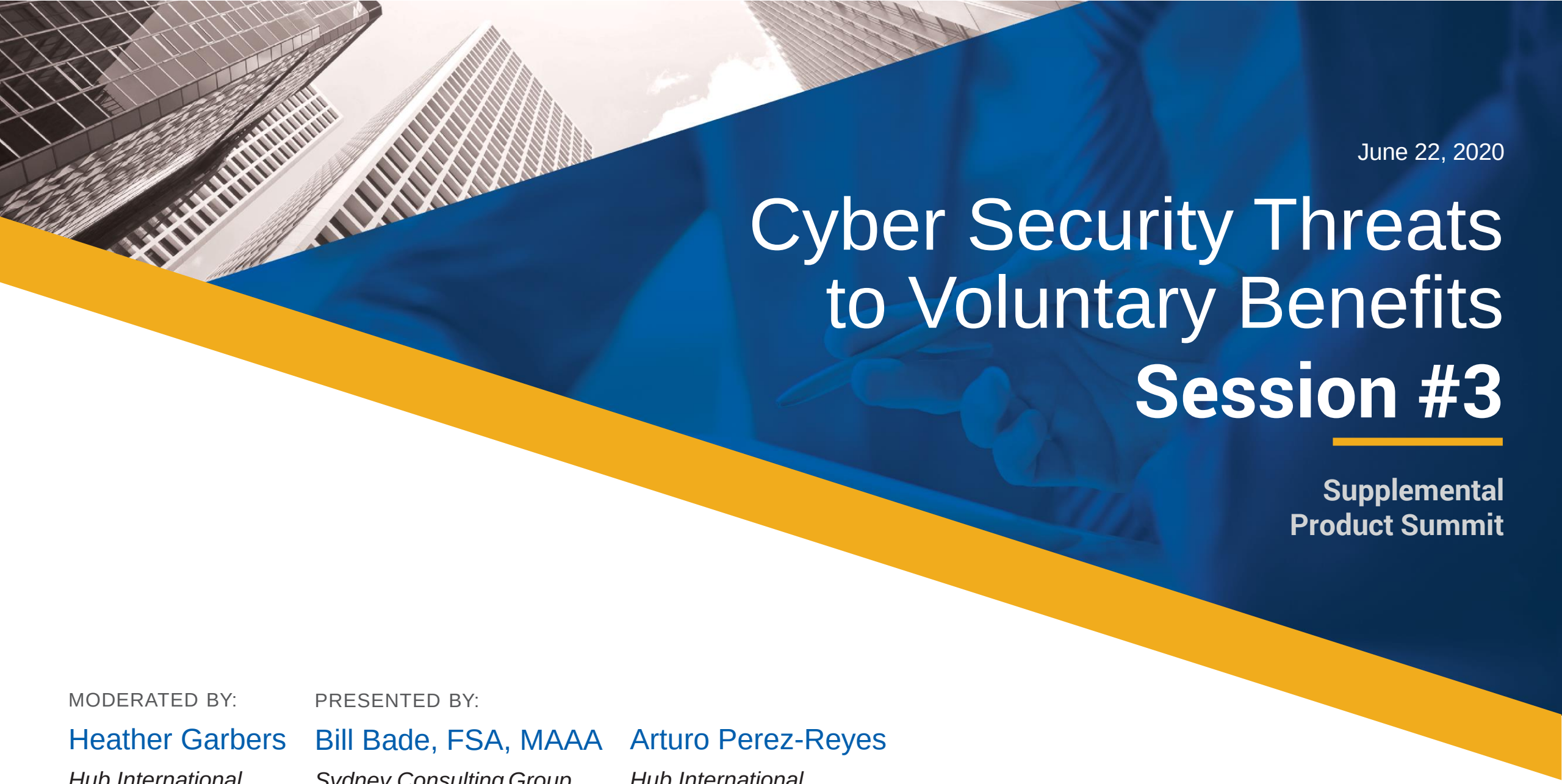


June 22, 2020

Cyber Security Threats to Voluntary Benefits

Session #3

Supplemental Product Summit

MODERATED BY:

Heather Garbers

Hub International

PRESENTED BY:

Bill Bade, FSA, MAAA

Sydney Consulting Group

Arturo Perez-Reyes

Hub International

INTRODUCTIONS

Heather Garbers
Vice President
Hub International

Arturo Perez-Reyes
Senior Vice President
Hub International

Bill Bade, FSA, MAAA
Consulting Actuary
Sydney Consulting Group

Topic

- Supplemental-insurance carriers:
  - Enroll consumers through third-party platforms
  - Exchange data with benefit-administration systems
  - Work with third-party administrators and other providers
- What are the cyber-security perils and potential losses?
  - What data assets do you have to lose?
  - What would it cost if you lost these assets or processes?
  - How do you protect by avoiding, preventing. mitigating, and transferring

CYBER SECURITY THREATS / LANDSCAPE

CYBER THREATS

Definition

A malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.

Examples

Malware / Spyware / Ransomware (software that performs malicious tasks on a device or network), Phishing, DoS (disruption of computer network by flooding the network with superfluous requests to overload the system), Zero-Day Exploits (flaws in software or hardware that are unknown to the parties responsible for patching the flaw), Trojans, Wiper Attacks (wipe the hard drive of the infected computer), etc.

Source: https://www.upguard.com/blog/cyber-threat

REAL WORLD CASES

Larry Basich gets health coverage after $407,000 Obamacare exchange glitch

Allscripts faces lawsuit after ransomware attack impacts doctors' offices across U.S.

Insurer Breaches

- Chubb 2020
  - Attacked by Maze
  - Ransomware with exfiltration
- State Farm 2019
  - User ID and password on Dark Web
- Dominion National 2019
  - Insurer and TPA of dental and vision benefits
  - 2.9 Million members affected by 9-year PHI breach

CURRENT **ENVIRONMENT**

Adoption of Cloud Computing

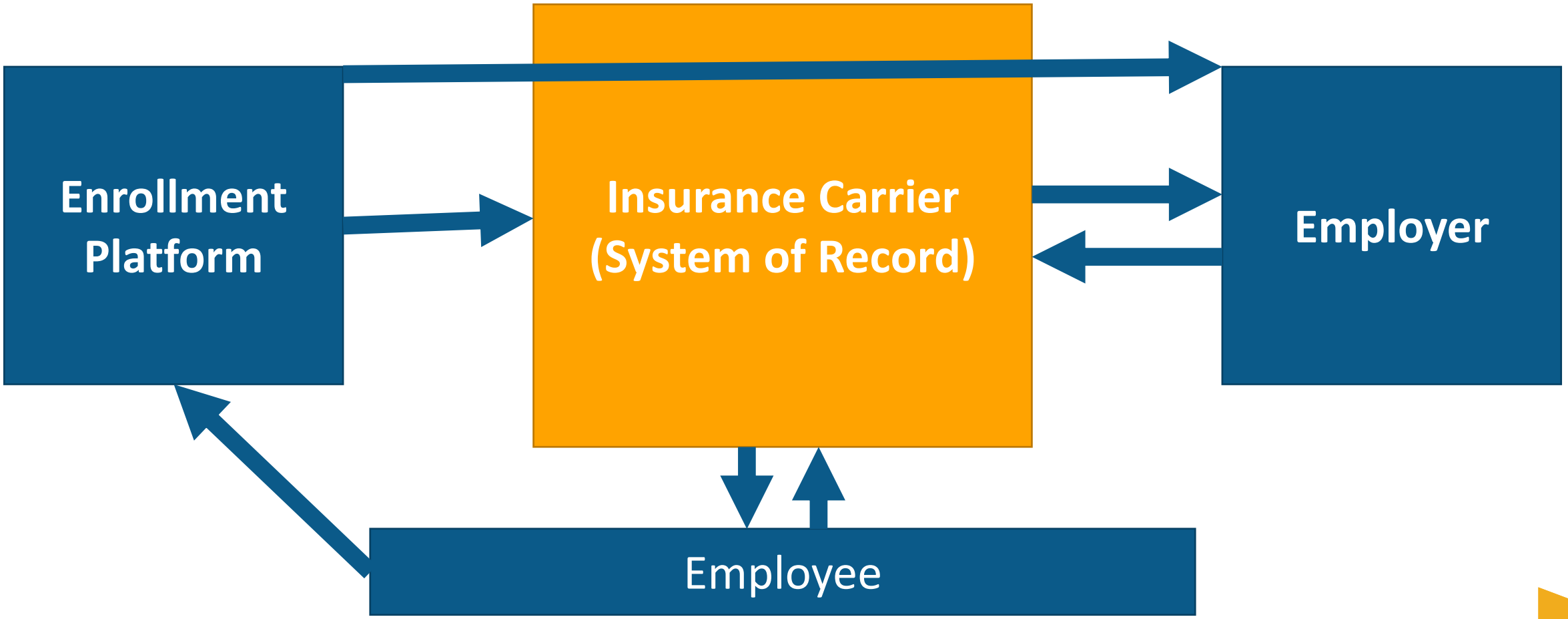
“This pandemic has increased the dependency of the healthcare industry on tech companies further. The need for smart and efficient ways of managing the spread and treatment of extremely contagious virus via advanced datasets, cloud computing techniques and analytics has become the utmost need of the hour.” – Shilpa Mete, Zacks

Adoption of Cloud Computing

“What is concerning […] is that as [cloud containers] are published, the race is on for attackers to develop an exploit because launching a successful attack on a container could have much broader consequences. Compared to other technology, containers can be more numerous and quickly replicated. The attack footprint could expand rapidly, and a number of victims may be extremely high.” – Marina Kidron, Skybox Security

THIRD PARTY RISKS

ENROLLMENT **PROCESS**



Vendor exposures

- What
  - Bomgar survey: On average, companies allow 89 vendors to access their networks weekly
  - Ponemon: 59% of firms have suffered a data breach from vendors
  - PwC: Data breaches related to third-party vendors has increased by 22% since 2015
- Why
  - Vendors serve many customers
  - Vendors are plentiful
  - Most companies improperly manage their vendor risk

Vendors losses

- Why
  - Industrial espionage by competitors
  - Espionage by foreign intelligence services
  - Ransomware and extortion of data and processes
  - Hacking and theft of assets by criminals or syndicates
  - User or corporate error regarding computers, nets, or apps
  - Accidental or premature distribution of a sensitive information
- How
  - 44% experienced a significant data breach caused by a vendor
  - 50% malware
  - 32% affected personal identifiable data
  - 29% included payment information
  - 26% of the breaches were stolen passwords
  - 24% exposed proprietary business data
  - 15% of firms were notified by vendor

Vendor breach consequence

- Operational Risk
- Compliance Risk
- Reputation Risk
- Strategic Risk
- Credit Risk

- Examples
  - 52% Increased operational complexity and cost
  - 27 % Disrupted operations
  - 26% Financial losses and penalties
  - 19% Reputational damage

Third-party data breaches 2019

- Quest Diagnostics, LabCorp, BioReference Laboratories, Carecentrix, and Sunrise Laboratories
  - What: 20 million patients: credit card numbers to bank account information and even social security numbers
  - Who:American Medical Collection Agency (Chapter 11 Bankruptcy
- U.S. Customs & Border Protection
  - What: 100,000 photos of license plates and travelers' faces
  - Who: unnamed subcontractor's network
- Focus Brands Inc. restaurant franchising group
  - What: payment information of countless customers vulnerable in from April 2019 to July 2019)
  - Who: Point of Sale (PoS) vendor was hacked
- FBI
  - What: 3 terabytes of information: investigation records, millions of files, personal data, system credentials, and internal communication records
  - Who: server belonging to Oklahoma Dept. of Securities.

Third-party data breaches 2019

- Facebook 1
  - What: 540 million records of user IDs, account names, comments, and more exposed on a publicly accessible server
  - Who: A digital media company called Cultura Colectiva, based in Mexico
- Facebook 2
  - Plaintext passwords and email addresses for 22,000 users were exposed
  - Who: At the Pool, a third-party Facebook app

Third-party data breaches of all time

- Target 2013
  - What: PCI of 41 million customers, PII of around 70 million. So 140 lawsuits and $292 million loss
  - Who: A third-party HVAC vendor
- Equifax 2017
  - What: 147 million consumers: names, SSN, DOB, addresses, driver`s license numbers. Credit cards of 209,000 US consumer. Costing $1.38 billion
  - Who: The open-source software Apache Struts
- Home Depot 2014
  - What: PCI on 150 million customers, and 53 million email addresses. Cost $289.5 million
  - Who: third-party vendor’s login credentials to install memory scraping malware on over 7,500 self-checkout POS terminals
- Marriott International 2018
  - What: 500 million guest accounts
  - Who: Starwood guest reservation database

Third-party data breaches of all time 2

- Under Armor 2018
  - What: 150 million accounts : usernames, passwords, and emails
  - Who: MyFitnessPal app, acquired in 2015 for $475 million.
- Saks, Lord & Taylor 2018
  - What: Credit and debit card data of more than 5 million people
  - Who: The cash register systems
- Managed Health Services 2018
  - What: 31,000 plan members names, insurance IDs, addresses, dates of birth, dates of service, and medical conditions
  - Who: LCP Transportation vendor company
- MyHeritage Genealogy Site 2018
  - What: Exposed records: 92,000,000: hashed passwords and emails.
  - Who: third-party payment processors for financial operations,
- Chili's and Applebee's 2018
  - What: Payment card data, including names and credit or debit numbers
  - Who: third-party payment processors for financial operations

Third-party data breaches of all time 3

- Universal Music Group 2018
  - What: Everything in UMG's cloud data storage, such as file transfer protocol (FTP) credentials, AWS Secret Keys and passwords, and the internal and SQL root password
  - Who: contractor who forgot to password protect an Apache Airflow server
- DoorDash 2019
  - What: 4.9 million people affected: names, email addresses, delivery addresses, order history, phone numbers, encrypted versions of passwords, last four digits of payment cards and bank account numbers, and100,000 delivery people were also accessed.
  - Who: third-party service provider

REGULATORY FRAMEWORK

Regulations: new responsibilities and risks

- Changed enforcement
  - CCPA on July 1
- Changed paradigms
  - GDPR and CCPA rights of individuals. From confidentiality to accessibility and integrity
- Changed exposures
  - Biometrics, “sensitive data” in GDPR and CalPRA
- Changed penalties
  - AG cure periods and action. But private right if no encryption
- Changing laws
  - CalPRA : threshold increases, but so do fines and new cure protocol allowing private right
  - Others on the way: WA, NY, NJ, IL, NV, MI, and others
  - BIPA private right to action

New challenges from GDPR, CCPA, and others

PROBLEM: Under GDPR and CCPA, firms could face regulatory actions and penalties that are not triggered by a breach of privacy.

DATA RIGHTS: These laws require firms to respect certain rights.

GDPR	CCPA
1. Right to be forgotten. 2. Right to opt out. 3. Right of access. 4. Right to data portability. 5. Right to object.	1. Right of Disclosure or Access 2. Right of Data Portability 3. Right to Deletion/Erasure (Forgotten) 4. Right of rectification 5. Right to Restrict Processing 6. Right to Object to Processing 7. Right to Object to Automated Decision-Making

DEFINITION: They enshrine the three legs of the CIA triangle. Privacy policies are about confidentiality

1. Confidentiality
2. Integrity
3. Availability

SOLUTION: Policies must respond to all aspects of local and foreign privacy statutes and regulations

Insurability of privacy fines

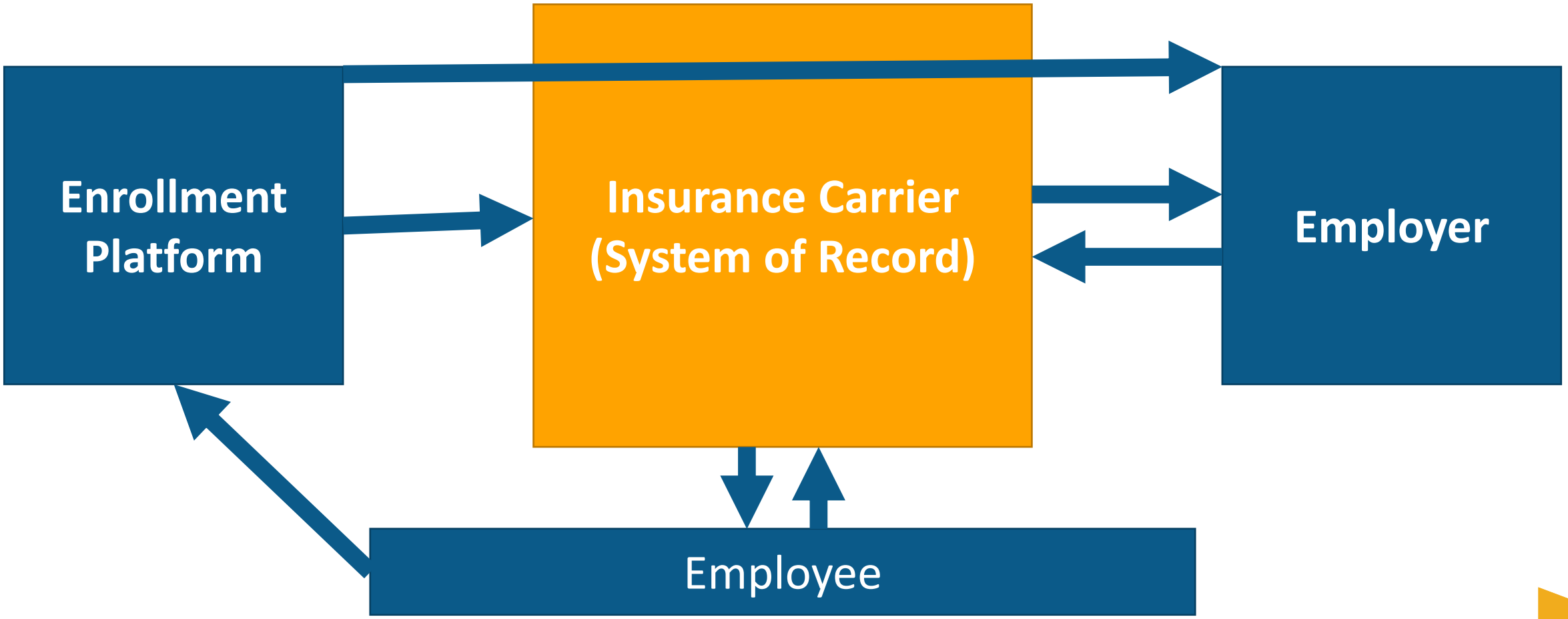
Criminal or intentional misconduct would draw punitive fines.

- **US**: They are not insurable in California and 21 states.
- **UK**: They are uninsurable in the UK, because they are barred by British law, their FCA's insurance regulations, and their Information Commissioner Office (ICO).
- **EU**: The situation is not yet litigated in the EU, but the moral hazard is the same. ICOs fines must be "effective, proportionate and dissuasive." Deterrence bars insurability.

- **Negligent or inadvertent conduct** could also result in fines. The scale of the regulatory reaction will depend on the degree of negligence and the need to deter. For example, Google and Facebook have faced increasingly larger fines, as their errors have accumulated. A 2018 survey by DLA Piper found that in 20 of the 30 EU countries fines are uninsurable. In eight countries, the situation is unclear. And only in Finland and Norway would fines be insurable for negligent conduct
- **Statutory responses to breaches** tie to jurisdictions and laws. The EU has modelled its privacy notification requirement on California. There are stricter state laws and several, like CCPA, in the works. The cross national standard is likely to be the highest legal standard. See the FTC's Choicepoint decision that found it unfair to all not to use the highest standard available to some.

RISK MITIGATION

RISK **MITIGATION**



Supplier-risk management (SRM)

- Questions
  - What do you have to lose?
  - What would it cost if you lost it?
  - How are you going to protect it?
  - If you can’t, how will you mitigate its loss?
  - And can you turf the risk or loss via a contract or via insurance?
- Processes
  - Effective vendor selection process
  - Streamlined due diligence and continued oversight
  - Structured vendor risk assessment approach
  - Efficient vendor performance monitoring
  - Disciplined vendor governance framework

Residual problem

- Contracts
  - Vendors will refuse to give indemnities
  - Because their aggregated exposure is huge
  - They also cap losses at the value of the contract
  - Contract value bears no relationship to the asset value
- Insurance
  - Privacy insurance covers losses by vendors contracted by the insured
  - But it does not cover liabilities caused by sub contractors of contractors
  - Example: Insurer uses a vendor that uses a cloud provider, and the latter breaches

Same problem for individuals

- A firm provides retirement benefits using a trust and TPA
- Someone steals money from an employee. No one can identify who lost what
- Often the employee was the cause of the loss and expects to be compensated
- Ditto for wealth managment
- The employer and vendors do not have insurance that covers losses of individuals
- Nor are they obligated by law to make them whole, though it is a custom
- The solution is to insure the whole chain by providing the employee or wealth client with crime and identity coverage

SPEAKER INFO

Heather Garbers

- Heather is responsible for driving Voluntary Benefit strategy and solutions at HUB International. In this capacity, she partners with the HUB team and clients to create strategies to engage employees in benefits with custom product, enrollment, and communication solutions. Her carrier agnostic strategy allows Hub to truly partner clients with the best fit for their and their employees' needs. She is very passionate about the Voluntary Benefits industry and its ability to allow employees to personalize benefits to their unique needs, by providing financial wellness solutions to protect themselves and their loved ones.

- Heather is a Certified Voluntary Benefit Specialist (CVBS) and an Executive Member of the National Advisory Board for the Voluntary Benefits Association. She has also been recognized as a leader in the industry including recipient of Employee Benefit News 2015 Voluntary Advisor of the Year Award and was named one of the "15 Women in Insurance You Need to Know" by LifeHealthPro in March 2016

- Prior to joining HUB International, Heather was a Voluntary Sales Executive with a regional brokerage and Regional Sales Manager and Training Specialist with a carrier. Overall, her insurance industry experience spans 14+ years. She earned a Bachelor's of Science degree in Business Administration from the University of Nebraska-Lincoln.

Arturo Perez-Reyes

- Arturo Perez-Reyes is an SVP at Hub International where he works as an insurance broker, risk consultant, and leader of the Cyber and Technology Practice. He has spent 19 years helping companies identify, quantify, and insure risks from technology, services, value chains, intellectual property, regulatory compliance, information security, and privacy.

- He developed the first privacy policies and produced hybrid products that provide insurance and information-security services. He is an expert in manuscripting placements to adjust for exposures, gaps, and overlaps.

- He also does enterprise-risk consulting and issue-specific engagements for mid-cap to Fortune 50 companies. The studies have identified, quantified, and mitigated liabilities and losses from data losses, privacy violations, confidentiality torts, intellectual-property invalidation and litigation as well as from new technologies, emerging services, IT value chains, information sharing, and regulatory compliance.

- Arturo is also a member of the professional faculty at the Haas School of Business, UC Berkeley. He teaches e-commerce, insurance, sales, green business, and communication.

Bill Bade, FSA, MAAA

- Bill Bade is a Consulting Actuary at Sydney Consulting Group, where he provides supplemental life and health support to insurance carriers, brokers, and technology firms of all sizes. Bill specializes in all aspects of product development, strategy, pricing, valuation, and financial reporting.

- Prior to founding Sydney Consulting Group, Bill held roles of increasing responsibility at Allstate Benefits in Jacksonville, Florida. Bill's experience at Allstate Benefits spanned both actuarial and non-actuarial positions, including as Vice President of National Account Management.

- Bill also founded Sydney Administrators to provide third party administrator (TPA) service to carrier clients. Sydney Administrators actively supports insurance carrier clients and is licensed by state insurance departments.

- He is active in his community and previously founded and grew a non-profit organization.

CLOSING REMARKS / QUESTIONS