RAISING THE BAR

IFA LEGAL SYMPOSIUM

MAY 5-7, 2019 | WASHINGTON, DC

IFA
INTERNATIONAL FRANCHISE ASSOCIATION

Navigating the Changing Privacy and Data Security Landscape

David Allsman *(moderator)*

Elizabeth Simpson

Linda Emery

Shawn Clark

IFA LEGAL SYMPOSIUM
MAY 5-7, 2019 | WASHINGTON, DC

IFA
INTERNATIONAL FRANCHISE ASSOCIATION

Roadmap

Privacy & Security in franchise networks

Preparing for the Future

Franchisee Support = Brand Protection

Practical Risk Reduction

How to join

Web

1

2

Text

1

2

Privacy & Security in Franchise Networks- GDPR

- EU Data Protection Regulation
- Effective May 25, 2018
- Fines up to €20 million or 4% of a company's total global revenue for the preceding fiscal year, whichever is greater
- Applies to US Companies with Customers in the EU

Privacy & Security in Franchise Networks-
GDPR Applies to US Companies

- operating in the EU
- offering products or services to EU residents
- collecting data from the EU (for example placing cookies on a EU person's computer) or monitoring behavior of EU residents
- using vendors in the EU

Privacy & Security in Franchise Networks-
GDPR Scope

- Collection and processing of **personal data**
- What is "**personal data?**"

  "Any information relating to an identified or identifiable natural person"

Privacy & Security in Franchise Networks-
GDPR Scope

- Collection and **processing** of personal data
- **What is "processing?"**

  "Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means"

- Not just electronic

Privacy & Security in Franchise Networks-
GDPR Features

- Lawful Basis for Processing
- Individual Rights:
  - Right to be forgotten
  - Right to portability
  - Right to be informed
  - Right of access
  - Right to object
- Accountability:
  - Data Privacy Officer
  - Privacy Impact Assessment
  - Privacy/Security by Design

Can US Companies Transfer EU data to US?

- **Prohibited** unless adequate safeguards in place in the US
- Options to fulfill the adequate safeguards requirement
  - ✓ Consent (not really)
  - ✓ Privacy Shield
  - ✓ Model contract terms
  - ✓ Binding corporate rules (approved by a DPA)

Privacy & Security in Franchise Networks-
GDPR Fines

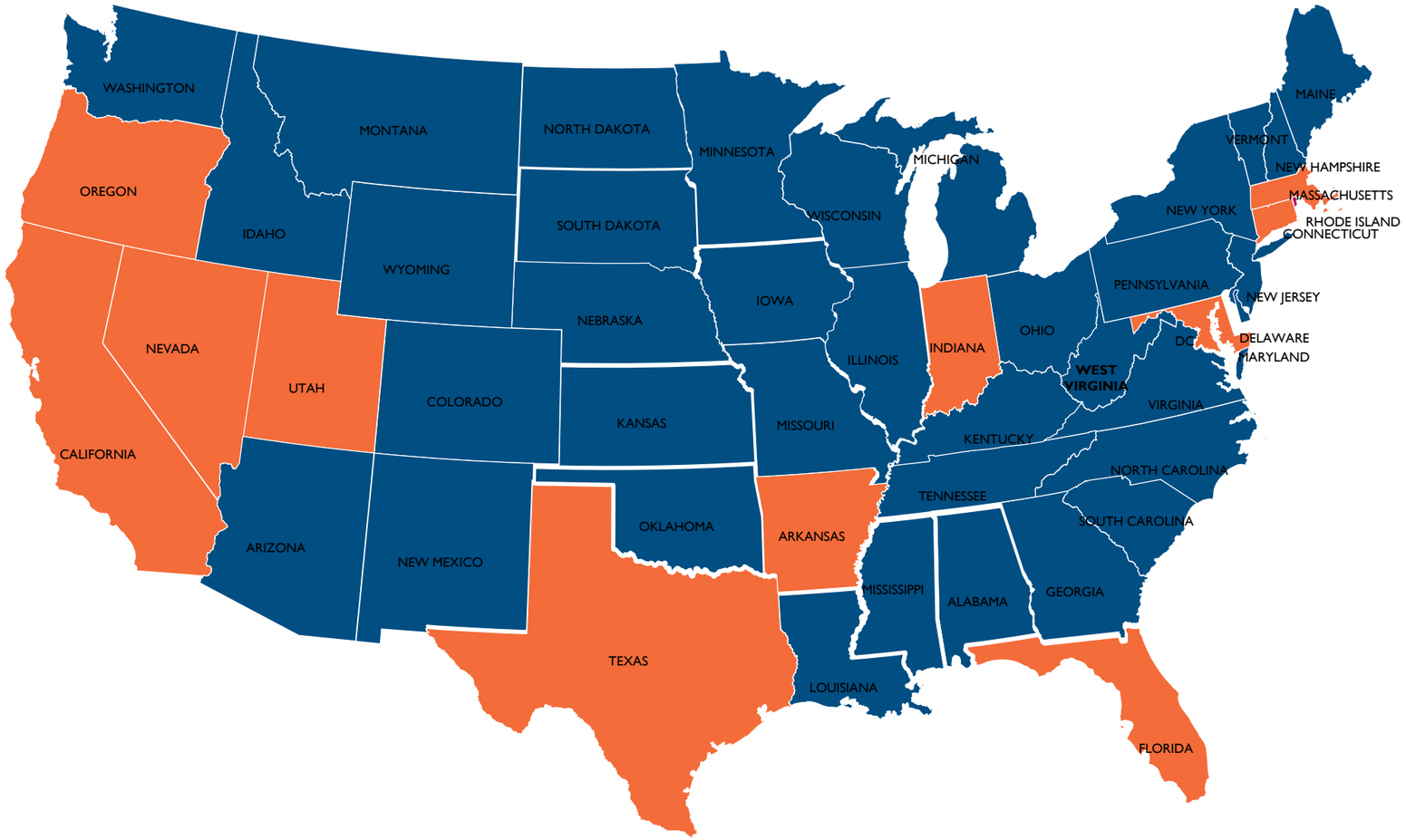
- France's Regulator ("CNIL") fined Google $57 million for GDPR violations
  - Fine was far lower than what GDPR would have allowed
- Google's violations included:
  - Lack of transparency (difficult to access privacy terms)
  - Conflation of processing methods to increase targeted ads

Where to Start

- Add standard data protection language to your contracts and standard terms *(i.e.,* your business partners agree to protect the data)
- Update your existing privacy notices
- Update your internal privacy policies and procedures
- Revisit your consent procedures
- Make sure your data security system is state of the art
- Review your agreements with third parties
- Ask whether your company even needs to collect the personal data
- Ask whether it is feasible to anonymize the data (so that the GDPR does not apply)

Preparing for the Future

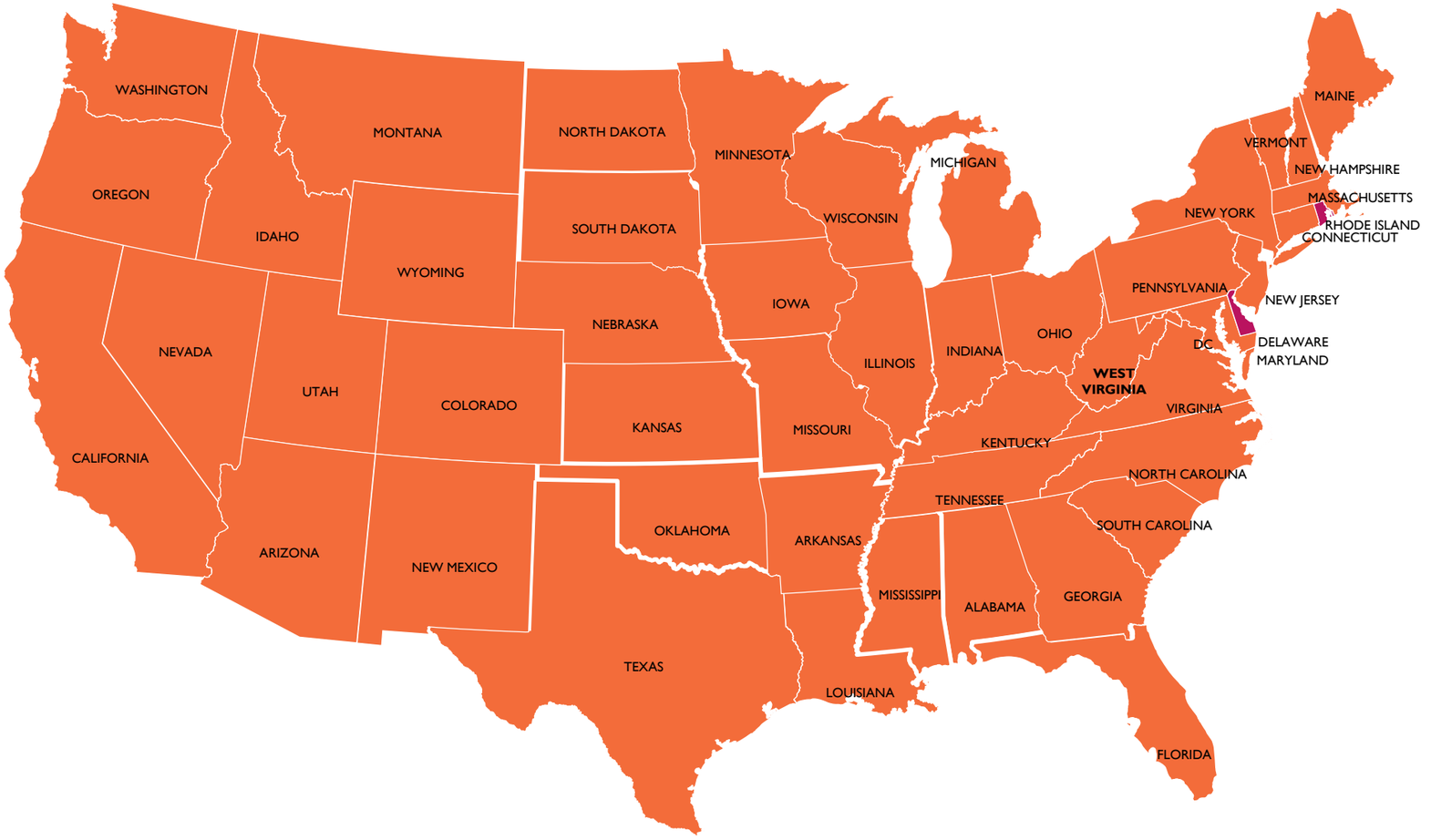
Privacy & Security Standards
State Laws 2016



States with Privacy & Security laws applicable to private business

States with no Privacy & Security Laws applicable to private business

Privacy & Security Standards
State Laws Today



States with Privacy & Security laws applicable to private business

States with no Privacy & Security Laws applicable to private business

California Consumer Protection Act (CCPA)

- Becomes effective January 1, 2020
- Penalties of up to $7,500 per intentional violation / $2,500 per unintentional violation
- Private right of action (class action)
- Data breach involving credit cards or other sensitive information is subject to statutory damages between $100-$750 per CA resident

Will the CCPA Apply?

- B2C and B2B
- Any business worldwide:
  - doing business in California; and
  - receiving personal information of CA residents that satisfies one of the following thresholds:
    - Annual gross revenues of $25 million
    - Obtains, buys, sells or shares personal information of 50,000 or more CA residents, households or devices annually
    - Receives 50%+ of annual revenue is from selling CA residents' personal information

*A parent or subsidiary using the same branding is covered even if they themselves do not qualify

Who and What is Protected?

- California consumers = California residents (excluding employees)
- Natural persons; not businesses
- "Personal Information" is broadly defined

  "...information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household...."
- Definition includes a long list of examples
- Includes online identifiers, IP address, internet or other electronic network activity information, browsing history, geolocation, etc.
- Most cookies will be considered Personal Information

What Individual Rights Apply?

Right to know (Must Disclose):

- Categories and specific pieces of Personal Information collected
- Categories of sources from which Personal Information was collected
- Must inform the resident of his / her right to request deletion of Personal Information
- Purposes for collecting, using, and selling Personal Information
- Categories of third parties to whom Personal Information is shared

Right to Request Deletion

Resident's right to request Personal Information be deleted (with some exceptions)

Right to opt-out

Resident's right to opt-out of the sale of their Personal Information (must provide a "Do Not Sell My Personal Information" link on the company's website)

Businesses Must:

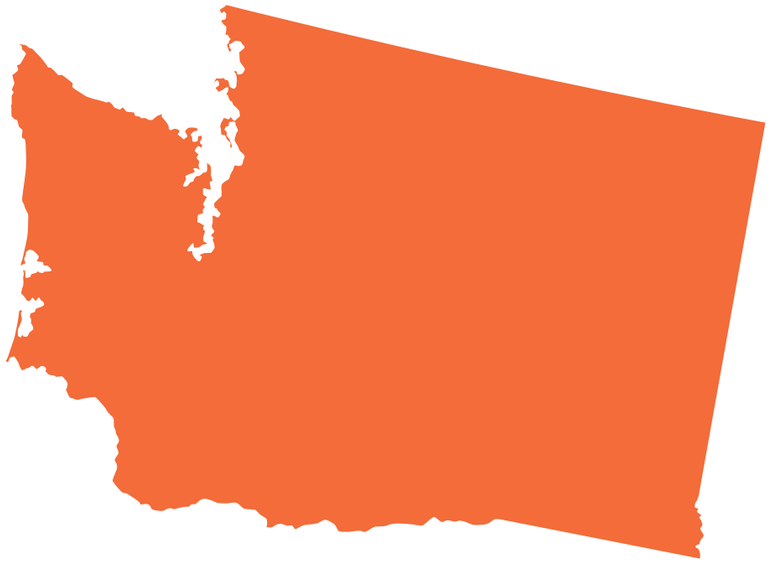
- Respond within 45 days (generally) to requests without charge
- Make 2+ methods available to make requests, including via phone & a website
- Ensure employees are able to direct CA consumers how to exercise their rights
- Inform CA consumers, at or before collecting Personal Information, of the categories & purposes of Personal Information collection
- Disclose in the privacy policy the individual privacy rights to request information
- Refrain from discriminating against CA consumers exercising their CCPA rights (*e.g.* by charging a different price or providing a different quality of goods or services *unless* the differences are reasonably related to the value provided by the personal data)
- Establish a process to verify consumers' identity

Next Steps:

- Monitor changes to the CCPA prior to implementation
- Data mapping
- Update privacy policies
- Create policies around responding to CA resident requests to exercise their rights (data disclosure, portability, and deletion, including at a minimum a toll-free telephone number and website address)
- Implement a processes for responding to California residents' requests noted above within 45 business days (and a process for extensions);
- Generate a clear and conspicuous "Do Not Sell My Personal Information" link
- Implement a process for avoiding requesting opt-in consent for 12 months after a California resident opts out

Ask for Protections From Vendors:

- Privacy Policies
- Data Mapping – What process do you have in place to respond?
- Ensure Vendor contracts include data security and privacy provisions and provisions to protect network access
- Employee Training
- Security Incident Response Plan



Washington Privacy Act- SB 5376

- Would have provided rights similar to CCPA but would specifically exclude employee data for employers
- Failed to be approved by the house by the deadline for consideration of non-budgetary matters.
- Watch for revival in 2020

Breach Notification Expansion-HB 1701

Privacy & Security Standards
Selected States with Similar Legislation

Illinois-- HB 3358
- Data Transparency and Privacy Act
- passed the house, pending in senate

Nevada--SB 220
- Passed house, pending in Senate
- Requires opt-out of data sale

New Jersey—AB 4902
- Requires consumer notices on disclosures and opt-out of data sale

New Jersey—AB 4974
- Requires notice for geolocation or GPS data is collection through a mobile application.

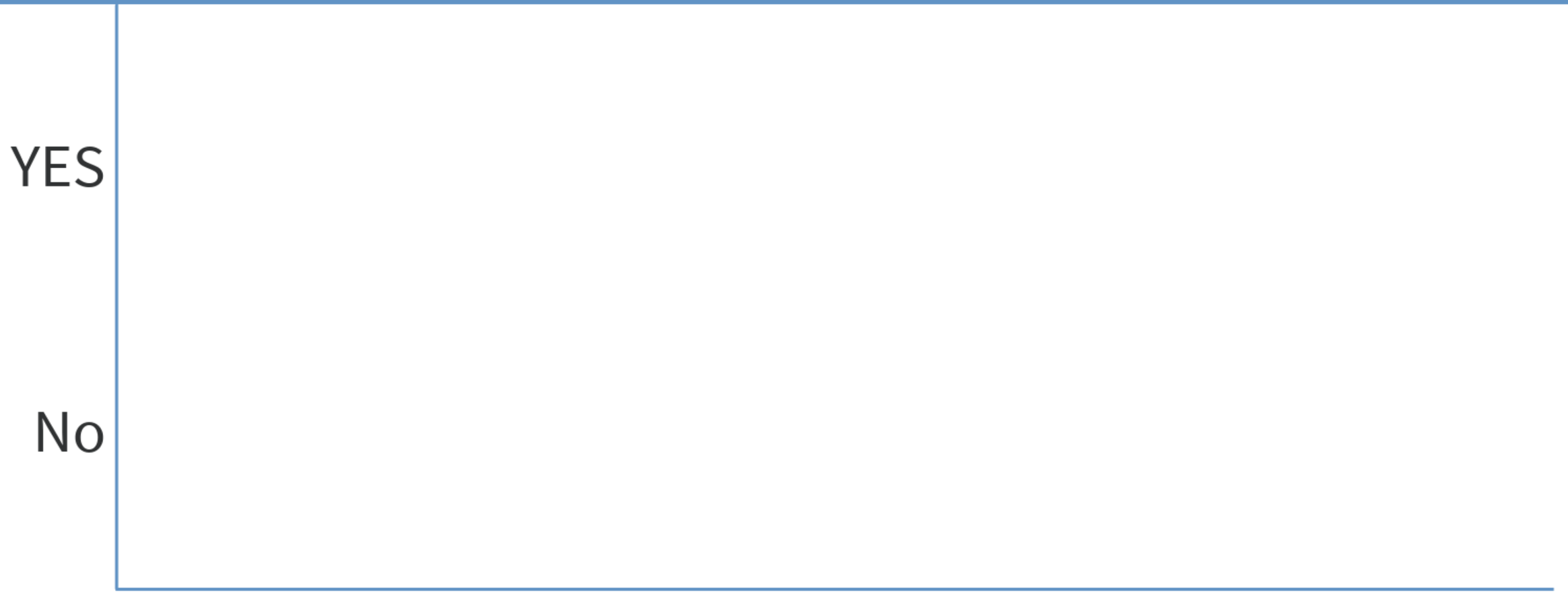
Insurance Data Security Model Law (MDL-668)

- based requirements of New York Department of Financial Services (NYDFS)
- Applies banking, insurance and financial service entities licensed in each state and regulated by state insurance departments.
- Versions passed by SC, OH, and MI

Franchisee Support = Brand Protection

- **Education and Resources**
- **System-Wide Response Plan**

Does your network have system-wide privacy and/or security training?



What resources does the franchisor provide to franchisees in your network?

1) Templates-- policies & procedures, contracts, etc.

2) Mandated policies & procedures, contracts, etc.

3) Some items are mandated and others are not

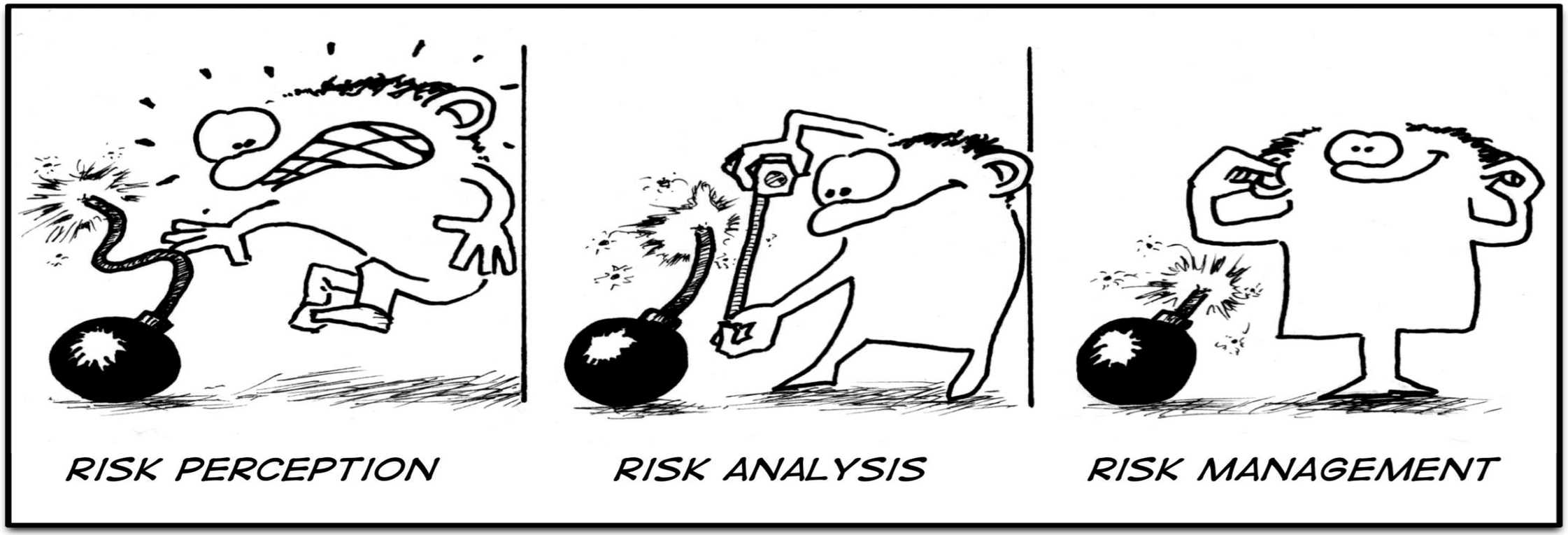
4) Franchisees are independently owned and operated

Franchisee Support = Brand Protection

System Wide Response Plan

- addresses the impact on the brand (i.e press and social media coverage).
- Insights from multiple constitutes within the organization including legal, compliance, IT, marketing and HR.

Practical Risk Protection



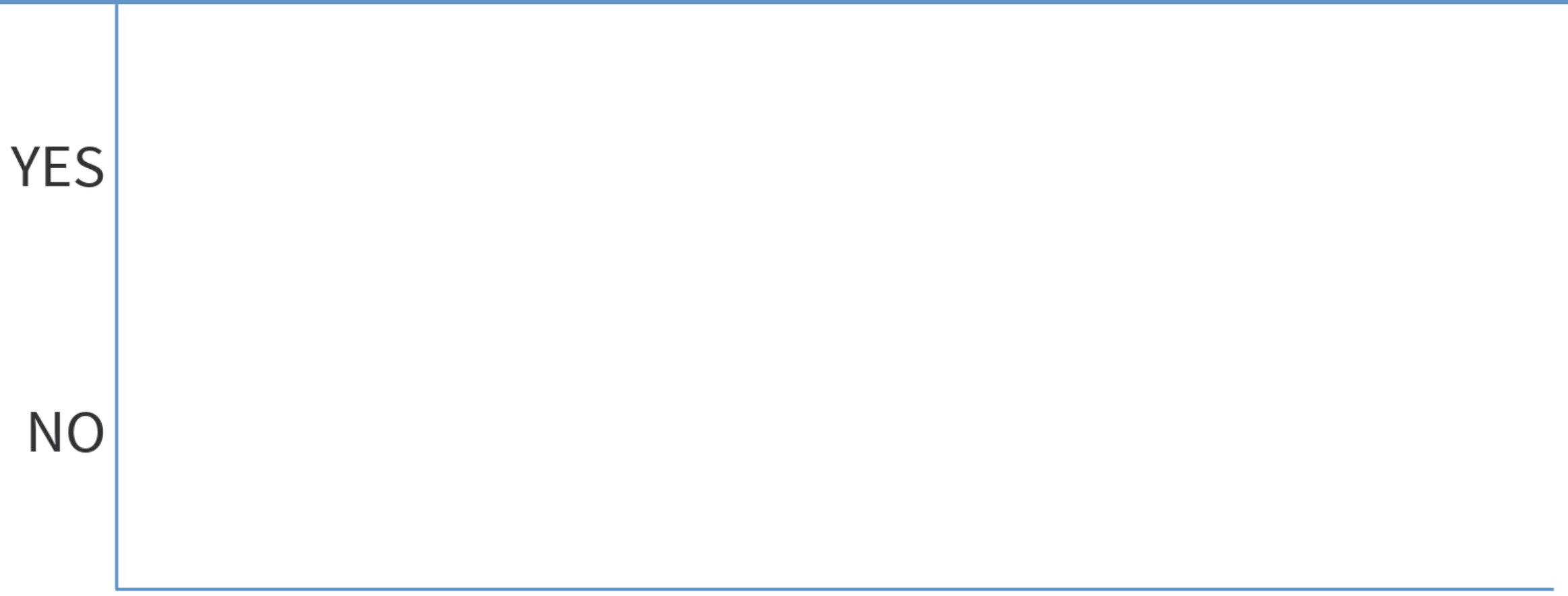
Practical Risk Protection- Methods for Limiting Risk

- Risk Assessments & Breach Prevention
- Policy Development: Adopt comprehensive privacy policies and comply with those commitments
- Vendor Contracts: Limitations of Liability & Indemnification
- Insurance

Practical Risk Protection- Risk Assessment

- Knowledge of all data flows within company devices/systems and personal devices/systems used for work
- Identify Key weaknesses and make a plan for management of that risk

If you are a franchisor, have you performed a risk assessment to identify your greatest risks?



Practical Risk Protection-

The Costs of a Breach in 2018*

- Average total cost of a data breach: $3.86 million
- Average total one-year cost increase: 6.4%
- Average cost per lost or stolen record: $148
- Likelihood of a recurring material breach over the next two years: 27.9%
- Average cost savings with an Incident Response team: $14 per record

*2018 Cost of Data Breach Study conducted by the Ponemon Institute

Practical Risk Protection-Breach Prevention--Sources

- Accidental Breaches
- Employee/Ex-Employee Actions
- Hackers and Thieves
- Corporate Espionage

Practical Risk Protection– Common Security Threats

- Virus
- Malware
- Trojan Horse
- Spyware
- Computer worm
- Others?

How Data Breaches Occur

1 Research

Attacker looks for weaknesses he can exploit

2 Stage Attack

SOCIAL ENGINEERING

Phishing email, spam with malware, phone call, dress like the night janitor, etc.

INFRASTRUCTURE WEAKNESS

SQL injection, vulnerability exploitation, session hijacking, etc.

Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved

3 Exfiltrate

DATABASE AND FILE SERVERS

Personally identifiable information (PII), credit card numbers, email addresses, other social details, etc.

HTTP-based path, FTP, email, etc.

Accessed data is exfiltrated back to attacker

Once the attacker maintains acess to the system, exfiltration can indefinitely proceed

Practical Risk Protection–
Example 1: Identity Spoofing

- It was near the end of the week, and one of our attorneys received an email from the CEO. He wanted to do something special for the legal team so he asked the attorney to purchase $100 gift cards for each member of the team and to send him the card numbers so he could reimburse her, but don't tell anyone since he wanted it to be a surprise.
- The attorney was happy to help and admired the CEO for being so thoughtful. The gift cards were purchased on her personal credit card and the gift cards numbers put in the reply email back to the CEO as requested. When the gift cards were handed out to the legal team, it was discovered that no money was on any of the gift cards.
- When the technical team investigated, we found that the email from the "CEO" was actually in disguise and sent from an untraceable AOL account. The thief spent all the gift card money as soon as he received the gift card numbers. The attorney resigned over the embarrassment and lack of due discretion.

Practical Risk Protection–
Example 1: Identity Spoofing

Lessons learned:

- There was no breach by force, therefore, firewalls and other traditional security devices were ineffective.
- This was a social engineering breach where the employee willingly, yet unknowingly, gave the hacker the information they desired.
- Employee education is the best defense to counter social engineering attacks. (An educated user would have looked at the CEO's email address and noticed the AOL email address.)

Practical Risk Protection–
Example 2: Mobile Device Security

- A hospital had several satellite offices for outpatient services. Patient's medical information was guarded with the best technical security available. This included multi-factor authentication to access patient data, which required the hospital employee to enter something they know (password), something they have (text message sent to their phone), and something of themselves (fingerprint) before they gained access to patient data.
- One day the police alerted the technical team that several patients of one of our clinics had their identity stolen.
- Upon investigation, the hospital discovered one employee accessed each of the patient's medical records whose identity were stolen.
- Printing of the data was blocked which lead to an audit of mobile devices which were managed through big brother software.
- The hospital found pictures of the computer monitor on the phone showing the patient information.

Practical Risk Protection–
Example 2: Mobile Device Security

Lessons Learned:

- The thief had permission to access the patient's records since they were directly involved in patient care.
- The advanced technology in place would not prevent access since access was appropriate for care.
- The mobile device management software was the key to providing evidence to convict the thief. It also showed we used reasonable precautionary measures to protect patient data.

Practical Risk Protection–
Example 3: The Imposter

- A large company invested a significant amount of money on data security; spared no expense on firewalls and other intrusion detection devices.
- The CFO hired a Microsoft employee to test the new security system. The two discussed the proposal in person, in the CFO's office. The Microsoft employee was a member of the Microsoft security team and had experience with hacking methodology.
- The CFO challenged the security expert to infiltrate the company's network and access sensitive financial data.
- The CFO was confident in the newly purchased hardware, and the security expert accepted the challenge on the spot and left the office.
- An hour later the Microsoft expert walked back into the CFO's office and delivered all the company's financial data on a thumb drive.
- The CFO was shocked to see all the financial data and in such a short amount of time.
- When asked how he infiltrated all the security, the hacker said after leaving his office he walked straight over to the receptionist and claimed he was with the IT department and needed her password for system testing.
- The receptionist, trained to be accommodating, provided her username and password.

Practical Risk Protection–
Example 3: The Imposter

Lesson Learned: Technical security is only one part of a comprehensive data privacy plan. User education and empowerment are another.

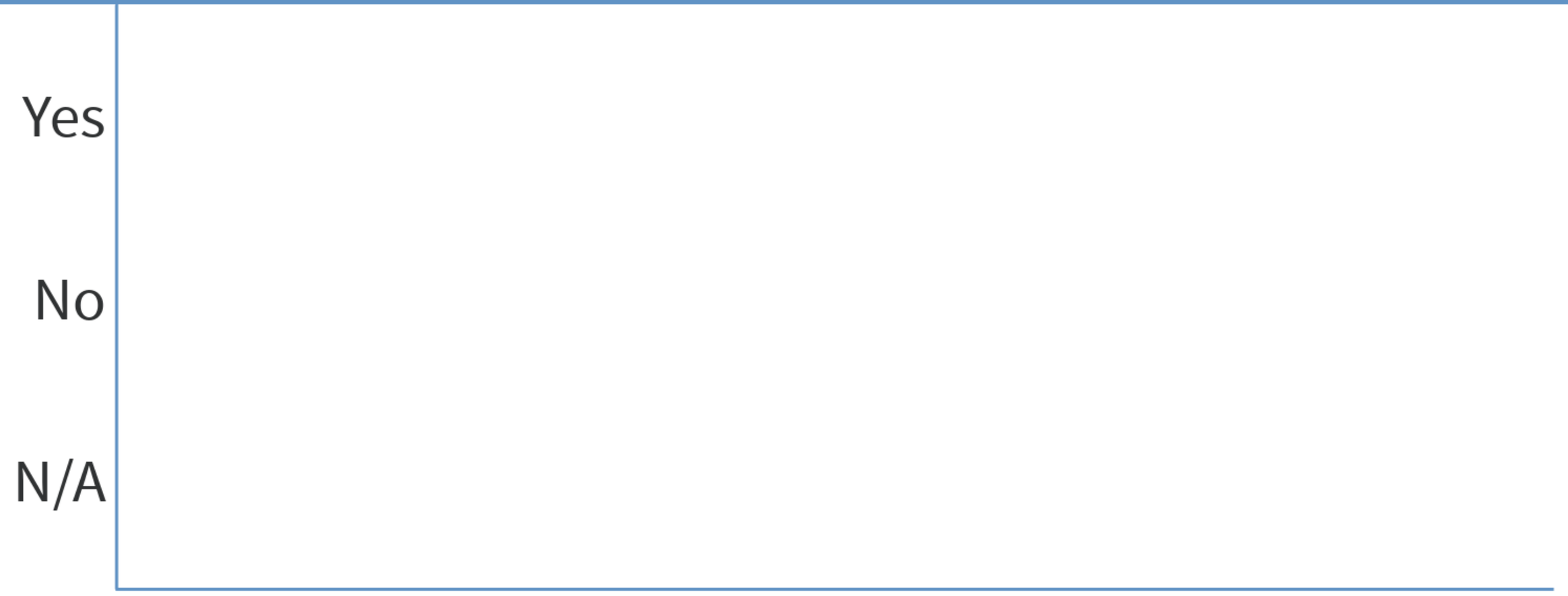
Practical Risk Protection–
Example 4: Sub Contractors

- In 2017 the US government discovered that Russian hackers gained access to a significant portion of the US electrical grid.
- Upon investigation is was found the hackers gained access by using phishing emails.
- Phishing is when a hacker sends you an email that looks legitimate and entices you to click on a link or open an attachment. This action triggers a virus which provides the hacker access to your system.
- In this case, the hacker did not phish the electrical company directly. Instead, they sent the malicious email to vendors who do work for the electrical company.
- Vendors are often given access to a company's network to perform specific work. However, not all companies are good about revoking access after the work has been completed. The hacker was able to get the username and password of a vendor who still had access to the main system grid. From there they were able to access sensitive system information and control.

Practical Risk Protection–
Example 4: Sub Contractors

Lesson Learned: Companies must be diligent about allowing third-party access and removing access.

If you are a franchisor, do you have privacy and security policies and procedures in place?



Practical Risk Protection-
Indemnification

- Allocating risk by express agreement whereby one party (the indemnifying party) agrees to compensate the other party (the indemnified party) for direct claims, third-party claims, or both (covered events).

Practical Risk Protection-

Limitation of Liability

Limitation of the **Amount** of Liability

Common Caps: fixed dollar amount, amount covered by indemnitor's insurance, and fees received under the contract over a period of time (e.g., 3x the annual value of the contract)

Limitation of the **Type** of Liability

Exclusion of certain types of damages - e.g., consequential damages

RISK ALERT: Inappropriate waiver of indirect and consequential damages.

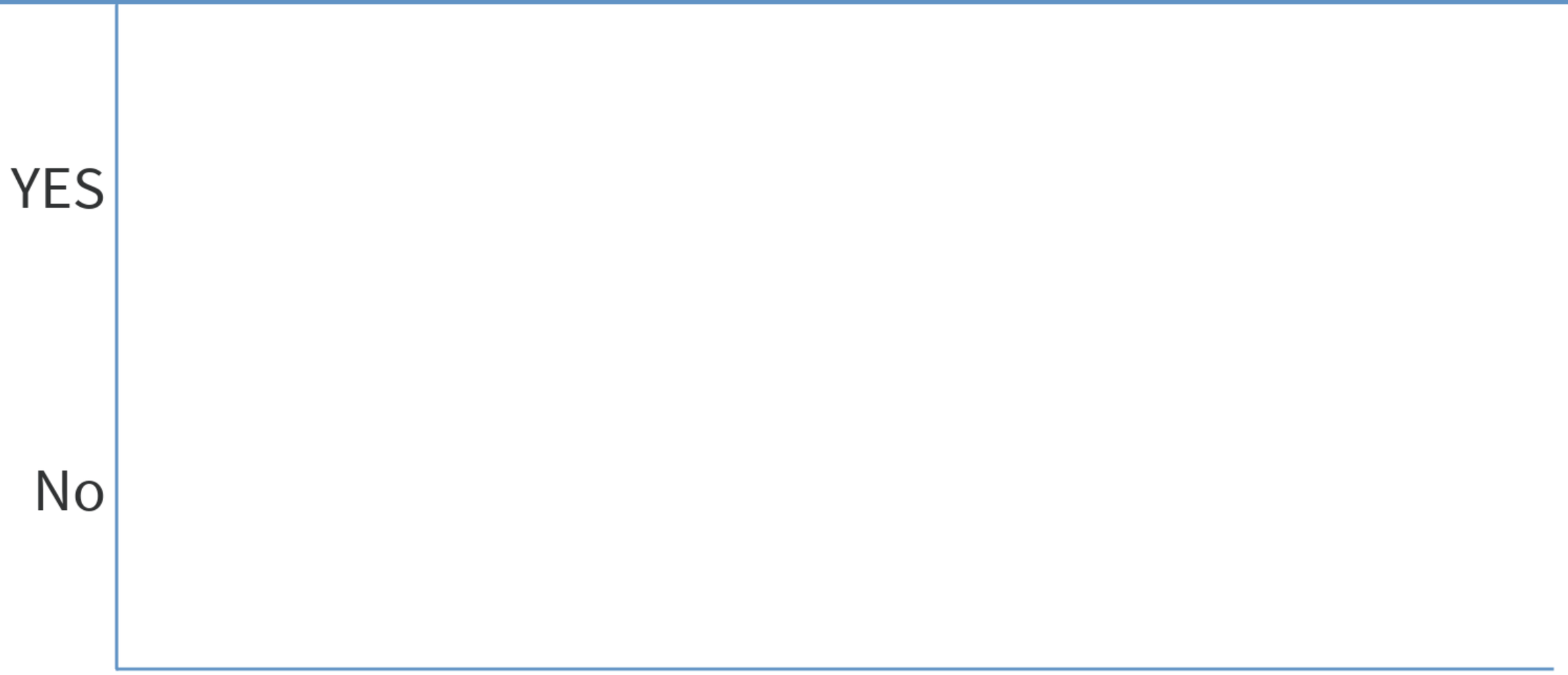
Common Carve-Outs: third-party claims under indemnification provisions, personal injury, breach of confidentiality, intellectual property claims, gross negligence, data breach, violations of law and willful misconduct or fraud

RISK ALERT: Failure to include appropriate carve-outs.

Practical Risk Protection- Insurance

- Commercial General Liability insurance generally does not cover data breaches and related losses
- Provisions to look for in Cyber Insurance Policy
  - Coverage of data breaches (e.g. theft of personal information)
  - Cyber attacks on your network
  - Cyber attacks on your data held by vendors
  - Cyber attacks that occur worldwide (not just in the US)
  - Terrorist attacks
- Other provisions to consider
  - Duty to defend
  - Whether coverage is excess

Do you currently have cyber insurance coverage?



THANK YOU