ABA® INSURANCE
Administered by USI Affinity

USI AFFINITY | designedprivacy | XPAN LAW

Real World Cyber Risks for Attorneys

Educational Webinar for American Bar Association Members

Please Note: This webinar is for informational purposes only. Opinions shared by the panel do not reflect the official position of the ABA. Information compiled and used for this presentation was provided by insurance carriers, subject matter experts, clients and other sources of information which was gathered over time.

AGENDA

- Speaker Introductions
- Covid-19 Effects on Cyber Threats
- Why Law Firms
- Cyber Losses
- Risk Management
- Cyber Insurance
- Live Question & Answer Session

Introduction

Doug Kreitzberg

CEO, Designed Privacy, LLC

- Bio Information Here

Mike Mooney

Senior Vice President & National Practice Leader, USI Affinity

- Bio Information Here

Rebecca Rakoski

Managing Partner, XPAN Law Partners

- Bio Information Here

Covid-19 Effects

Increased Attacks

- Up to a 700% increase in phishing emails, including BEC – Theft of Funds
- Attacks on devices and remote network vulnerabilities
  - Network/Device Mapping, Inventory, Security and Patching
- Business Associate, Software Supply Chain and Cloud Attacks – Theft of Data
  - Data Mapping, Vendor Risk Management Program, BAA, Cyber Insurance
- Ransomware Attacks – Patient Care and Safety Issue. Encryption of Data
  - Redundant Offline Backups, Patching, Incident Response Plan and Exercise
- Theft of COVID Related Research, Treatment Protocols and Vaccine Research
  - Risk Management Program to Identify Risk and Protect Research and Preserve Government Funding

Target Rich Environment

- National Security
- Intellectual Property
- Business Intelligence
- Protected Health Information
- Bank Account and Credit Card Information
- Personally Identifiable Information

Cyber Exposures – Law Firms Are Prime Targets

Rich Collection of Data

- Sensitive Information
- Bank Information
- PII

Poor Safeguards

- Lack of internal training and controls
- Lack of IT resources
- Wireless access
- Vendor Management
- Lost of stolen devices

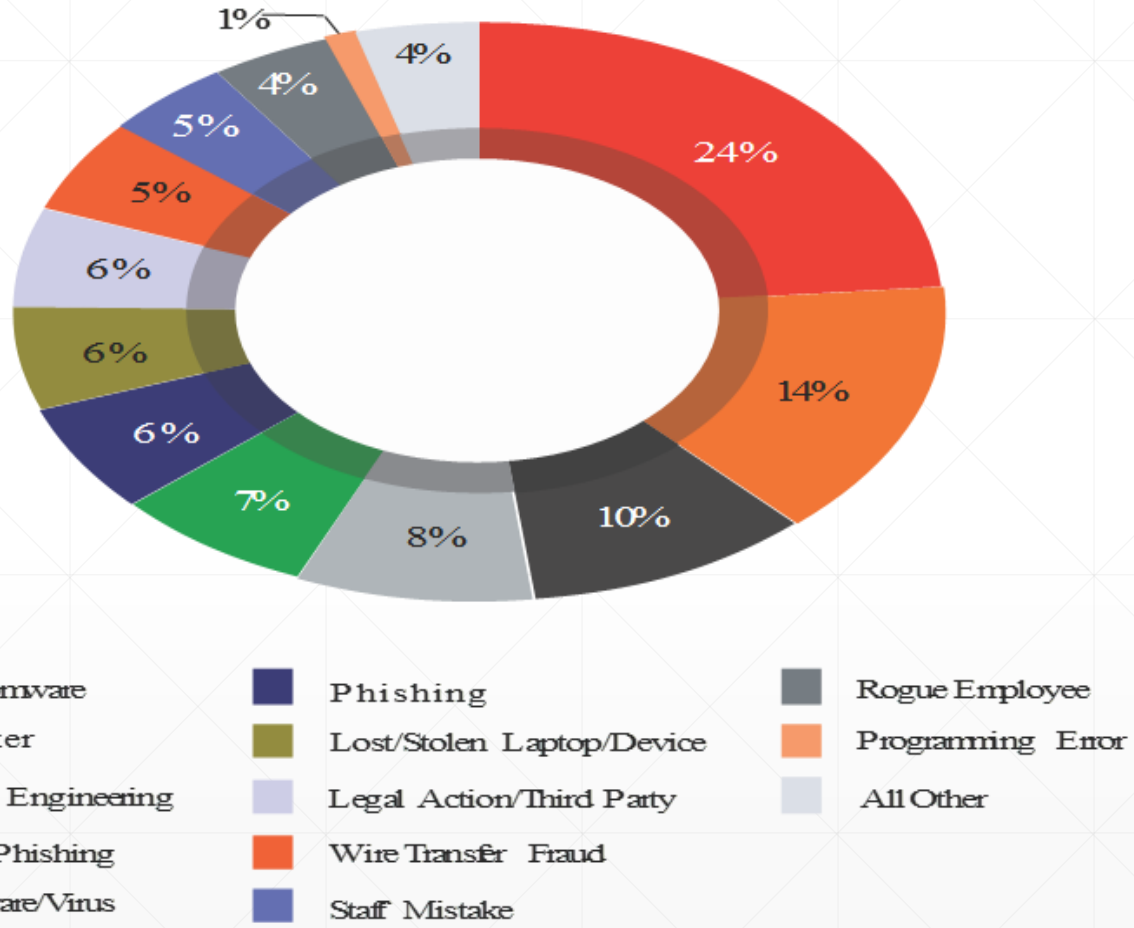
Internal Exposures

- Rogue employees
- Careless staff

External Exposures

- Business associates, vendors and suppliers
- Organized crime
- Hackers

Claim Statistics – By Cause of Loss



Source: NetDiligence Cyber Claims Study

High Cost of Data Breach

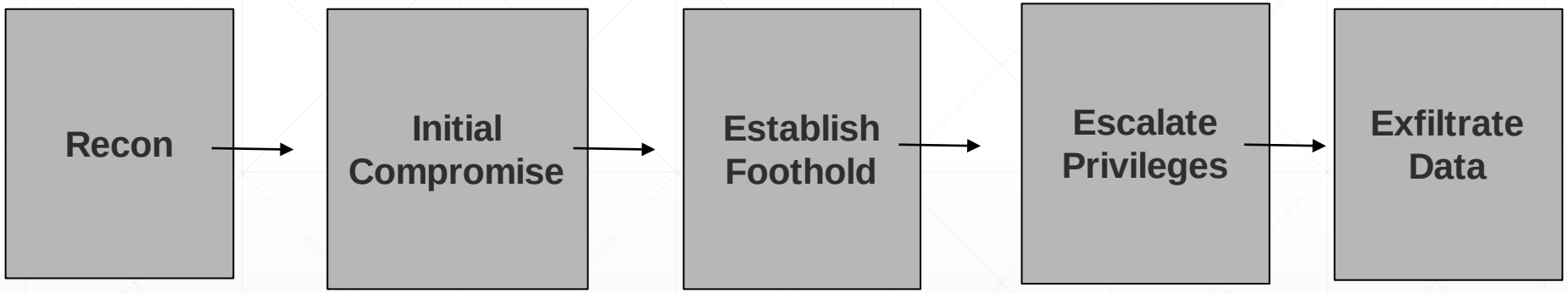
IBM Security: Cost of a Data Breach Report 2020

- $3.86 Million→ Global Average
- $150/ record for PII data
- $8.64 Million→ United States Average

Cyber Exposures – Cyber Loss

- Loss or damage to data/information
- Loss of revenue due to a computer attack
- Extra expense to recover/respond to a computer attack
- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches (not just computers!)
- Regulatory actions and scrutiny
- Loss or damage to reputation
- Cyber-extortion
- Cyber-terrorism
- Management time expended on breach response

Anatomy of Cyber Breach



Competence and Diligence

Rules 1.1 and 1.3

- Competence – A lawyer shall provide competent representation to a client requiring the legal knowledge, skill, thoroughness and preparation reasonably necessary got the representation – derived from ECs
  - Eliminates the concept of "zealous" representation in favor of "competence"
  - Part of "competence" is "keeping up with the times"
- Diligence – A lawyer shall
  - Act with reasonable diligence and promptness in representing a client
  - Not neglect a legal matter entrusted to the lawyer

Social Engineering

- Social Engineering is the psychological manipulation of legitimate users into performing actions, breaking security procedures, divulging confidential information and parting with tangible assets

- Social Engineering scams take advantage of the "human factor" to perpetrate a fraud

Social Engineering – NOT AN ISSUE FOR MY LAW FIRM

- **WRONG!**
- 26% of all law firms already victim of a data breach
- 51% of law firms have taken no measures to prevent data breach
- 50% have no data breach response plan
- Ransomware attacks occur every 10 seconds

Information compiled and used for this presentation was provided by insurance carriers, subject matter experts, clients and other sources of information which was gathered over time.

Types of Social Engineering Scams

- Email/fax from “client” to law firm with change in payment instructions
- Email/fax from “law firm” to client with change in payment instructions
- “Internal” email directed payment or turn over of personal information from partner/management level employee
- Email impersonating third party vendor

Examples of Social Engineering Scams Involving Law Firms

- Misdirection of Escrow Funds
- Fraudulent court notices
- Fake job posting/resumes for review
- Bank account/LinkedIn/Netflix password reset/purported "unauthorized access"
- Email with incoming fax notification
- Recent Examples of Ransomware Attacks:
  - 3 small SD Law Firms were subject to ransomware and threated to expose confidential data
  - TX boutique firm client data was released because of a ransomware attack

Ransomware Trends 2020-2021

- Attacks are highly targeted against specific entities
- Phishing emails is still the primary "attack vector" – because it's simple and it works
- Increasing in sophistication and severity. Ryuk, Conti and DopplePaymer, Mamba, Nefilim
- Network and data backups may be targeted first
- Ransomware may now execute within hours or minutes upon initial compromise leaving very little reaction time to identify and contain
- Ransom demands are increasing and scaled based upon size of organization targeted, multi-million dollar requests common, reports of ransom demands exceeding $60,000,000 in 2020
- High volume/disruptive telephone calls to executives and staff demanding ransom payment.
- Ransomware attack combined with other cyber crimes - data extortion. Criminals threaten to sell /publish stolen data

Avoiding Social Engineering Scams

- Use common sense
- Avoid clicking on links in emails
- Utilize SPAM filters, malware detectors and anti-virus software
- Click on “details” for email address of sender
- Verify with a phone call to client/law firm
- Secure and frequent backups
- Note: ABA Formal Op. 477 (May 11, 2017) (using encrypted emails)

WHEN WE THINK OF CYBER ATTACKS,

WE OFTEN THINK OF THIS.....

ABA INSURANCE
Administered by USI Affinity

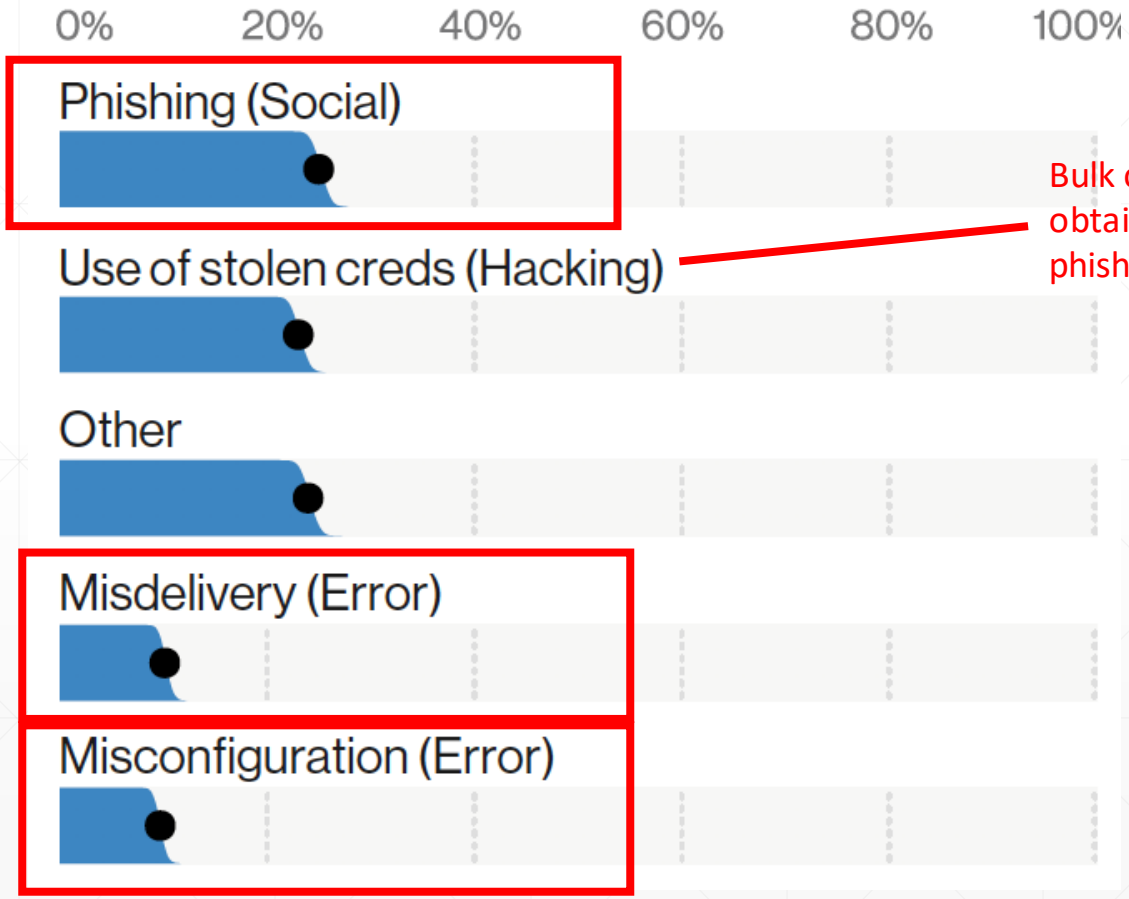
WHEN IN FACT,

WE SHOULD BE LOOKING HERE.....


WE HAVE MET THE ENEMY AND HE IS US.
© 1971 WALT KELLY

If you want to address Cyber Risk, you need to focus on Human Risk: Phishing and Errors represent 3 out of the top 5 threat actions, and Errors have been growing consistently year over year.

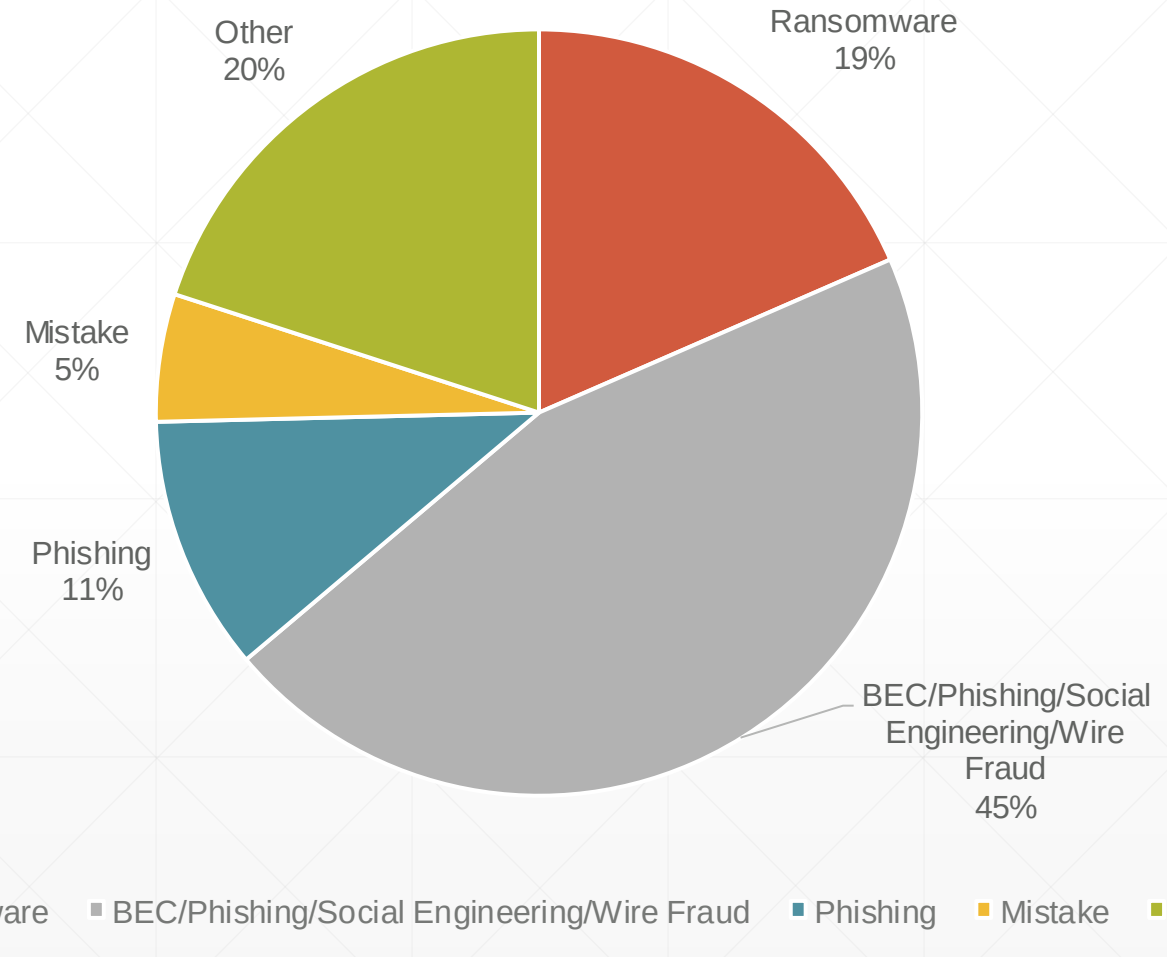
Figure 13. Top threat Action varieties in breaches (n = 2,907)



Source: Verizon DBIR 2020

HUMAN RISK ACCOUNTS FOR OVER 65% of PROFESSIONAL SERVICE CYBER LOSSES

Professional Services Cause of Loss – SINCE 2018

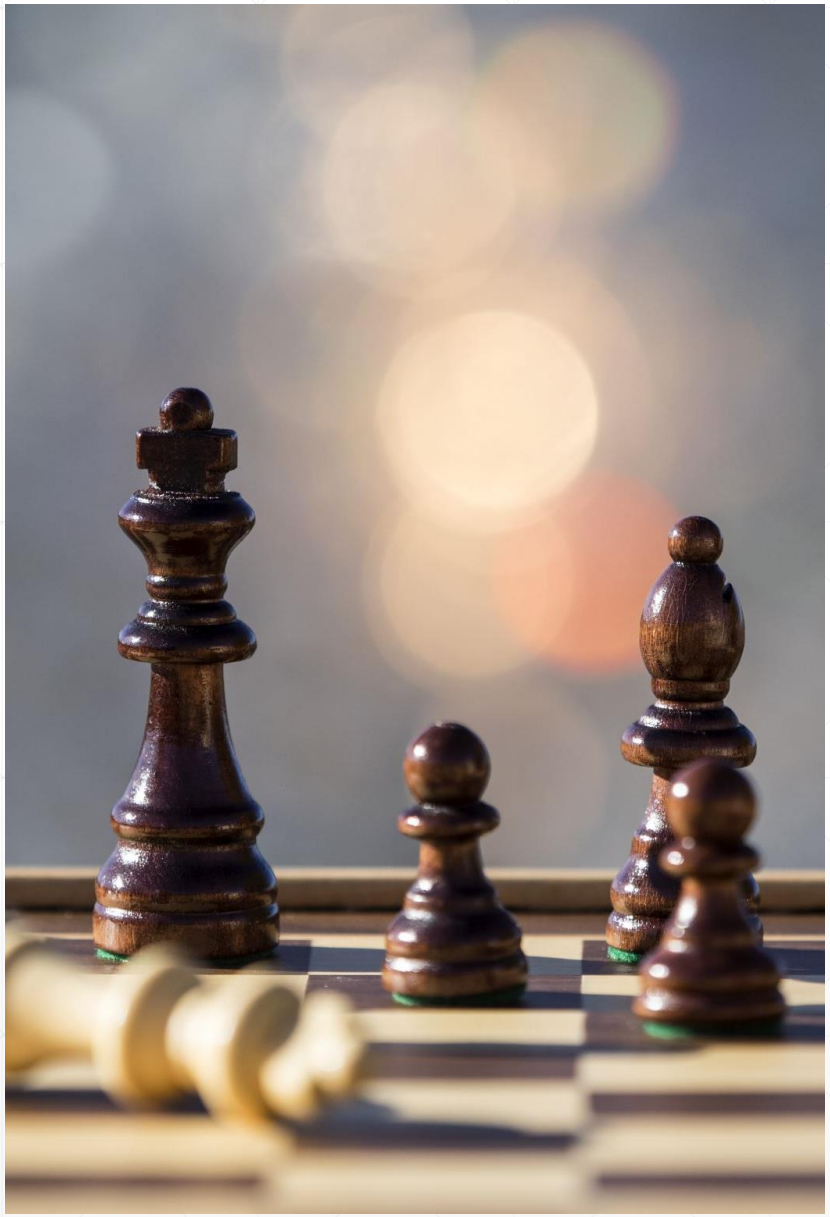


Source: Crum & Forster / NetDiligence

The next new wave of cyber risk involves human risk, as well

Disinformation Attack Vectors

Social Media	Fraudulent Domains
Deep Fakes	Insiders



KEY ISSUES

- **Cyber-security specific issues:**
  - Most breaches come from known vulnerabilities –
    - behaviors around patching, configuration and alert monitoring are critical.
  - Incidence Response Plans have a major impact on incident and reputational mitigation.

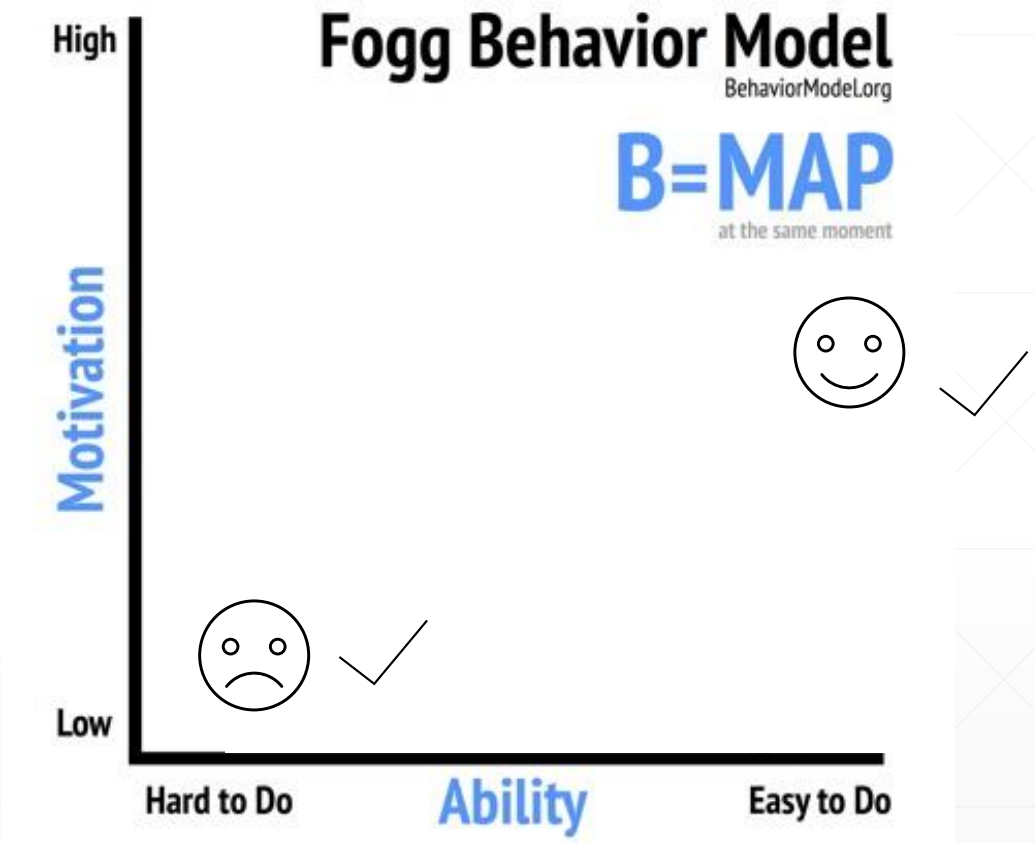
- **Lack of Strategic Alignment between Business and IT/Cybersecurity.**
  - Partners typically focus on overall strategy, clients, human capital and market risks;
    - IT focused on framework maturity and controls.
  - Partners acknowledges that there are risks inherent in strategy;
    - Cybersecurity is, by nature, risk averse.

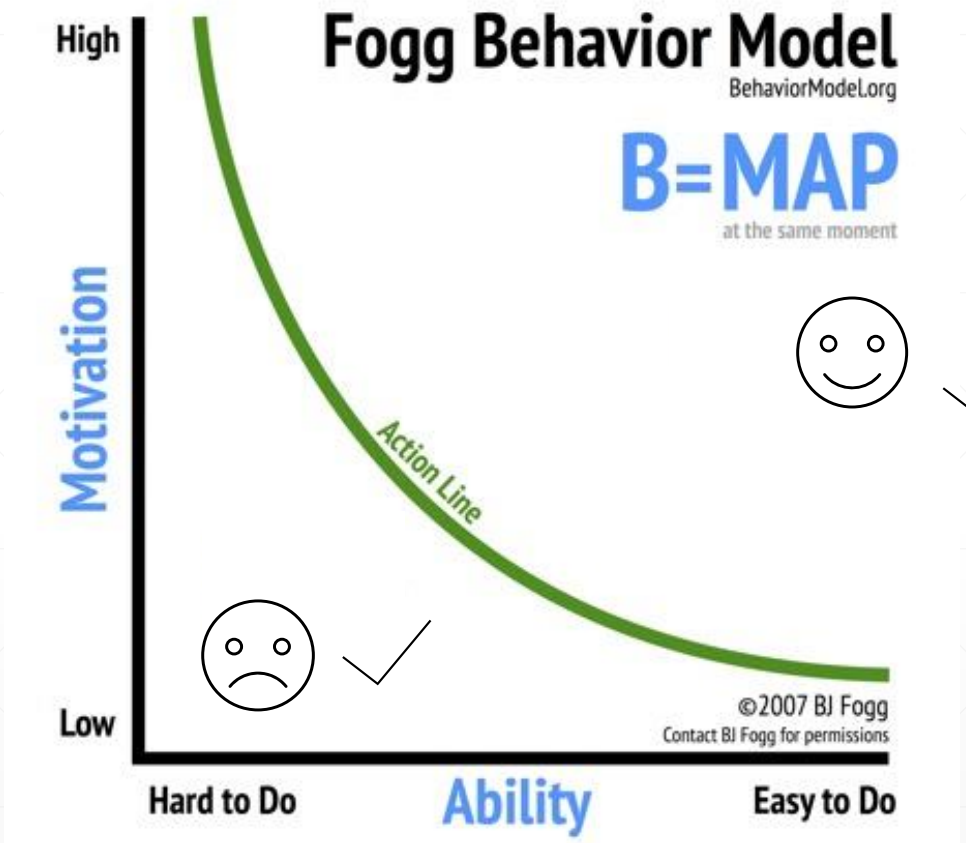
- **Employee behavior, in the context of a strategic risk culture, is a key contributing factor to assessing, communicating and mitigating cybersecurity risk**

TAKING ACTION

It's all about behavior


Fogg Behavior Model
BehaviorModel.org
B=MAP
at the same moment


Fogg Behavior Model
BehaviorModel.org
B=MAP
at the same moment
High
Motivation
Low
Hard to Do
Ability
Easy to Do


Fogg Behavior Model
BehaviorModel.org
B=MAP
at the same moment
High
Motivation
Low
Action Line
©2007 BJ Fogg
Contact BJ Fogg for permissions
Hard to Do
Ability
Easy to Do

Fogg Maxim #1

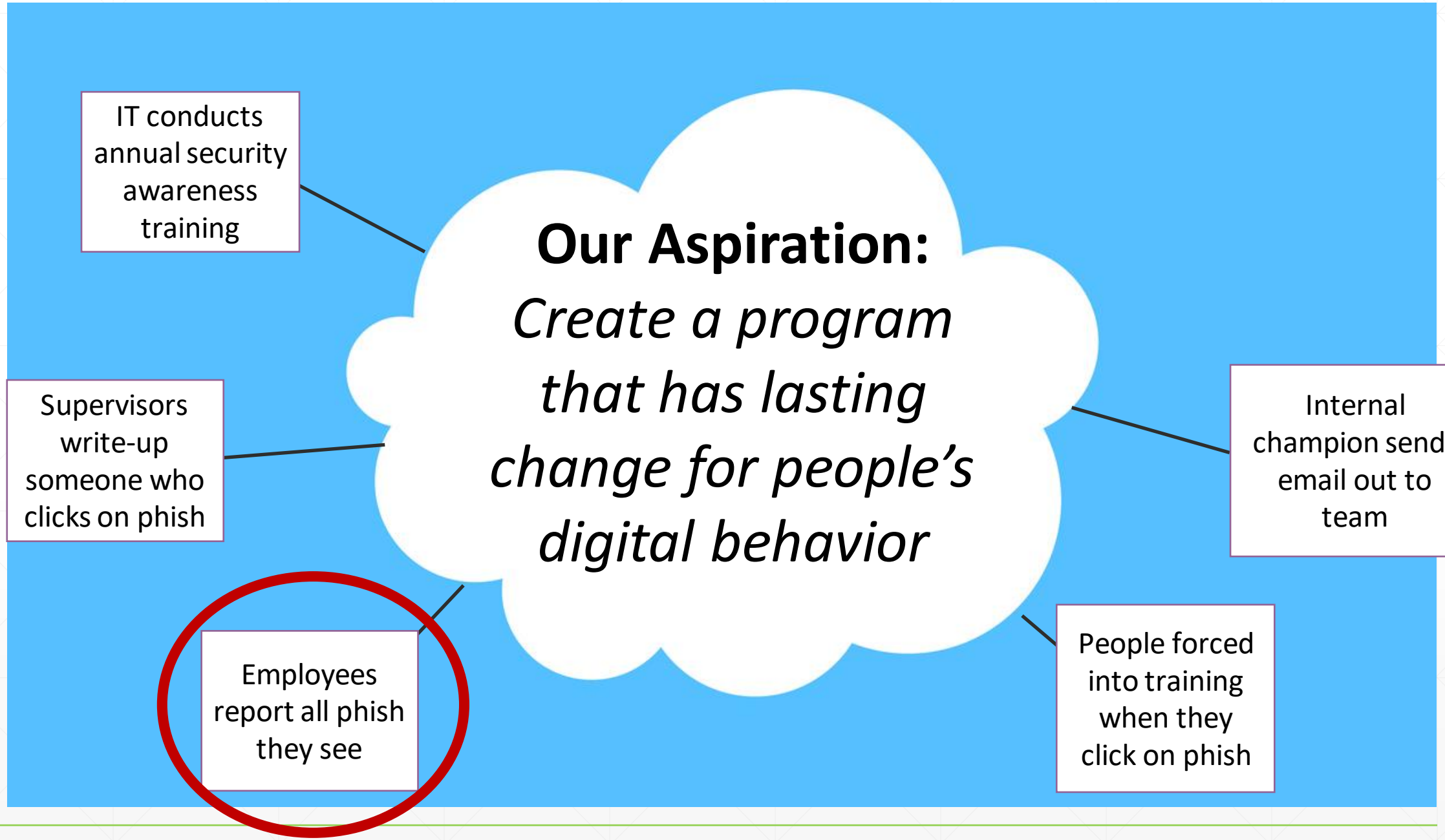
Help people do what they already want to do.

Fogg Maxim #2

Help people feel successful.

Behavior Designing Cybersecurity


IT conducts annual security awareness training
Supervisors write-up someone who clicks on phish
Employees report all phish they see
Our Aspiration:
Create a program that has lasting change for people's digital behavior
Internal champion sends email out to team
People forced into training when they click on phish


IT conducts annual security awareness training
Supervisors write-up someone who clicks on phish
Employees report all phish they see
Our Aspiration:
Create a program that has lasting change for people's digital behavior
Internal champion sends email out to team
People forced into training when they click on phish

Putting it all together

Anchoring

After I get an email

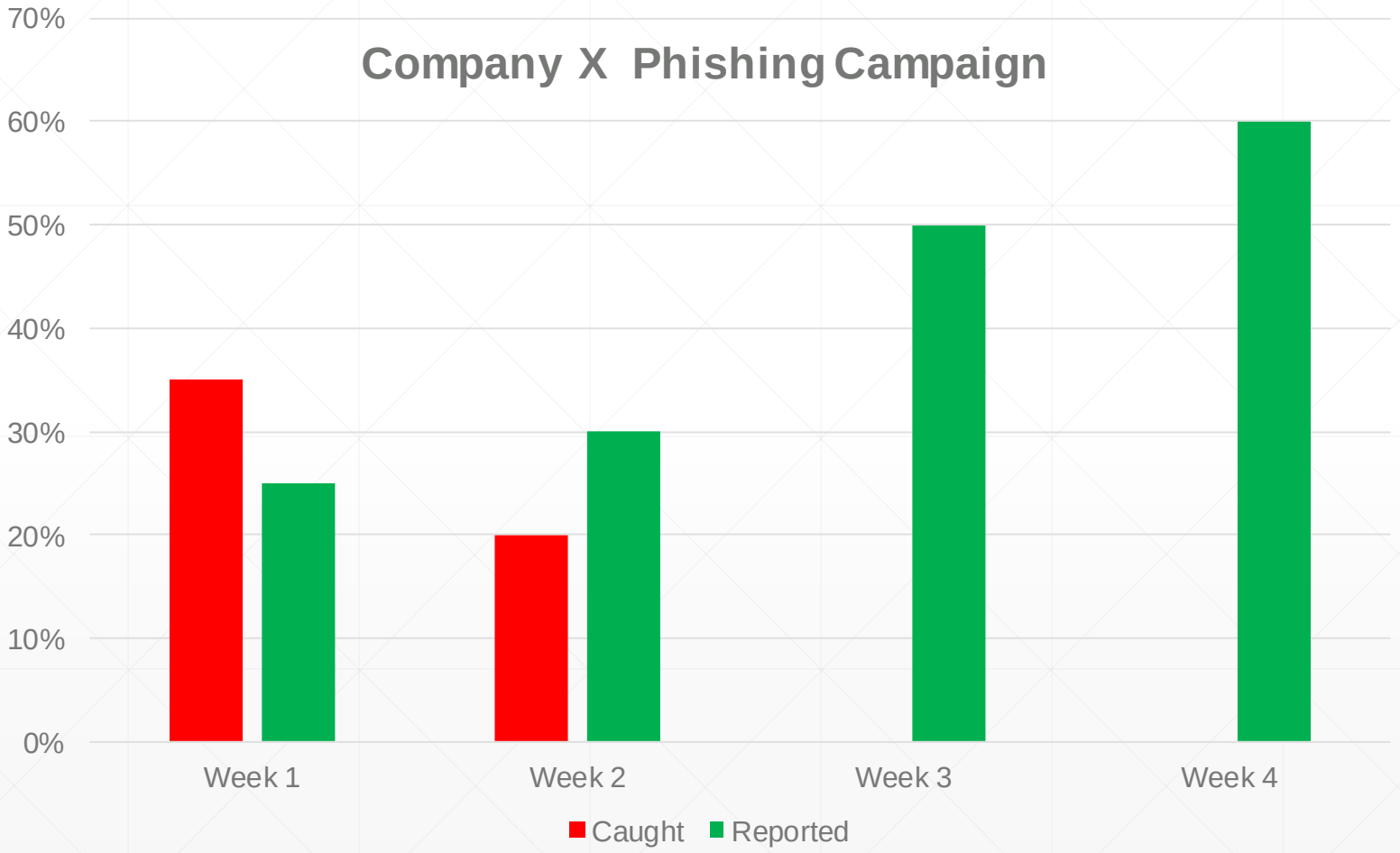
Behavior

I review it to see if it looks like a phish and report it if it is....

Celebrate

Then I receive a humorous congratulatory note celebrating my achievement.

Total Caught / Reported: Dramatic decrease in phish caught after week 2 suggests that "sentinel effect" plus weekly summaries promote increased awareness; increase in reported through the campaign reflects a strong initial core that is added to over the succeeding weeks.



Note 1: 3 Phish were sent out weeks 1-4


Governance
Behaviors

LEADERSHIP & IT WORK TOGETHER TO ALIGN CYBERSECURITY WITH BUSINESS OBJECTIVES

INCIDENCE RESPONSE

- **KNOW YOUR TEAM**
- **KNOW WHAT TO DO & WHEN**
- **PRACTICE**

Focus on Outcomes

- Phish Response Rates
- Mean Time Vulnerability Remediations
- Mean Time Incident Identification
- Mean Time and Cost Incident Resolution

3 Key Governance Behaviors

- Leadership / IT work together on aligning cybersecurity with business strategy
- Incidence Response
- Focus on Outcomes

3 Key Cybersecurity Behaviors

- Secure Configurations
- Patching
- Alert Monitoring

2 Key Staff Behaviors

- Report Phish or suspicious behavior
- Verify financial requests via analog channel

A SOLID CYBER-SECURITY POSTURE NEEDS ONE THING

YOU.

WALK THE TALK

- **COMMUNICATE**
- **SHARE TIPS LEARNED**
- **PAY ATTENTION TO YOUR IT TEAM**

3 QUESTIONS

1. **How does cybersecurity drive the organization's growth objectives and stakeholder needs?**

2. **What cybersecurity behaviors do we want to see from our IT Team? Staff? The Leadership Team? Myself?**

3. **How well is leadership communicating the importance of cybersecurity and privacy to the entire organization? And to our customers and other stakeholders?**

Insurance Coverage Gaps

	Property	General Liability	Crime/Bond	K&R	E&O	Cyber / Privacy
1st Party Privacy / Network Risks						
Physical Damage to Data						
Virus/Hacker Damage to Data						
Denial of Service attack						
B.I. Loss from Security Event						
Extortion or Threat						
Employee Sabatoge						
3rd Party Privacy/Network Risks						
Theft/Disclosure of private Info						
Confidential Corporate Breach						
Technology E&O						
Media Liability (electronic content)						
Privacy Breach Expense						
Damage to 3rd Party's Data						
Regulatory Privacy Defense/Fines						
Virus/ Malicious Code Transmission						

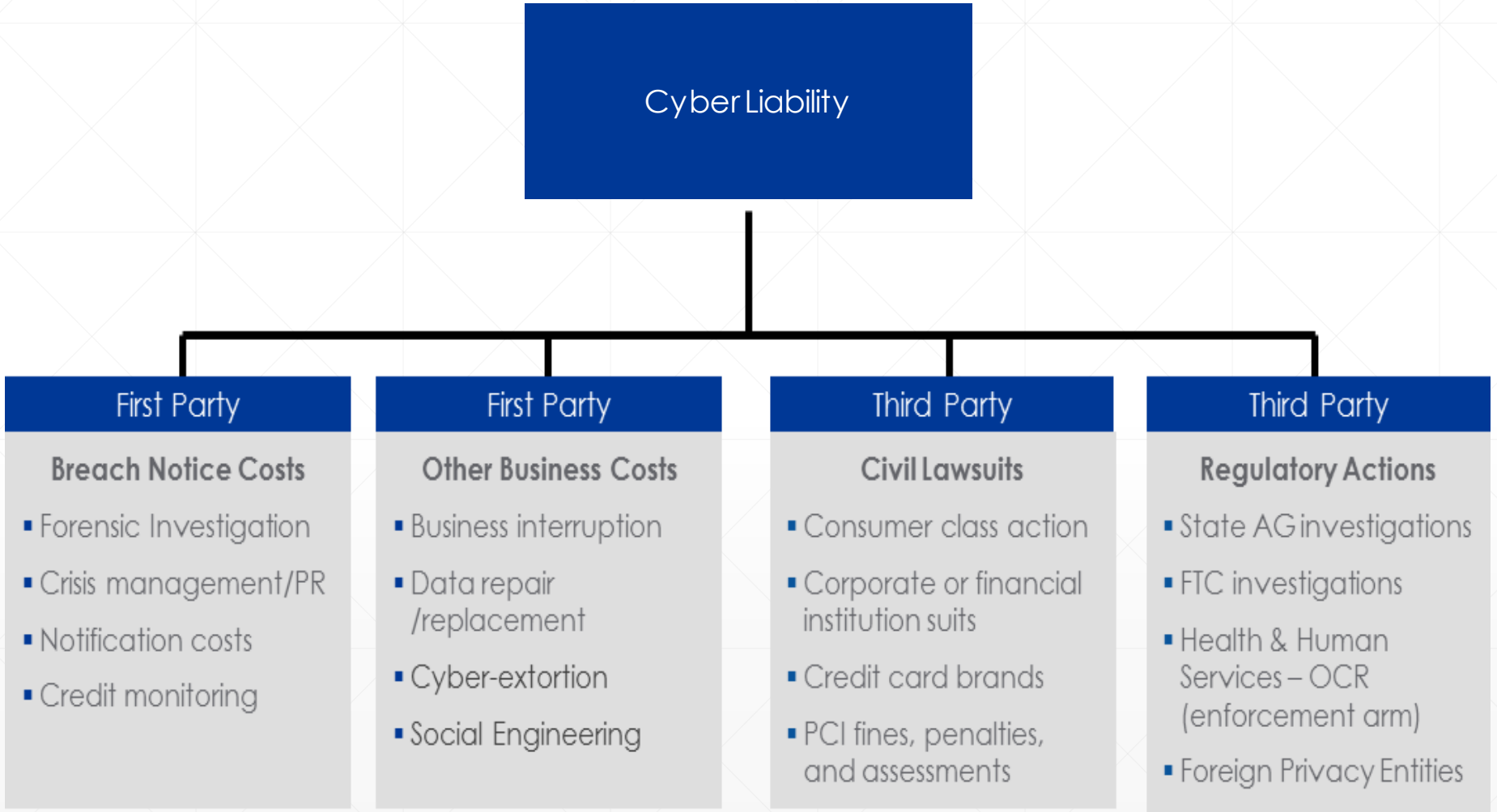
Coverage Provided:	
Limited Coverage:	
No Coverage:	

Traditional Insurance Gaps to name a few:

- Theft or disclosure of Third Party Information – GL
- Security & Privacy – "intentional act" exclusion – GL
- Data is not tangible Property – GL, Prop. and Crime
- Bi/PD Triggers – GL
- Value of Data if corrupted, destroyed or disclosed – Prop & GL
- Contingent Risks from external hosting, etc .

- Commercial Crime policies require "intent" and only cover "money securities and other Tangible Property"
- Territorial Restrictions
- Sublimits or long waiting periods applicable to any virus coverage available – Prop.

What Does Cyber Insurance Cover?



What is NOT COVERED by Cyber Insurance?

- Theft of Corporate Intellectual Property or Trade Secrets
- Brand Damage
- Loss of Future Revenue
  - As in the case of Target, for example, if sales were down due to customers staying away after data breach
- Negligence/Induced Incidents
- Nation State Attacks (excluded)
- Improved IT Security Measures (Starting to be covered by endorsement – Betterment Coverage)
- Hardware Damage – (Starting to be covered by endorsement – Bricking Coverage)
- Physical Damage

Critical Coverage Issues

- Choice of counsel
- Betterment Coverage
- Bricking Coverage
- Choice of third-party vendors
- Delete exclusions
  - Lack of patch upgrades/unencrypted data/devices
- Incident caused by a third-party vendor
- Allocation of coverage between necessary remediation costs and relative upgrades
- Extra costs incurred due to complying with a government order to take (or not take) certain actions to stop the incident
- “GDPR Endorsements”
- Definitions: Privacy Regulation/Law; Personal Information; Privacy Regulatory Proceeding (just proceeding or investigation/inquiry)
- Wrongful Collection Exclusions (“Spam” Exclusions) need to be addressed.

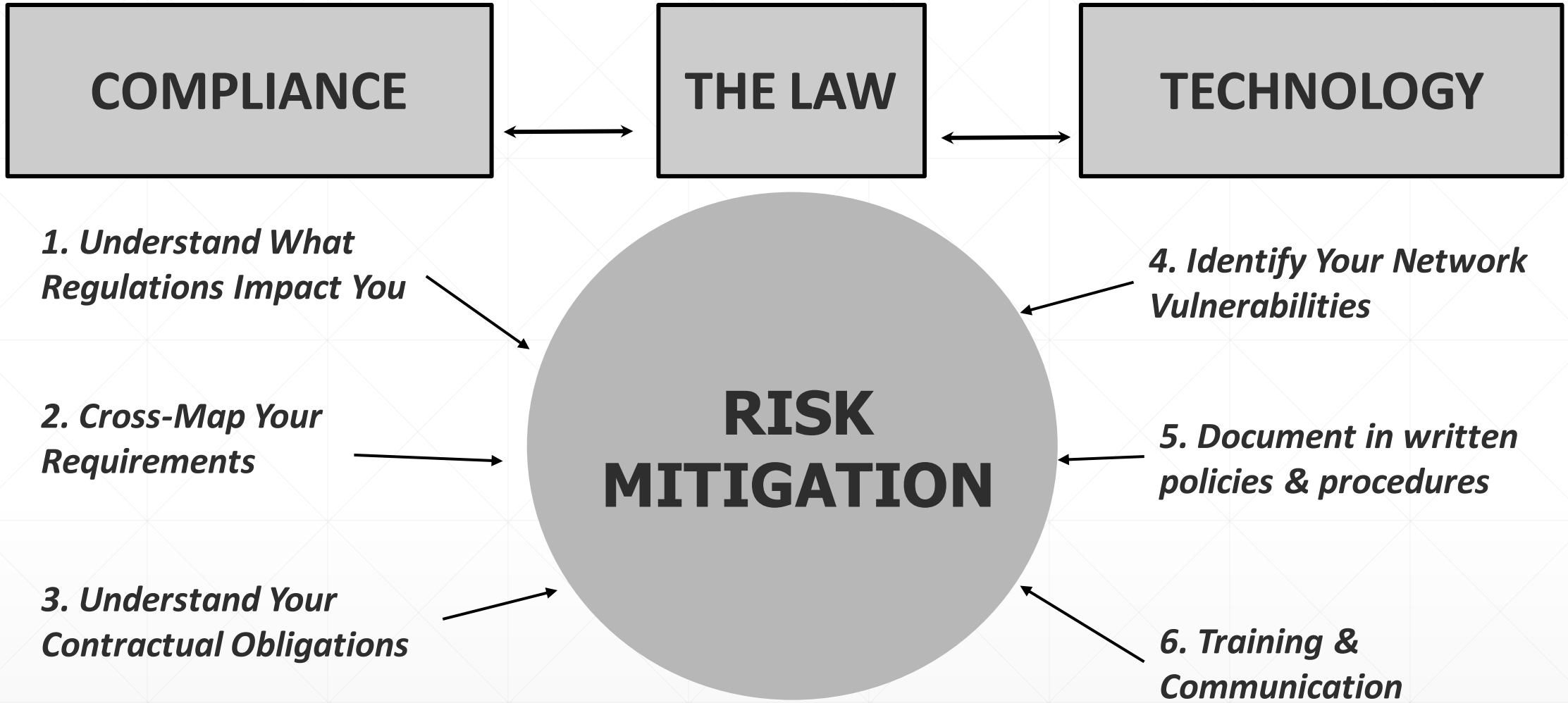
Cyber Exposures – How a Law Firm can Protect itself

- Buy Cyber Coverage!
- Incident Response Planning
- Employee Training
- Risk Analysis
- Encryption
- Two-factor Authentication
- Back-ups
- Document Retention Policy
- Penetration Testing
- Anti-virus and Patching
- Intrusion Prevention and Detection
- Vendor Risk Management

Risk Management

- Risk Management Tips for Employers
  - Require 2-factor authentication
  - Engage in regular security updates
  - Back up systems and data regularly
  - Advise employees to be wary of everything they click on
  - Use call back verification for vendor or client account changes and fund transfers for any amount above a predetermined threshold (i.e. $25K)

- Risk Management Tips for Employees
  - Keep computers and other devices in a secure place
  - Log out when you are not using your computer or system
  - Have strong passwords
  - Back up and save data regularly
  - Access corporate information with a VPN especially if you are accessing on a public network.


COMPLIANCE
THE LAW
TECHNOLOGY
1. Understand What Regulations Impact You
2. Cross-Map Your Requirements
3. Understand Your Contractual Obligations
RISK MITIGATION
4. Identify Your Network Vulnerabilities
5. Document in written policies & procedures
6. Training & Communication

Closing Remarks and Q&A Session

Thank you for attending todays webinar. We hope that you found it informative.

Mike Mooney, Senior Vice President & National Practice Leader, USI Affinity

Mike.Mooney@usi.com

610-537-1441

www.abainsurance.com/firm-products/cyber-liability/