

# Cyber 101

A crash course on cyber security,  
data protection and cyber insurance.

**Halifax CII**

Wednesday, 20th February 2019

**Berea.**

[www.berea-group.com](http://www.berea-group.com)

**Aaron Yates**

Chief Executive, Berea



**AWARDS  
2018**  
Finalist

# Berea

- Focused on high scale cyber support for SMEs.
- Work with insurers, MGAs and insurance brokers.
- Happy to explain more after our session.



# Why are we here?

- Is it really a problem?
- What, exactly, is the problem?
- What is cyber insurance?
- What's happening with distribution?
- How do Berea fit in?

**Let's make it real**

# Pop quiz

Is your website a risk?

[www.securityheaders.io](http://www.securityheaders.io)

Try us, too!

[www.berea-group.com](http://www.berea-group.com)

# Pop quiz

Is your iPhone secure?

**Let's find out...**

Settings → Touch ID/Face ID and Passcode → Erase Data

Is the setting **green** or **grey**?

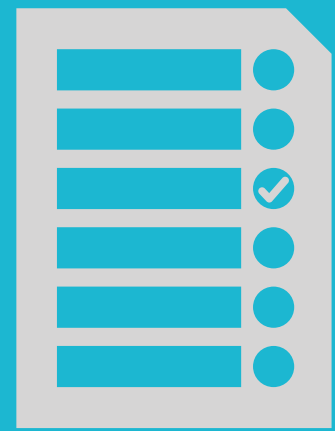
# Pop quiz

Have you been compromised?

**[www.haveibeenpwned.com](http://www.haveibeenpwned.com)**

If you've been with your employer less than a couple of years try using your personal email address.

# What just happened?



We have evidenced  
that you have  
vulnerabilities



We have made a  
**very small part**  
of the issue visible



These insights are  
symptomatic of a  
**far bigger problem**



# The far bigger problem

## “Cyber” (Oct 17 - Oct 18)

- 1.6m offences virus/Computer Misuse Act.
- 1.5m cyber-related fraud offences.

**8,493 /day.**

Probably not insured.

## Fires (Oct 17 - Oct 18)

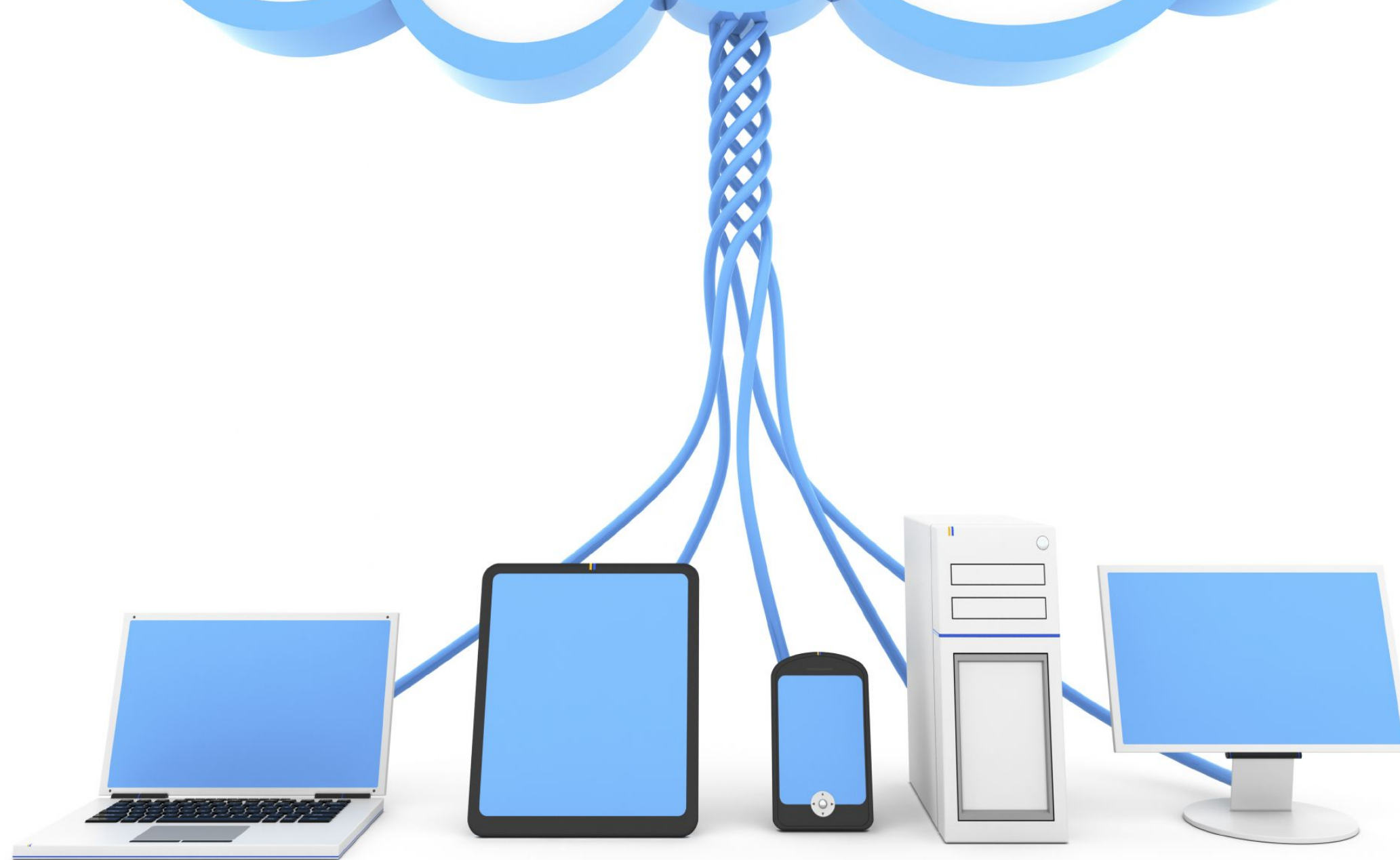
- 167,150 attended to nationally.
- Of which 15,577 were commercial premises.

**458 /day.**

Highly likely to be insured.

**What's the problem?**





# Why is it now such a problem?



*Because use of technology  
creates a vicious cycle*

**Pop quiz**

**Have you ever sent  
an email after 10pm?**

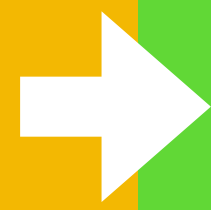
# Governance is patchy-to-MIA for most businesses

*Layers of legacy systems  
under new technology*

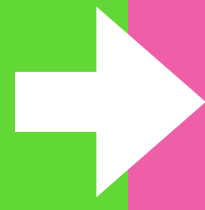
**What's happening,  
and why?**



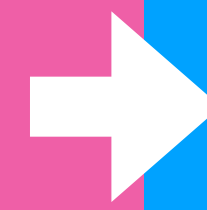
**We have  
an actor**



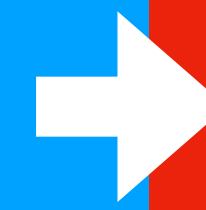
**Who has a  
motivation**



**And uses  
a vector**



**To exploit a  
vulnerability**



**Creating  
an incident...**

**Staff**

**Accident**

**Website**

**Human**

**Financial Loss/Costs**

**Organised Crime**

**Negligence**

**Email**

**Software**

**Reputation Damage**

**Opportunists**

**Malice**

**Physical media**

**Hardware**

**Legal/Regulatory**

**Script Kiddies**

**Financial**

**Physical office**

**Hacktivists**

**Ethical**

**Social media**

**Hackers**

**Moral**

**Telephone**

**Nationstate**

**Ego**

**Supplier**

**Customer**

~~Cyber~~

**Information  
Security**

**Data  
Protection**

# Information Security

## Background

- Not legally mandated
- Sensible business practice
- Identify and manage risks
- Risk score prioritises activity

## Key concepts

- Confidentiality
- Integrity
- Availability

# Data Protection

## Background

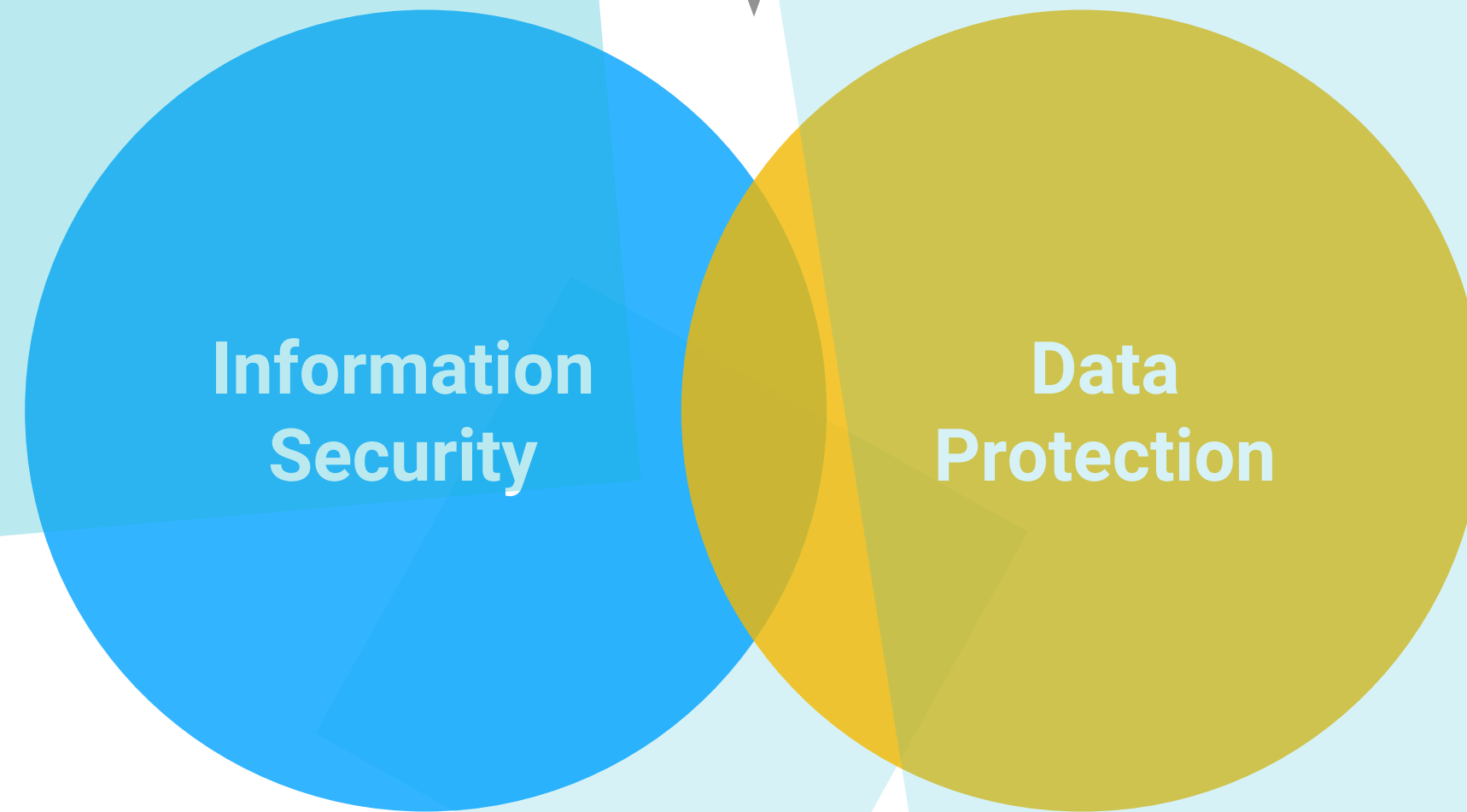
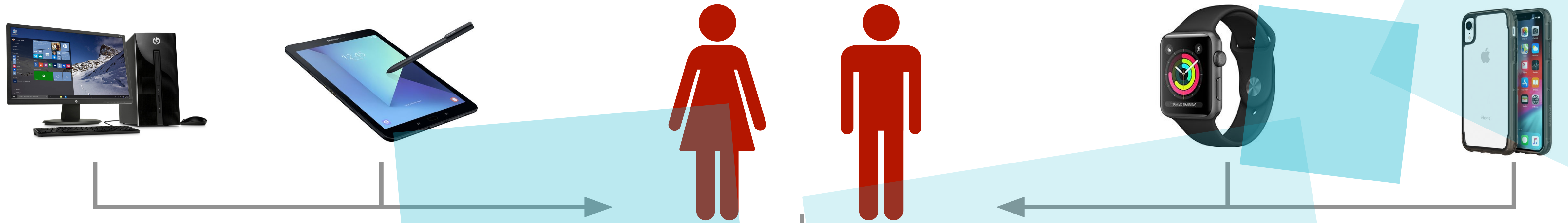
- Legally mandated by GDPR
- Requires data to be stored securely
- Honour the rights of individuals
- Lawful basis for processing
- Evidence compliance activity

## Why is legislation changing?

- 20 years of change
- Decisions are being made about us

## Consequences

- Penalties of up to 4% GAT or €20m
- Reputation damage



**Financial  
loss**

**Legal  
issues**

**Reputation  
damage**

**Cyber insurance?**

# When the worst happens

1

Identify what  
has happened

2

Stop the attack,  
restore service

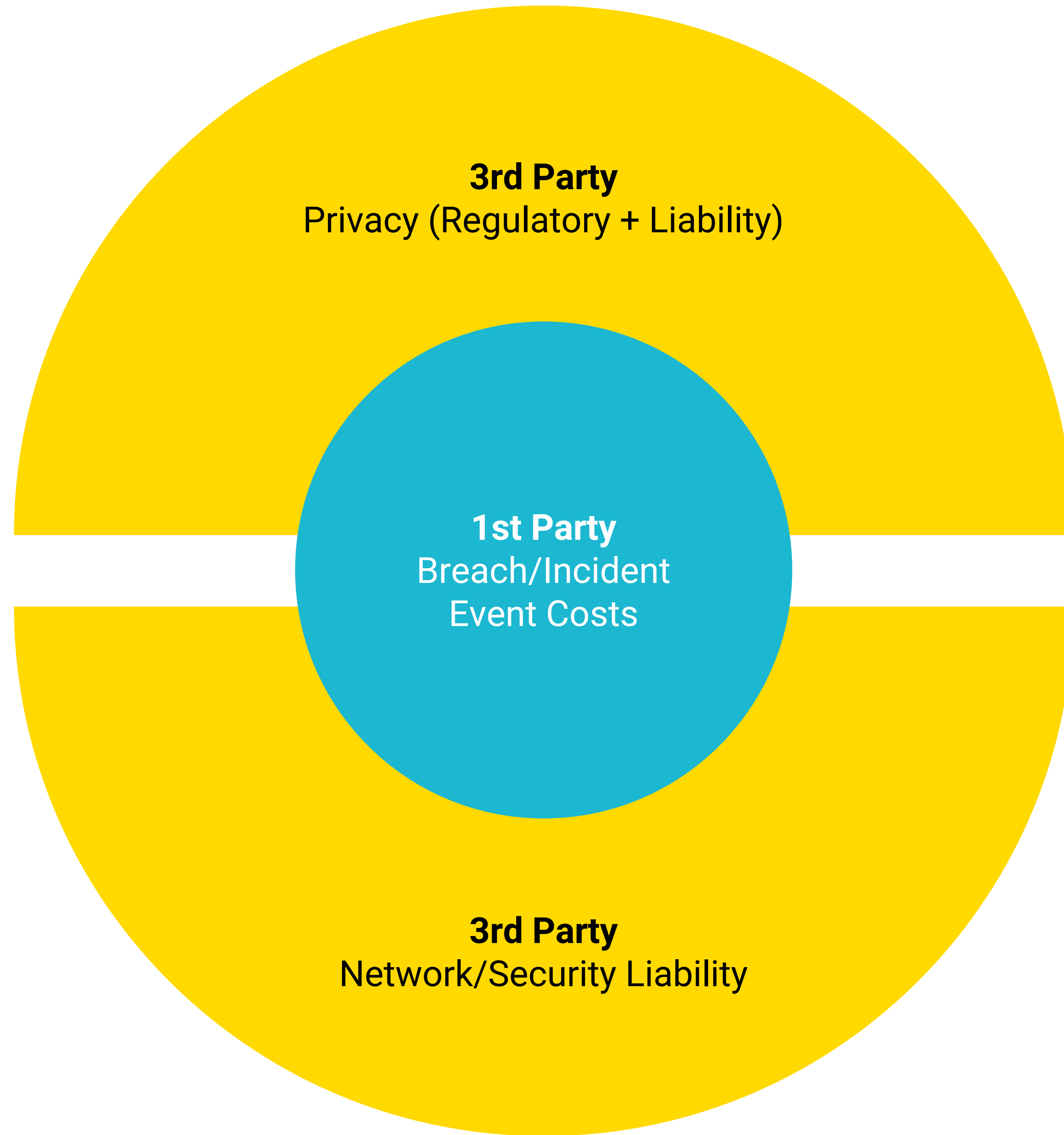
3

Contend with  
the fallout



**1st Party**  
Breach/Incident  
Event Costs



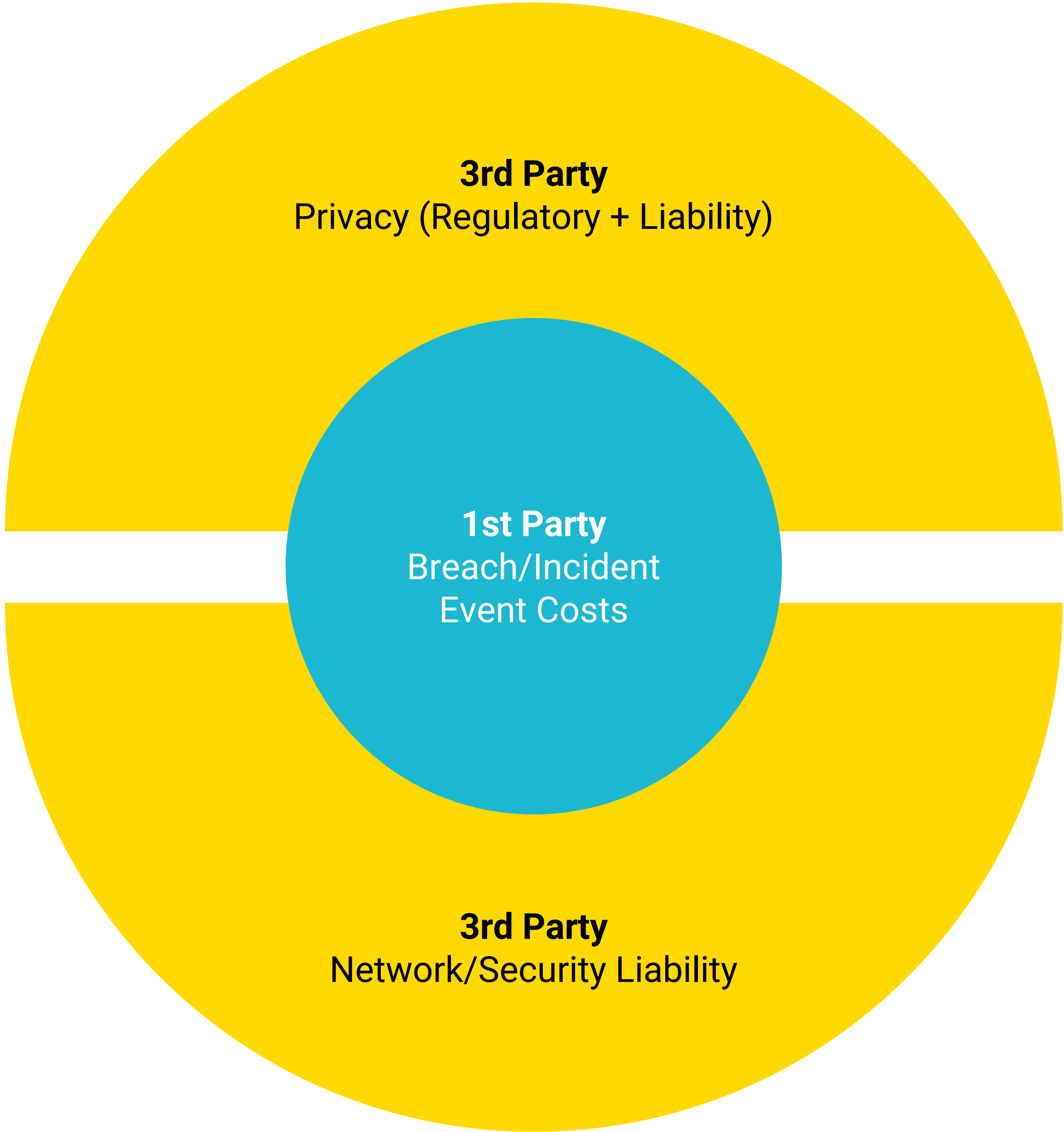


**3rd Party**  
Privacy (Regulatory + Liability)

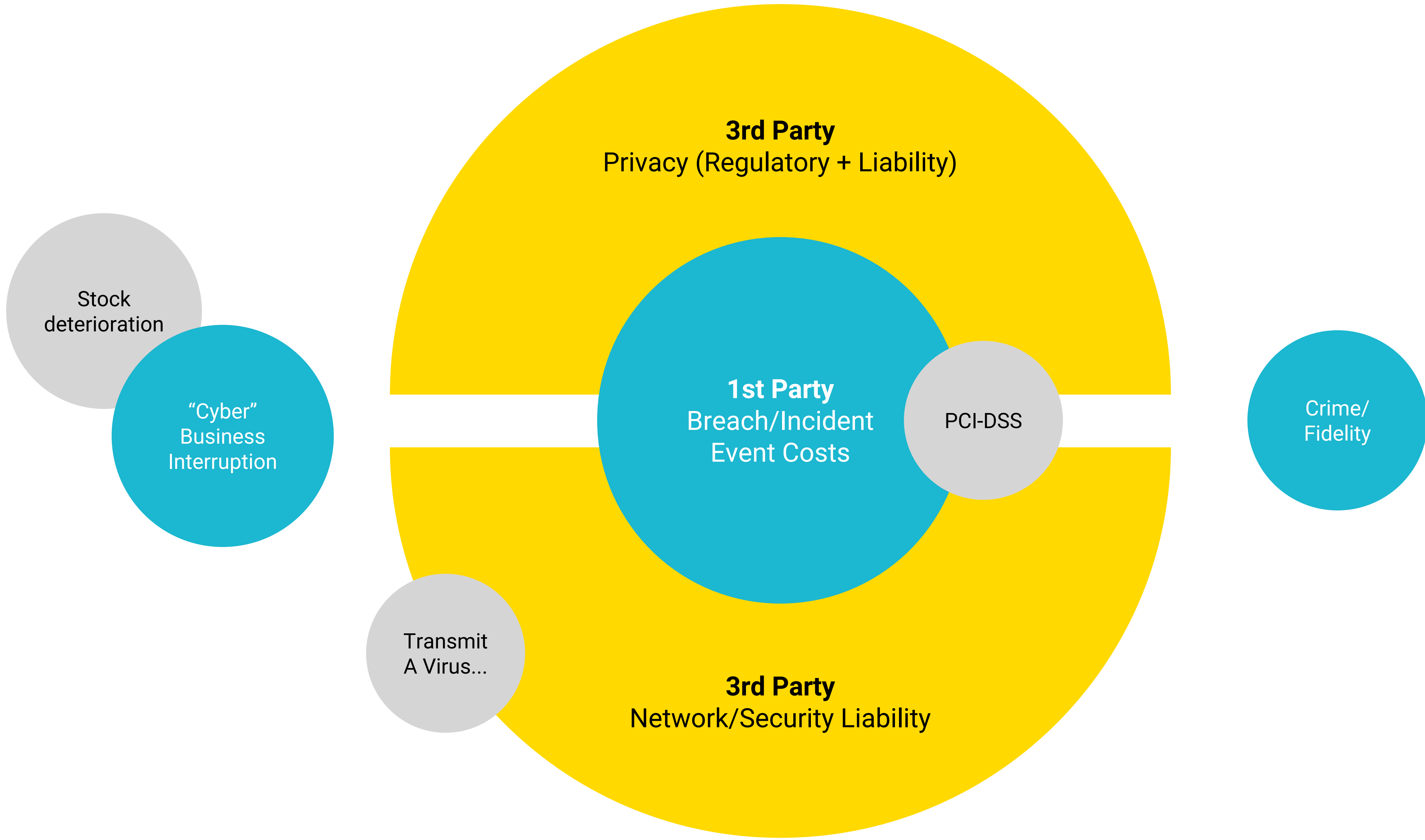
**1st Party**  
Breach/Incident  
Event Costs

**3rd Party**  
Network/Security Liability

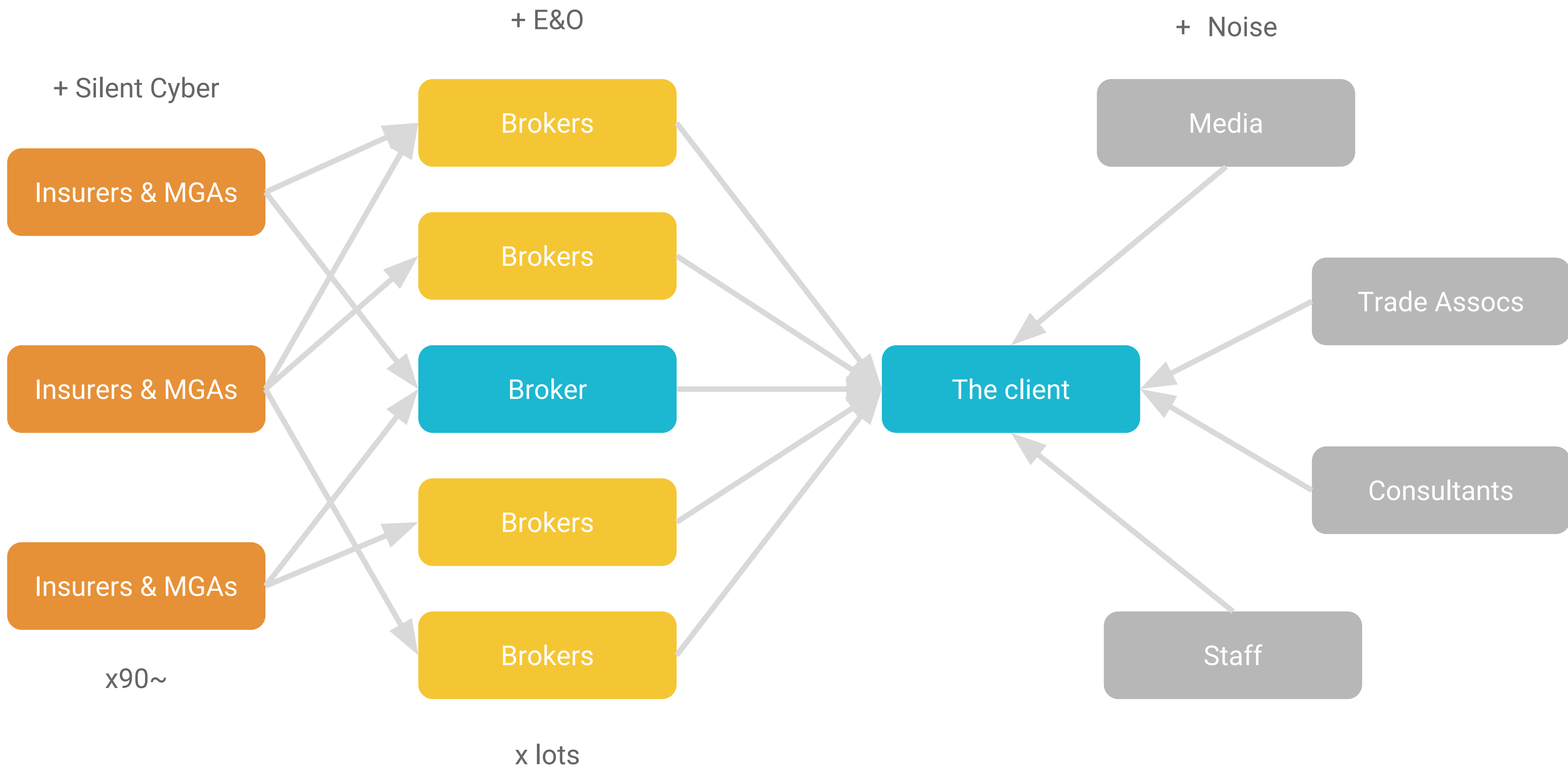
“Cyber”  
Business  
Interruption



Crime/  
Fidelity

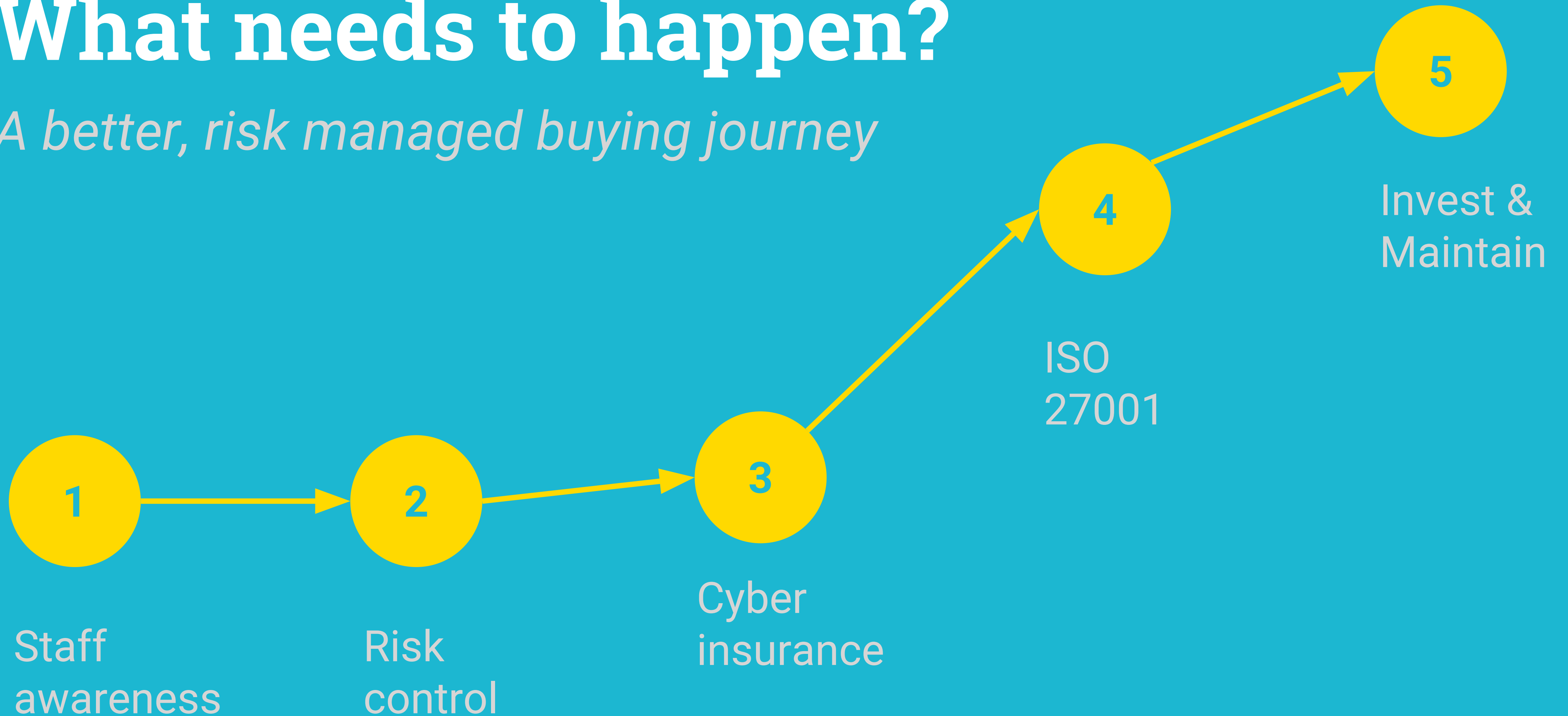


# Distribution issues



# What needs to happen?

*A better, risk managed buying journey*



# Governance specifications

## A growing alphabet soup

- Cyber Essentials
- ISO 27001
- PCI-DSS
- GDPR Fundamentals
- Insurance/client requirements

## With road blocks

- “DIY” possible with expertise
- Consultants cost >£1,000 +VAT
- Too few experts
- Firms are unsure where to start

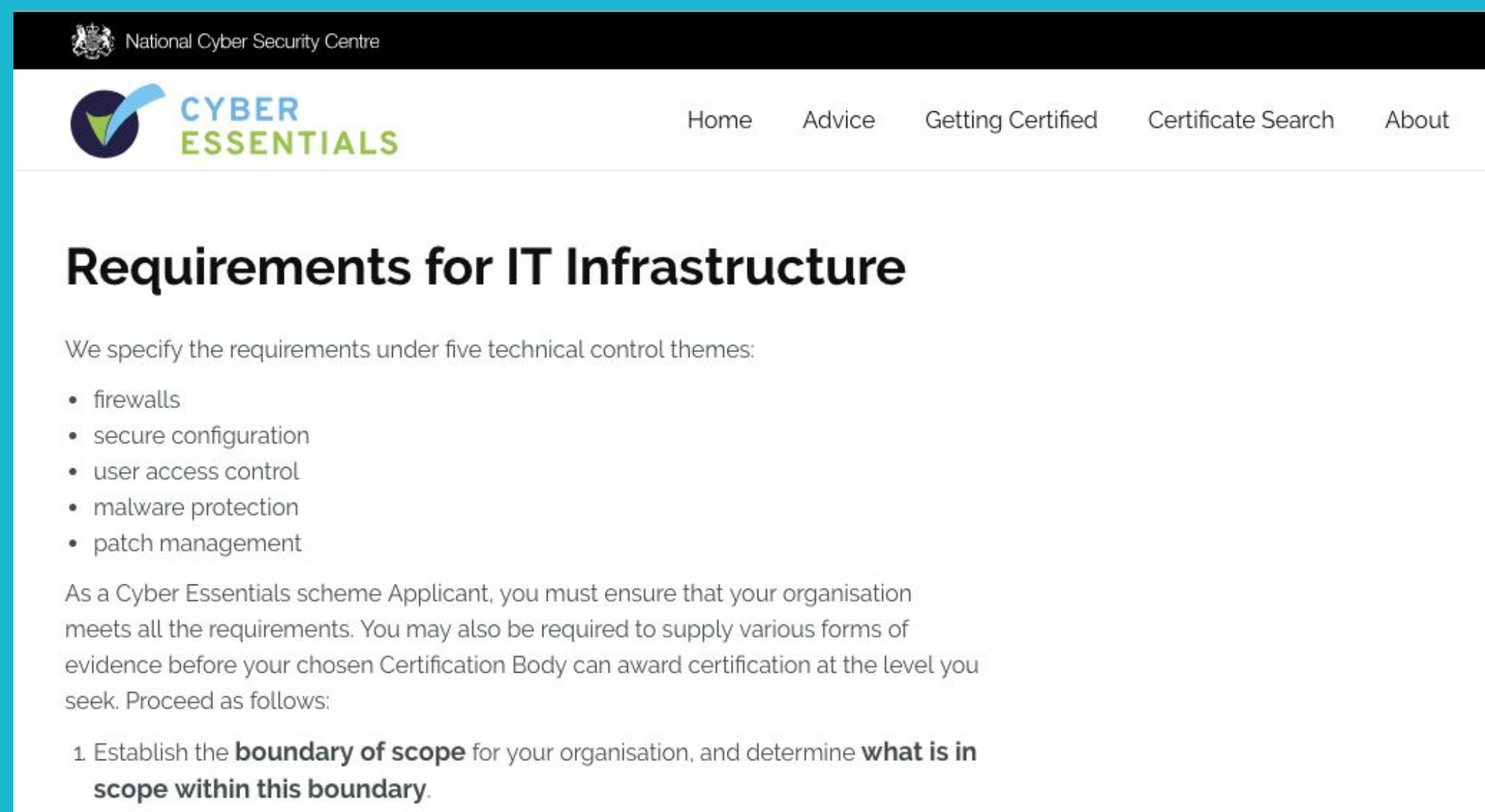
# Cyber Essentials

## What is it?

- Technical governance specification
- A recognised certification

## Background

- Standardise procurement assurance
- Minimum benchmark for British firms
- Reduce common threats by 70-80%
- Recognised by the ICO for GDPR
- Join risk management and insurance



The screenshot shows the National Cyber Security Centre website. The header includes the logo and navigation links: Home, Advice, Getting Certified, Certificate Search, and About. The main content area is titled "Requirements for IT Infrastructure" and lists five technical control themes: firewalls, secure configuration, user access control, malware protection, and patch management. It also provides instructions for applicants and a numbered list of steps to follow.

National Cyber Security Centre

**CYBER ESSENTIALS** Home Advice Getting Certified Certificate Search About

### Requirements for IT Infrastructure

We specify the requirements under five technical control themes:

- firewalls
- secure configuration
- user access control
- malware protection
- patch management

As a Cyber Essentials scheme Applicant, you must ensure that your organisation meets all the requirements. You may also be required to supply various forms of evidence before your chosen Certification Body can award certification at the level you seek. Proceed as follows:

1. Establish the **boundary of scope** for your organisation, and determine **what is in scope within this boundary**.



# How Berea fit in



## Insurers & MGAs

Embed Cyber Essentials as a risk management value add to your PI and SME packaged offerings.



## Insurance Brokers

Proactively engage clients with Berea's unique services as a ready-made sales journey to buying cyber insurance.

# Thank you

Any questions?

**Berea.**