



Premier Provider of Innovative Insurance and Surety Solutions



## INDUSTRY UPDATES WHAT YOU SHOULD KNOW

Jaki Ferenz, Vice President

Keith Sanchez, Divisional Vice President

March 20, 2019

# Topics We Will Cover

- Tariffs/Bond Stacking
- General Average
- SB1402
- CARB
- Carrier Vetting
- Cyber Liability



# Increased Tariffs and Bond Stacking



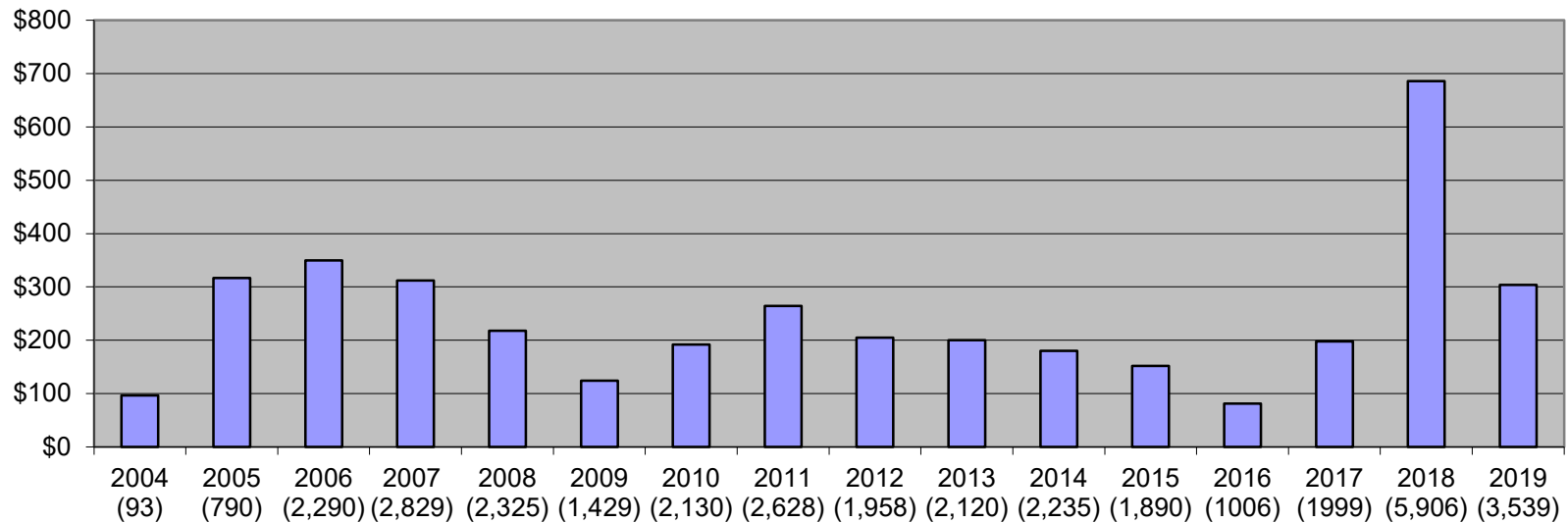
# Tariff Increases and Bond insufficiencies

- New tariffs causing significant increases in bond limits
- Sureties have received 3,500+ insufficiency notices so far this year with 15 days to terminate & replace.
- Previously duty free importers are going to \$1.8 - \$26M bonds (eek!)



# CBP Sufficiency Notification Statistics

**Bond Liability Amount Increases  
(Insufficiency Letters Issued)  
(2004-2019)**



# Tariff Increases and Bond insufficiencies

- **No Big Deal, Right??.....WRONG**
  - 15 days to obtain new CTB apps, current financials, possibly collateral, which can take time.
  - Importers financials may not support new duty requirements.
  - Collateral takes time.
  - Until bond sufficiency is resolved, possible CBP penalties, demurrage, delay can be incurred.

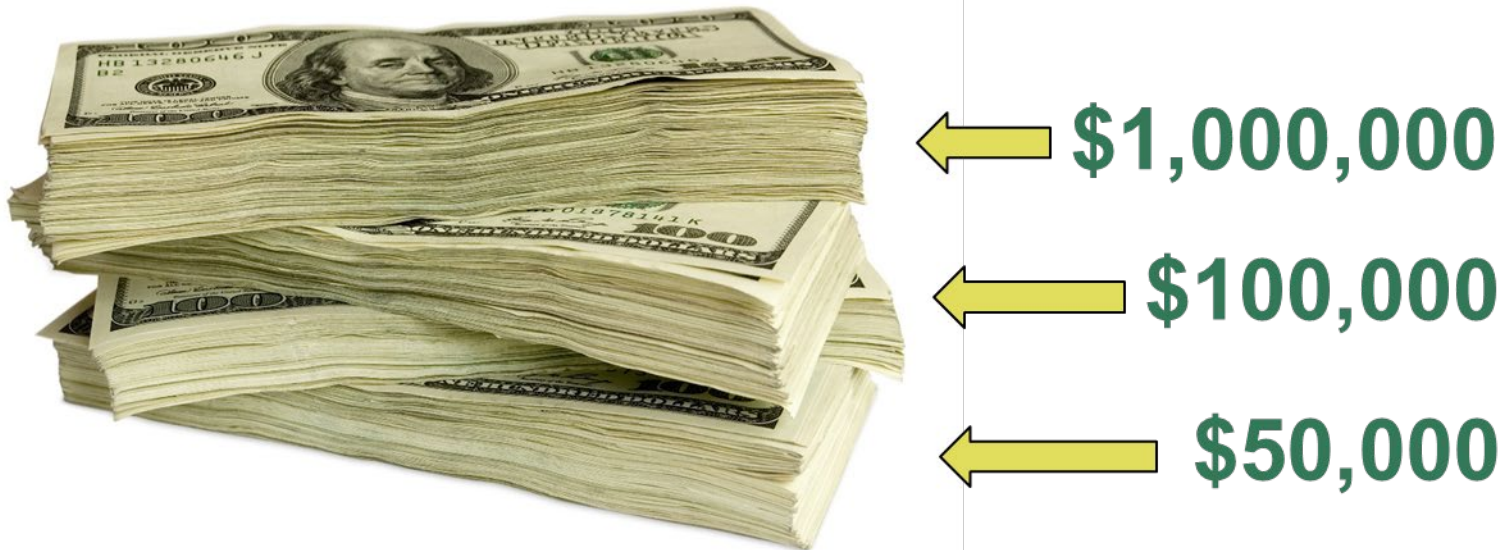
# Tariff Increases and Bond insufficiencies

- **Next Problem...**
  - CBP **looks back** 12 months at duties, taxes and fees, which may include only a few months worth of additional tariff increased duty amounts.
  - Importers need to accurately predict **future duties 12 months out**.
  - If the importer does not include future months with the higher duties considered, **another insufficiency notice may show up within the next three months!**



# Bond Insufficiency/Stacking Liability

- Stacking liability occurs when a surety has open exposure for multiple bond periods
- Sureties are liable for the full bond limit until all entries for the bond period have been liquidated for 90 days past last date of liquidation





# Bond Sufficiency Considerations

- CHBs can help importers monitor bond sufficiency – Be proactive vs. reactive!
- Surety provider insufficiency notices to CHB should not be taken lightly.
- CHBs should notify their importer ASAP, advise them to accurately forecast their future import duties, taxes & fees to increase bond amounts before CBP issues arise.
- Importers should consider an additional buffer of duty volume for the unexpected additional tariff increases.
- **FORECAST, FORECAST, FORECAST**

# General Average



# General Average

- Ocean marine loss
  - Voluntary sacrifice to save cargo/vessel/life
  - Extraordinary expenses are incurred
    - Jettison of cargo
    - Extinguishing a fire
    - Towing
- All cargo is seized. Amount of GA loss is determined
  - Must post security deposits



# Sample General Average calculation

Vessel and freight value	\$100 million
Saved cargo value	\$100 million
Contributing value (total)	\$200 million

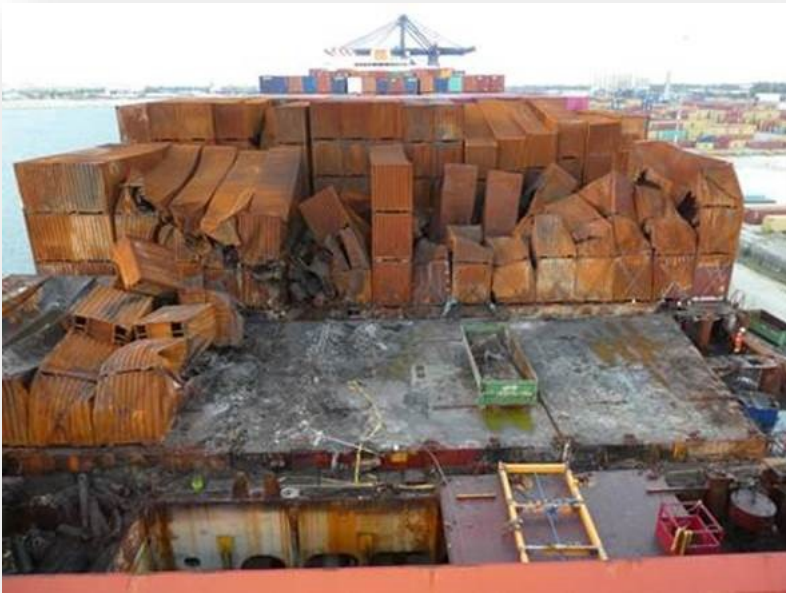
- \$40 million in cargo was sacrificed
- The loss represents 20% of the contributing value
- Cargo owners must contribute 20% of respective cargo values
- A shipper with a \$100,000 shipment must pony up \$20,000
- **HOWEVER** ..... if insured, the Insurance company puts up \$20,000 and cargo is released.
- GA claims take years to resolve.

# General Average Loss – Yantian Express Timeline

- MV Yantian Express
  - Deck fire on January 3, 2019
  - Crew was evacuated to salvage tug on January 5
  - Hapag-Lloyd declared GA on Jan. 25
  - Vessel towed to Freeport Bahamas on Feb. 4 where salvage adjusters will determine financial lost



# General Average Loss-Yantian Express



Photos courtesy of Master Mariner

# General Average Loss-Yantian Express Timeline

- As of February 12th, 2019 – **202 containers** are a total loss and around **460 containers** have yet to be surveyed. Salvage operations are ongoing.
  - Average Guaranty: 28%
  - Salvage Security: 32.5%
  - **60.5% CASH DEPOSIT FOR UNINSURED CARGO**
- March 11th, 2019 – The discharge of damaged cargo from the containership is expected to take an additional four weeks, said Ocean Network Express, an alliance member of ship owner Hapag-Lloyd.

A cargo owner with a cargo worth \$100,000 is going to have to pay **\$60,500** to get their goods!!!



# General Average – The perfect time to sell .....

## GENERAL AVERAGE

## & THE NEED FOR CARGO INSURANCE

Imagine receiving a message from an ocean carrier that all cargo aboard the vessel has been impounded and you need to post cash or a guarantee to retrieve it. This may sound like extortion, but it's actually a common maritime event known as General Average.

General Average is declared when an intentional sacrifice is successful in preserving the common safety of the ship, persons or property while at sea.

### Sample General Average Loss

General Average claims require all cargo owners on a vessel to contribute to the loss. Even if your cargo isn't damaged, you still need to make a financial contribution (based on the total value of the ship's cargo) for your goods to be released.

#### Here's how it works:

Value of vessel = \$60 million  
Value of cargo = \$140 million  
Total value of voyage = \$200 million

- Assume cargo loss and vessel repairs total \$20 million.
- Therefore, \$20 million out of \$200 million, or 10%, of the voyage suffered a loss.
- Each cargo owner must contribute 10% of the value of their cargo.
- A cargo owner with a \$100,000 shipment would have to put up \$10,000 to get the cargo released.

#### If cargo isn't insured

Cargo will not be released until the shipper posts a guarantee, which must be in the form of a cash deposit, bank guarantee or bond.

#### If cargo is insured

The marine cargo insurer should be notified immediately.

The insurance company will post the General Average Guarantee to meet the cargo owner's contribution and facilitate release of the cargo.

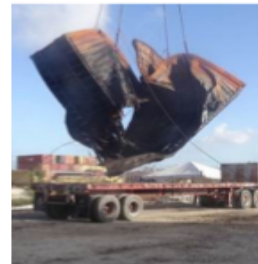


Photo Credit: Master Mariner



#### Yantian Express declares General Average

On January 25, 2019, due to a deck fire that spread to containers, Hapag-Lloyd formally declared General Average for the container ship Yantian Express.

As of February 12, 2019, 202 containers are a total loss and around 460 containers have yet to be surveyed. Salvage operations are still ongoing. Security for uninsured cargo requires a cash deposit of 28%.

**What would you do if your cargo was on board this vessel?**

For more information on how cargo insurance can protect you from the threat of General Average, contact your local Avalon representative.



WWW.AVALONRISK.COM

Atlanta | Boston | Charleston | Chicago | Houston | Los Angeles | Miami | New York | San Francisco | Seattle | Toronto



Form C308 2018/02/04

## Other General Average Exposures

- Will the uninsured shipper pay \$60,500 to get their \$100,000 container? Maybe Not...
  - Who will pay for the demurrage?
  - Who is the Shipper on the Master Bill of Lading?
  - Who is the Agent to the Shipper?
  - Do you have Extra Expense Coverage??
  - What if you stuffed the container that caused the fire?
  - What if you gave wrong shipping instructions?

## SB1402 - Effective on January 1, 2019

[https://www.dir.ca.gov/dlse/List\\_Port\\_Trucking\\_Companies\\_Outstanding\\_Judgments.html](https://www.dir.ca.gov/dlse/List_Port_Trucking_Companies_Outstanding_Judgments.html)

- CA Law - hiring carriers with labor violations could make you jointly and severally liable
- Any company that works with one of the trucking companies published on the DLSE's list will be risking liability should the company commit any more violations.
- Violations - failure to pay wages, failure to remit payroll taxes, failure to pay worker's comp coverage, or misclassification of employees and more.
- A list of port trucking companies with outstanding judgements can be downloaded monthly on the Labor Commissioner's office site.
- This affects other companies, not just based in California.

# Domestic Liabilities - SB1402

## SB1402

Example: Big trucking client

- Sued by 12 drivers for \$1.2M (\$100K per driver)
- Trucking company lost suit and is planning an appeal
- Appeal bond required. Financials not good. Collateral required.

CA Trucking Assn: Out of 100 cases in front of labor board, trucking companies lost 99 of them

### California Air Resource Board (CARB) mandates...

- Trucks older than 2004 must comply with the new regulation and meet the compliance schedule by January 1, 2020.
- California has strict regulations regarding Transport Refrigeration Units (TRUs or “reefers”).
- Brokers and freight forwarders are required to verify that reefer trucks hauling for them in California are CARB-Compliant.
- CARB compliance **includes out-of-state entities.**

## Domestic Liabilities - CARB

- CARB minimum fine per violation, per day is \$1,000.
- CARB fined Marten Logistics and Roadrunner Transportation Systems both acting as out of state brokers.
- Marten Logistics was fined \$100,000 and Roadrunner Transportation Systems, \$52,250.
  - Both entities were fined for failure to verify that **trucks hired or dispatched for service** were compliant with the state's tough Truck and Bus Regulation, and for not keeping adequate records as the law requires.

# Domestic Liabilities – CARB Compliance Considerations

- **How can a broker or forwarder know which carriers have compliant reefer units?**
  - Require carriers to provide proof of compliance.
  - Require the carriers they hire to register their reefer units in the Air Resources Board Equipment Registration (ARBER) system and provide an ARBER Certification Page for the units they will utilize for hauling the entities loads.
  - 100 Percent-Compliant Carrier List Search Page is: <https://arber.arb.ca.gov/publicTCCReports.arb>.
  - **Need more help? Discuss with your transportation attorney how to become CARB compliant.**



# Domestic 3PL Liabilities

How do you **define yourself when arranging for transportation** domestically on behalf of your customers?

Are you acting as a freight forwarder, or broker? Uncertain?

<https://www.fmcsa.dot.gov/registration/getting-started>

- Become licensed as a transportation broker/surface forwarder to reduce risk of being painted as an unlicensed motor carrier.

**Think catastrophic losses....Not properly licensed?**

# Domestic 3PL Liabilities



**Case law has increased domestic forwarder/freight broker vicarious auto liability exposures for bodily injury, death and property damages.**

**Potential exposures may include:**

- Taking too much control over motor carriers actions.
- Negligent selection of hiring a carrier exposure.  
(Common liability theory)

## Pro-active Risk Management Considerations:

- Have carrier vetting procedures in place to verify carrier's operating authority, safety rating, insurance, etc. **that employees must adhere to for every load.**
  - <https://safer.fmcsa.dot.gov/CompanySnapshot.aspx>
- As a broker, execute broker/carrier contract.
- As a forwarder, execute forwarder/carrier contract.
- As a surface forwarder, issue house bill of lading with terms and conditions attached.
- Confirm Carrier's motor truck cargo limits are adequate for the value of load being hauled.
- **Consider consulting with a transportation attorney to assist in drafting contractual agreements, vetting carrier business procedures, etc.**
- Consider becoming a Transportation Intermediary Association (TIA) member.

## Insurance Considerations for cargo liabilities/vicarious auto liability exposures:

- Errors and Omissions
- Contingent Auto Liability (for domestic freight forwarders and brokers)
- Contingent Cargo (for brokers)
- Primary Cargo Legal Liability (for domestic forwarders).
- Shippers Interest Cargo insurance.

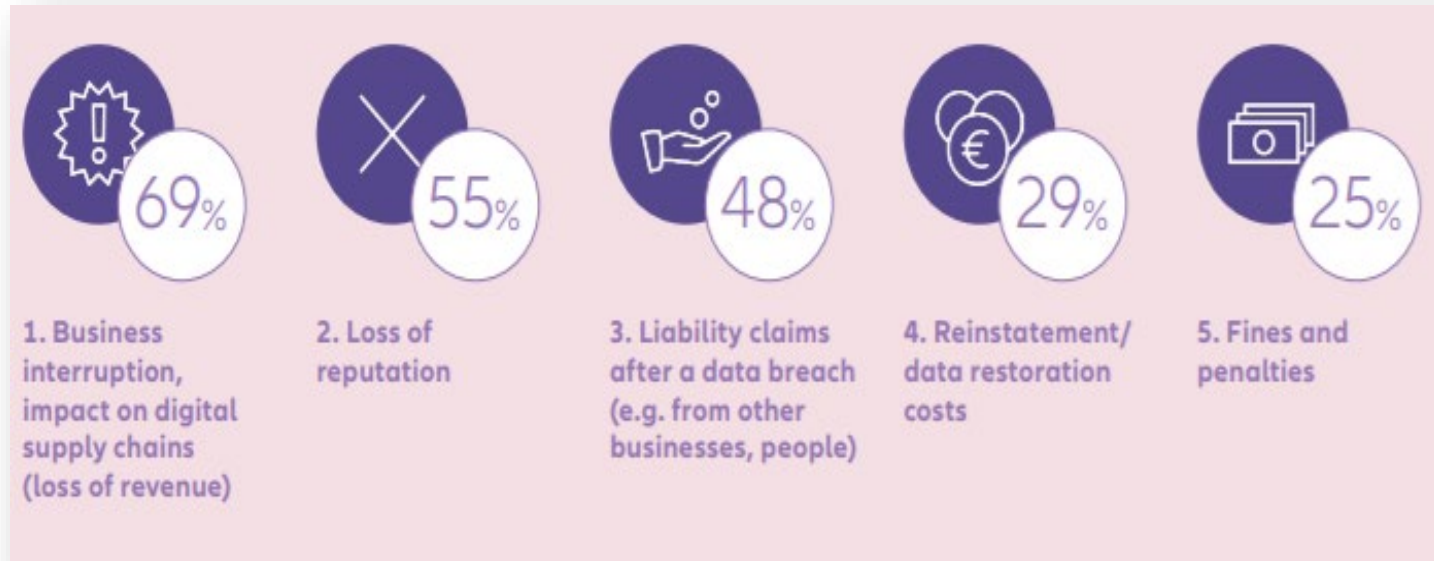
# Cyber



## Top 5 Risks in Marine and Shipping Risks For 2019

Rank		Percent	2018 rank
1	Natural catastrophes (e.g. storm, flood, earthquake)	34%	1 (34%)
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	32%	2 (31%)
3	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation) <b>NEW</b>	28%	-
4	Business interruption (incl. supply chain disruption)	26%	2 (31%)
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration) <b>NEW</b>	24%	-

## Main Causes of Economic Loss after a Cyber Incident



Source: Allianz Risk Barometer 2019



# The Cost of Cyber Risk

- The Ponemon Institute estimates that a single lost or stolen record cost an average of \$148.
- Do the Math:
- A small business with 3,200 customer records at \$148 is \$473,600 in expenses.
- 60% of small businesses fail within 6 months of a cyber attack

# The Cost of Cyber Risk

## State of Oregon notification requirements due to a data breach

Information Covered / Important Definitions	Covered Entities <sup>1</sup> / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
<p><b>Information covered:</b> Personal information of Oregon consumers.</p> <p><u>Definition includes (i) biometric data (i.e. data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial/other transaction, (ii) a consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer, (iii) any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment or (iv) any information or combination of information that a person reasonably knows or would know would permit access to an individual's financial account.</u></p> <p>Any of the data elements standing alone or in combination can be considered personal information if they have not been encrypted, redacted or rendered unusable and the data element taken would enable a person to commit identity theft.</p> <p><b>Important definitions:</b> <i>Security Breach:</i> Means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information.</p>	<p><b>Subject to statute:</b> Any person, legal entity or public body (as defined in ORS 174.019) that owns, licenses, <b>or otherwise possesses</b> personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities.</p> <p><b>Third party recipients:</b> Any covered entity that maintains or otherwise possesses personal information on behalf of, or under license of, another person must notify the other person after discovering a security breach.</p>	<p><b>Written, telephonic or electronic notice must be provided</b> to victims of a security breach <b>no later than 45 days from discovery of the breach</b>, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement).</p> <ul style="list-style-type: none"> <li>• <u>Notice to affected residents is required to contain specific content described in statute.</u></li> <li>• <u>Substitute notice is available</u> by means prescribed in the statute if costs to exceed \$250,000, affected class exceeds 250,000 persons, or covered entity has insufficient contact information.</li> <li>• <u>Notice not required if</u>, after appropriate investigation or consultation with relevant law enforcement authorities, <b>it is determined that no affected consumers are likely to suffer harm</b>. Written documentation of this determination is required and must be retained for 5 years.</li> </ul> <p><b>Other obligations:</b> Any covered entity that must notify more than 1,000 Oregon residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies without delaying notice to affected Oregon residents.</p> <p>Covered entities must develop, implement and maintain <b>administrative, technical and physical</b> safeguards to protect personal information. <b>Note: ORS §654A.22(2)(d) contains expanded information security requirements</b></p>	<p><b>Encryption Safe Harbor:</b> Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unusable by other methods.</p> <p>Safe harbor not available if a security breach involves encrypted data but the encryption key has been compromised.</p> <p><b>Other exemptions:</b> Exemption for good faith and inadvertent acquisition of personal information by a covered entity or a covered entity's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.</p> <p>A covered entity is deemed in compliance with the Oregon statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as protective as Oregon's statute.</p>	<p><b>Attorney General must be notified electronically or by mail if a single breach affects 250 residents.</b></p> <p><b>A determination of no likelihood of harm:</b> Does not require notification to Attorney General.</p> <p><b>Other exemptions, cont'd:</b> A covered entity that complies with other state or federal law that is at least as thorough as Oregon's statute is exempt from Oregon's statute.</p> <p>A covered entity that is subject to GLBA or HIPAA is exempt from Oregon's statute.</p>	<p>Violations are an unlawful practice under ORS 646.607.</p> <p>Penalties can include \$1,000 per violation.</p> <p>In the case of a continuing violation, each day's continuance is a separate violation. Maximum penalty of \$500,000.</p>	<p><b>Private Cause of Action: No.</b></p> <p>Enforcement by the Director of the Department of Consumer and Business Services.</p> <p>If the director has reason to believe that any person has engaged or is engaging in any violation of the Oregon statute, the director may issue a cease and desist order, or require the person to pay compensation to consumers injured by the violation. The director may order compensation to consumers only upon a finding that enforcement of the rights of the consumers by private civil action would be so burdensome or expensive as to be impractical.</p>

Source: Mintz law firm

## Different Types of Cyber Risk

- Data Breach
  - Identity Theft
  - Fraudulent Activities
- Cyber Extortion / Ransomware
- Denial of Service Attacks
- Malicious Code/Virus Transmission

## Top 5 Global Business Risks For 2018

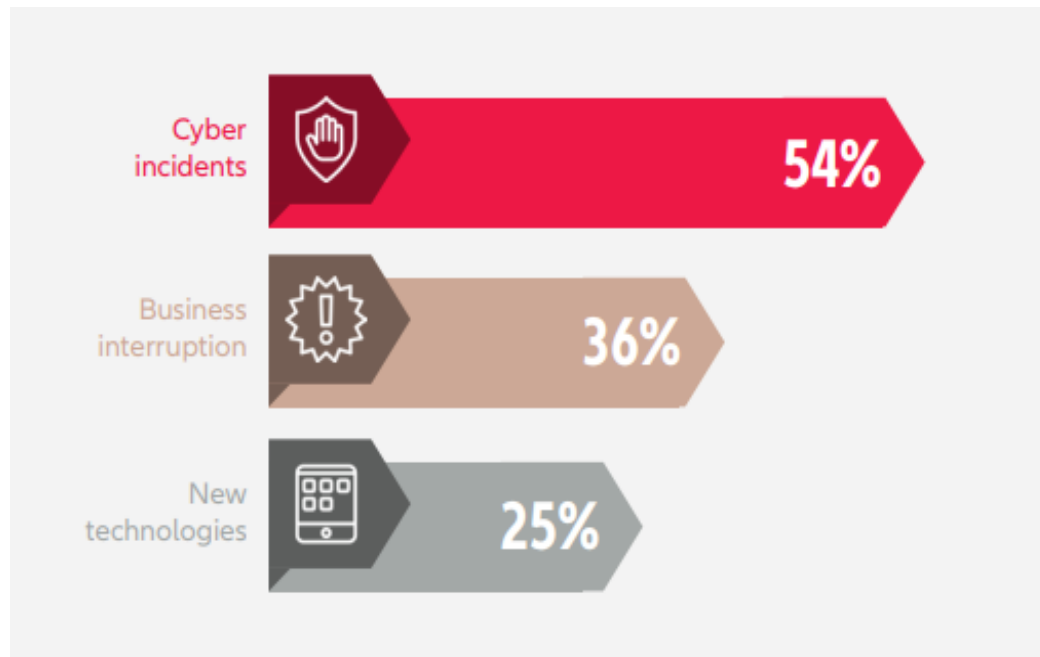
- Business Interruption, Supply Chain Risk – 37%
- Market Developments – 31%
- Cyber Crime, IT Failures, Espionage – 30%
- Natural Catastrophes – 24%
- Changes in Legislation & Regulations – 24%

Source: Allianz Risk Barometer 2018

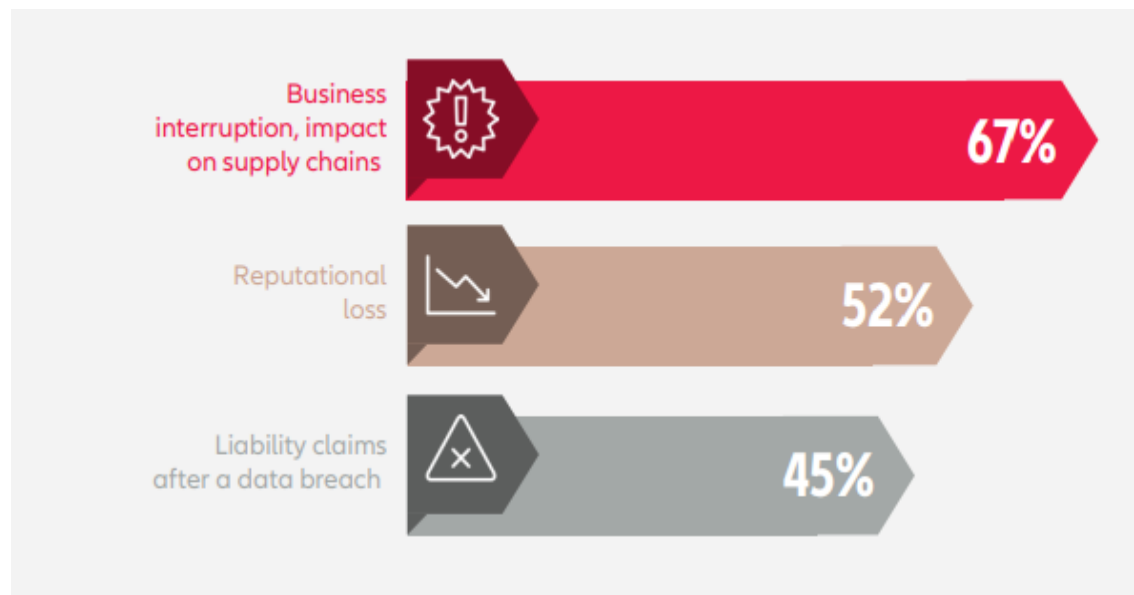
Which causes of business interruption do businesses fear the impact of most?



## Most underestimated business risk



## Main causes of economic loss after a cyber incident





# Cyber Security Risk

- According to the Insurance Journal, cyber risk now costs the global economy **\$445 billion** each year. A 2018 McAfee study puts it at **\$600 Billion**.
- **\$108 billion** of those dollars comes from U.S. company losses.
  - Notables:
    - Target, Anthem, Home Depot and Sony

- **Target Breach** - hackers gained access to their systems through Heating , Ventilation and Air Conditioning vendor (HVAC) during a service call.
  - Est. Accrued Cost to date - **\$252 million**
  - \$100 million of Cyber Insurance.

# The Cost of Cyber Risk

- What are the expenses:
  - Cost of lawsuits from clients or other vendors
  - Cost for Customer notification, Customer support and credit monitoring
  - Cost of restoring, replacing and updating business assets
  - Business Interruption and extra expense
  - Liability for libel, slander, copyright infringement
  - Cyber extortion and Cyber Terrorism
  - Cost for IT forensics
  - Cost for fines and penalties from government agencies

# Who are cyber criminals?



# Cyber Criminals

- According to the FBI, there are four kinds of cyber attackers:
  - **State-sponsored**
  - **Criminals**
  - **Hacktivists**
  - **Insiders.**
- In general, these people steal sensitive information to extort or steal money, interrupt business, or expose private information. All of these possible outcomes can cripple companies large and small alike.

# The Role of Technology



# Cyber Theft Technology

- **Ransomware**
  - Ransom for encrypted data necessary for day-to-day business
- **The Internet of Things**
  - The inherent weakness of wireless devices
- **Phishing/Social Engineering**
  - Now plaguing the corporate world
  - 196 days is the average Dwelling time without detection
- **Cloud Services**
  - Off-site services are at risk

# Cyber theft in the transportation and logistics industries

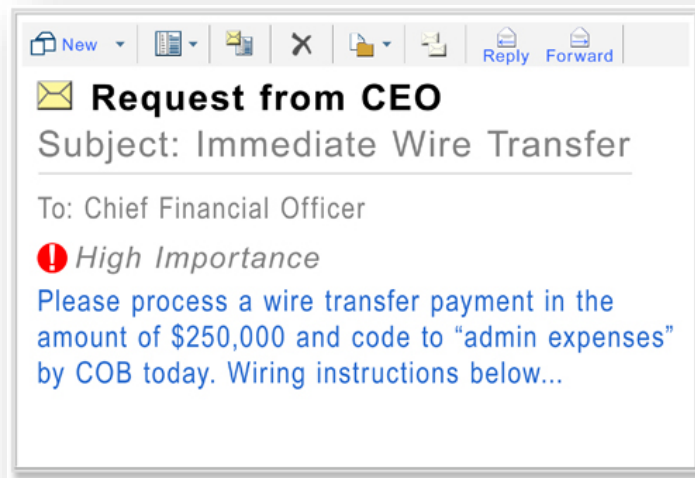




# Industry cyber risks

## Fraud

Phishing scam/Business Email Compromise (BEC) scams. Dwelling



## Identity Theft & Carrier Qualifications

Thieves pretend to represent a legitimate cargo carrier or get in the carriers system.

- Documentation can be forged.
- This can lead to fictitious pickups – they know the commodity and pick up times
- They pick up the load before you get there

## Fictitious Invoices

- Hackers infiltrate your system and send out fictitious invoices with your logos with different wiring instructions or payable instruction
- Your clients payable department misses it
- Your client pays the \$25,000
- THE MONEY IS GONE!!
- This can happen in reverse.... Your overseas agent is hacked.

# Industry Cyber Risks

## Ransom

- An employee's laptop was compromised
- Hackers encrypted all the data
- Demanded \$7,000 in Bitcoin

# Best Practices



# Best Practices

- More than ever companies need to protect themselves against the threat of cyber security. Some suggestions to help safeguard your systems
  - User education
  - Create a cyber security strategy
  - System audits
  - Manage user privileges
  - Install malware and anti-virus software (keep updated)
  - Monitor removable data
  - Control devices and remote access
  - Vet carriers and other third parties
  - Add Cyber Security/Insurance to your contracts

- Vulnerability Scan
  - Have a 3party service try to breach your system (Nessus Cloud software)
  - Report shows summary report of vulnerabilities detected and their perceived severity
  - Provides a brief analysis on the security of your public facing networks.
  - Provides a detailed report to network specialists for review

# The Role of Insurance





**If you are unsure of your cyber security preparedness, ask yourself these questions:**

- What would you do if your customer data was compromised?
- Many states require companies to notify their customers in the event of a security breach. How much would you be forced to pay in notification expenses?
- What if your customers or vendors initiated a lawsuit against you?

# Role of Insurance – Major Areas of Coverage

(Note: Offerings vary widely by Insurer)

- **Liability (Damages to 3rd Parties losses)**
  - Privacy Injury Liability
    - Liability resulting from unauthorized collection, disclosure, use of Protected Information; failure to maintain policies and procedures stating insured's obligations regarding protected information
  - Network Security Liability
    - Liability resulting from causes like: inability of authorized 3rd parties to gain access to insured's network; denial of service; transmission of malicious code from insured's network
  - Privacy Regulation Fines
    - Civil fines/penalties insurable under applicable law and imposed under privacy regulation proceeding for violation of any Security Breach Notice law governing protected information

# Role of Insurance – Major Areas of Coverage

(Note: Offerings vary widely by Insurer)

- **First Party Damages**

- Business Interruption
  - Income that insured would have earned during the period of restoration if not for the network impairment.
- Damage to Insured's System/Network
  - Reasonable expenses that are required to restore the network or information residing on the network to pre-impairment condition.
- Basic E-theft
  - Loss of insured's money/securities/goods resulting from electronic theft committed by a 3rd party.

# Questions?



**For more information, contact:**



**Jaki Ferenz, Vice President**

Office: (206) 784-6376 | Cell: (206) 371-1764

Email: [jferenz@avalonrisk.com](mailto:jferenz@avalonrisk.com)



**Keith E. Sanchez, Divisional Vice President**

Office: 310-337-7050 | Cell: 310-337-7050

Email: [ksanchez@avalonrisk.com](mailto:ksanchez@avalonrisk.com)





Premier Provider of Innovative Insurance and Surety Solutions



THANK YOU!

[WWW.AVALONRISK.COM](http://WWW.AVALONRISK.COM)