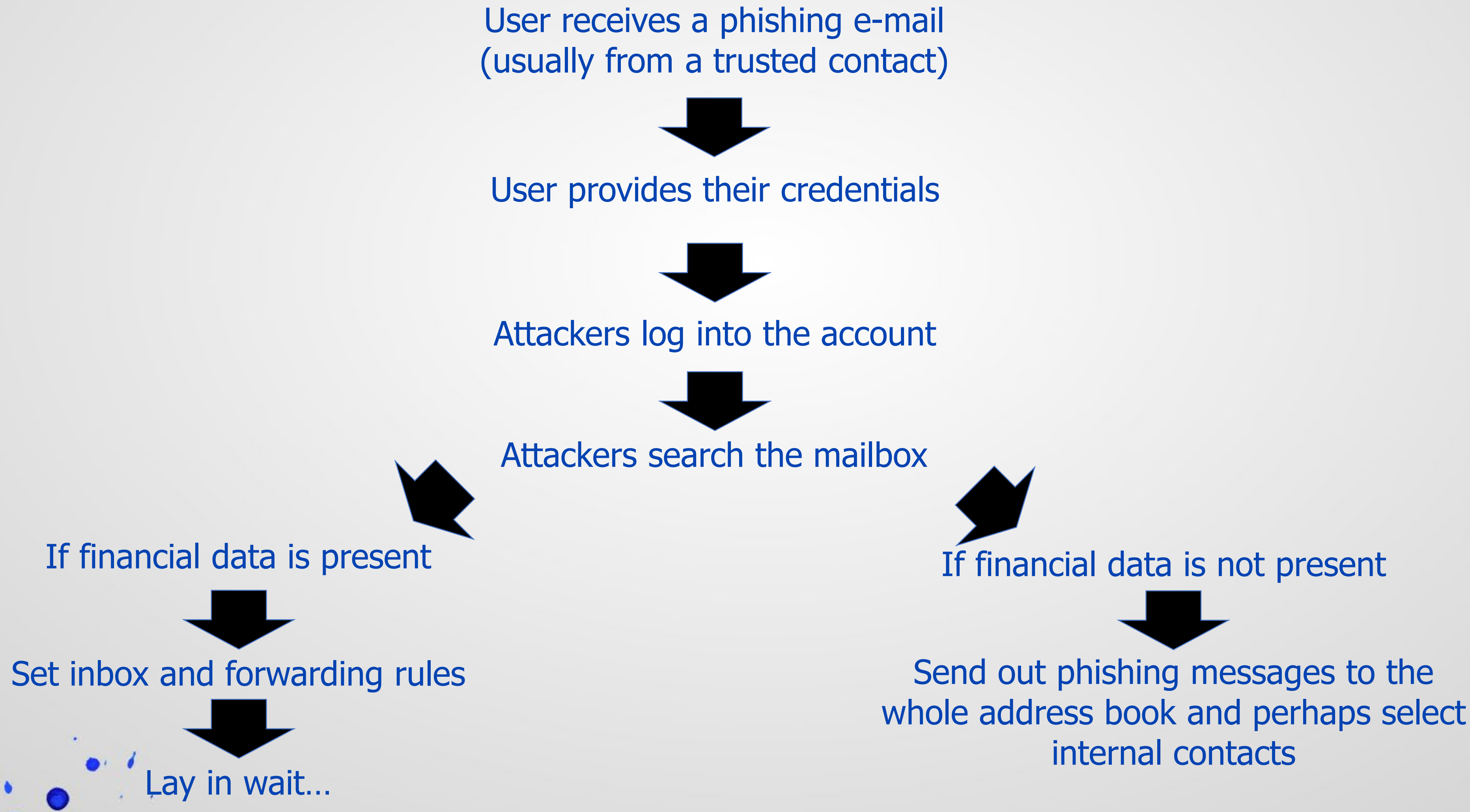


"Our Firewall Will Save Us from Everything"

Defense In Depth

Continuous Breach Theory

Business E-Mail Compromise



User receives a phishing e-mail
(usually from a trusted contact)

User provides their credentials

Attackers log into the account

Attackers search the mailbox

If financial data is present

Set inbox and forwarding rules

Lay in wait…

If financial data is not present

Send out phishing messages to the whole address book and perhaps select internal contacts

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- To educate and assist plan sponsors in their compliance efforts, the US DOL ERISA Advisory Council created the Cybersecurity Considerations Document
  - Prevention of a cybersecurity threat is impossible, but there are steps that can be taken to limit the threat
  - At present, there is no consensus within the industry regarding which cybersecurity framework constitutes a ‘best practice’ approach
  - Not a “one-size-fits-all” approach
  - Determine what is reasonable from a commercial perspective and an ERISA perspective for each plan
  - The cybersecurity risk management strategy cannot be a static checklist
  - The program should include regular reporting, frequent reviews and process updates that are specifically tailored to the plans’ needs

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Inventory the plan's data, and consider using, sharing and maintaining only the minimum amount of data necessary. This applies to the plan sponsor's data, as well as that used, shared and maintained by service providers
- Devise a framework upon which to base a cybersecurity risk management strategy (e.g., the NIST framework or the SAFETY Act as models or possible starting points)
- Establish a process that includes, implementation, monitoring, testing and updating, reporting, training, controlling access, data retention and/or destruction, and third party risk management
- Balance the scope and cost of a cyber-risk management strategy against the size and sophistication of the plans and the plan sponsor
- Decide what if any portion of the cyber-risk management costs should be borne by the plan, versus the plan sponsor, including insurance
- Ensure that any program also addresses any state specific cyber-risk requirements

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Service Providers
  - Review applicable contract provisions with service providers, and require vendors to attest that the service provider or vendor has proper procedures in place to protect the plan's data
  - Plan sponsors should monitor the cyber protocols and practices of these providers on an on-going basis to ensure they are robust enough
  - Plan sponsors, fiduciaries and third party service providers may want to consider whether SAFETY Act certifications could fit into their overall cybersecurity risk management strategy
    - Plan sponsors can take advantage of the Act's liability protections by retaining vendors that have or use SAFETY Act approved processes or procedures

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Insurance
  - Plan sponsors should evaluate their insurance coverage/bonding policies to ensure they are covered in the case of a cybersecurity attack
  - A Fiduciary may look into purchasing an insurance policy or bond to protect against potential loss to the plan and plan participants
  - Discussions with insurance brokers has led us to understand that a few different coverages (e.g., a cyber-policy, a crime policy, errors and omissions and fiduciary insurance) may all need to be bundled to provide a comprehensive solution
  - It is also important to address cyber-breaches which can occur at different plan interfaces, e.g. at the trustee, participant or administrator's interface
    - A negative factor with respect to insurance coverage is where the actual cyber-breach occurs may dictate whether the insurer will pay the claim

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Insurance
    - It is also important to address cyber-breaches which can occur at different plan interfaces, e.g. at the trustee, participant or administrator’s interface
        - A negative factor with respect to insurance coverage is where the actual cyber-breach occurs may dictate whether the insurer will pay the claim
        - Unless the cyber-breach occurs at the plan sponsor’s interface, the claim may be refuted
        - Even if a plan sponsor has adequate insurance coverage, the insurer may refuse to pay a claim if the breach happens at the site of the service provider, or if the plan participant’s negligence led to the breach
        - It is critical to get counseling on the appropriate Cyber Insurance plan to cover your specific needs

Top 20 Critical Security Controls

1	Asset Inventory
2	Software Inventory
3	Secure Hardware & Software Configurations
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Admin Privileges
6	Maintenance, Monitoring and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols & Services
10	Data Recovery Capability
11	Secure Network Configurations
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Training
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Implications for the Director

Responsibilities you cannot shift to management

1 **RESPONSIBLE FOR RISK**

If a Cyber risk is raised to you, either mitigate it or risk accept it; do not ignore it.

2 **SHOW: BUSINESS JUDGEMENT**

Make Cyber a regular topic

3 **SHOW: OVERSIGHT**

Get the right metrics on status of security regularly

Review Cyber incident reports to monitor attacks and trends

4 **KNOW THE LAW**

Get advice on privacy and data regulation in markets you operate

5 **GET RISK ASSESSED**

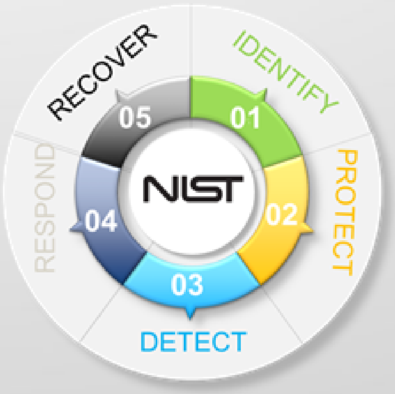
- Internally
- By third parties

6 **USE KNOWN FRAMEWORKS**

- NIST-
- ISO
- COBIT

7 **RESPONSE**

Test the company response



#EO2019

10 Lessons from 10 Years of Incident Response & Active Threats

1 Denial: It won’t happen to us…

…we don’t have data hackers are interested in…

2 People: Training…

…and testing those users, with consequences…

3 Multifactor Authentication

Not just for remote access

4 Business Continuity/Disaster Recovery: Backups

How much can you afford to lose?

5 Solid Network Fundamentals

Make it hard for the attackers one they are in…

- Patching
- Host Based Firewalls
- Network Segmentation
- Least Privilege & Separation of Roles

6 Endpoint Monitoring

EDR: Endpoint Detection & Response

EMPLOYEE OWNED 2019

ESOP™

7 Logging

Keep a year of logs (network, firewall, authentication, access) at a minimum…

8 Letting AV “Remove a Problem” doesn’t always remove the problem

Multistage malware is here to stay

9 Policy without technical controls is worthless

Hackers don’t care about policy…

10 Have cyber insurance and sign a MSA in advance with one or more Incident Response providers…

Sign a zero dollar or low dollar MSA with a provider on panel

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

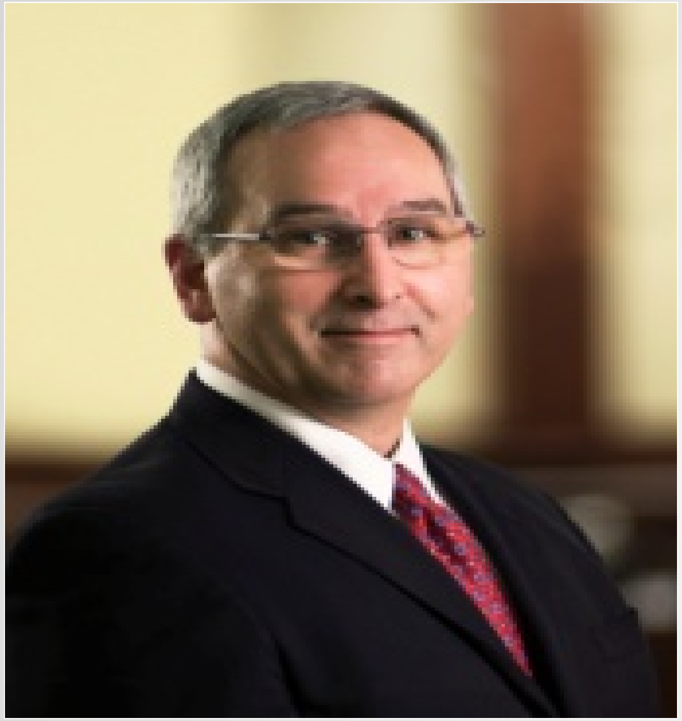
Senior Managing Director and Global Cyber Security Practice Leader

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™