CHICAGOLAND RISK FORUM
CHICAGO & MID-ILLINOIS RIMS CHAPTERS

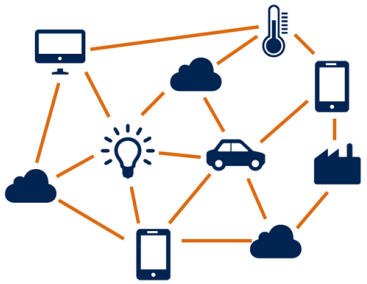
EMPOWERING RISK MANAGEMENT 2018

Emerging Risk Management and Coverage Challenges Presented by the Internet of Things and Vendor Breaches

John D. Hackett & Margaret A. Shipitalo, Cassiday Schade LLP
Kenneth K. Suh, Technology, Media, and Business Services, Beazley Group
Neil Blauvelt, Enterprise Risk Management, United Airlines

What is the Internet of Things (IoT)?

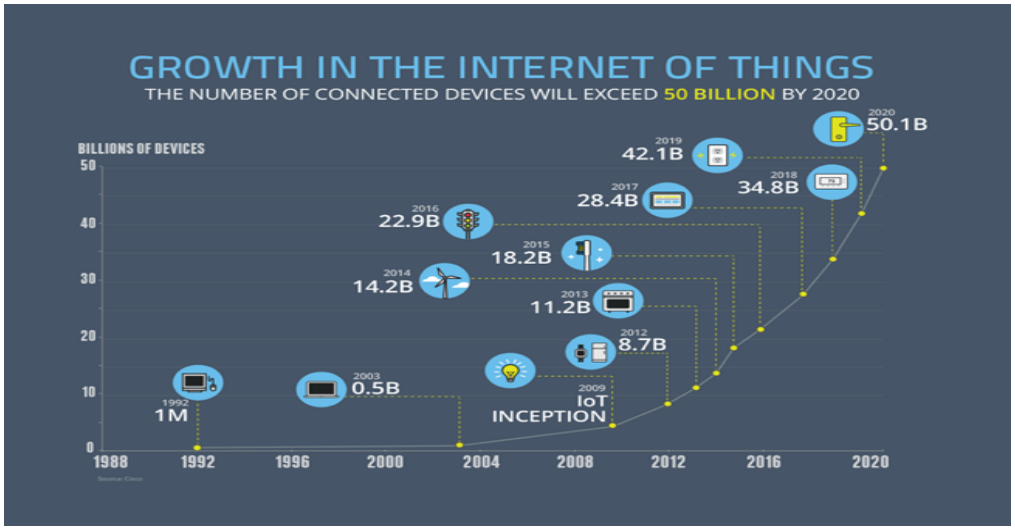
- **Definition** – The concept of connecting any device with an on/off switch to the Internet.
  - "A Simple Explanation of the Internet of Things," *Forbes*, May 13, 2014.
- **Origin** - The term "Internet of Things" was coined as early as 1999 by Kevin Ashton while working at Proctor and Gamble as an assistant brand manager.
  - Shawn DuBravac & Carlo Ratti, "The Internet of Things: Evolution or Revolution" (2015).



IoT Statistics

- In 2003, there were about 500 million devices connected to the internet. Today, there are more than 6.4 billion, with approximately 5 million more connecting to the internet each day.

- 50 billion IoT devices are projected to be utilized by 2020, and consumer IoT products are expected to be the third largest segment of market purchases.



- Global spending on IoT products is forecasted to reach $1.2 trillion by 2020.

IoT Examples

Kuva 1. Internet of Things. Lähde: Huffington Post

- Streetlights
- Security systems
- Factory equipment
- Automobiles
- Fitness trackers and other health monitoring devices
- Home appliances (e.g., smart locks, thermostats, lightbulbs, smart plugs, refrigerators)
- Smart speakers (e.g., Google Assistant, Amazon Echo)
- Even cement!

Affected Industries

- Manufacturing
- Agriculture
- Logistics
- Infrastructure
- Utilities
- Healthcare
- Transportation
- Retail
- Banks
- Food Services
- Hospitality

Entities Affected by IoT

- Manufacturers of IoT devices;
- Businesses that use IoT devices; and
- Businesses that have vendors and suppliers that use IoT devices.

IoT Security Issues

- Billions of IoT devices are constantly acquiring vast amounts of information regarding people and their surroundings.
- They generally have little security features.
- They typically don't run standard operating systems that support commonly-used security tools or just don't have enough memory for them.
- Many also lack the ability to apply firmware updates, making it impossible to patch security vulnerabilities as they come to light.

IoT Security Issues

- Software malfunction resulting in financial loss, property damage, or bodily injury
- Attacks leading to financial loss, property damage, or bodily injury
- Attacks leading to the collection and/or dissemination of sensitive personal data

Security Issues and Recent Events

Notable Hacks Involving IoT:

- Turkish Pipeline (2008)
- FDA Recall of Pacemakers (2017)
- WannaCry (2017)
- British Casino (2018)

Risk Management and Data Breach

Data Breach Costs – 2018 Ponemon Institute Study[1]

Records breached	Direct Cost[2]	Cost per Record
<10,000	$0.7M	$133
10,000 - 25,000	1.0	56
25,000 - 50,000	1.5	43
50,000 - 100,000	2.0	29
1 million	24	24
10 million	95	9
50 million	232	5

1. **Ponemon Institute 2018 Cost of a Data Breach Study: Global Overview, sponsored by IBM Security.**
2. **For breaches <100,000 records, indirect costs, which account for 65% of the total, are excluded. For breaches >1 million, "lost business costs" are excluded.**

Data Protection

Currently, there is no U.S. federal law on data protection and breach response, but…

- 48 U.S. states have their own laws that define notification requirements, etc.
- European Union General Data Protection Regulations (EU GDPR)
  - Became effective 25 May 2018
  - Penalties up to 4% of a company's global revenue

Personally Identifiable Information is a critical risk exposure

Traditional Insurance Policies

- IoT losses can consist of the compromise of data, malfunctions within the physical device itself, or malfunctions of the remote computer programs or algorithms. The results are normally financial losses, bodily injury, or physical damage to tangible property.
- Traditional first-party property policies are often silent on whether they respond to cyber-related damage.
- Since 2014, CGL policies have typically contained an **electronic data exclusion**, or an access or disclosure of confidential personal information exclusion.
- Other common CGL exclusions might also apply.

Traditional Policies

- Gaps in Traditional CGL policies create coverage issues with respect to cyber-related risks.
  - *Capitol Comm'n v. Capitol Ministries*, 2013 WL 5493013, *4 (E.D. N.C. 2013) (electronic data and computer software is not "tangible property" within meaning of a CGL policy).
  - *Zurich American Ins. Co. v. Sony Corp.*, 2014 WL 8382554 (N.Y. Sup. Ct. 2014) (no "publication" of material within meaning of CGL policy's "personal and advertising coverage" when hacker steals insured's data and posts it on the web).

Cyber/Privacy Insurance Coverage

Breach Event Expenses – costs to respond to a data privacy or security incident

- Computer forensics
- Legal expenses
- Public relations costs
- Consumer notification
- Consumer monitoring services (usually for 1 year)
- Post-breach call center
- Expenses for notifying affected banks and credit card companies
- Identity theft monitoring

Cyber/Privacy Insurance Coverage

First Party Losses

- Business Interruption
- Extra Expense
- Digital Asset Protection

Cyber/Privacy Insurance Coverage

First Party Losses (cont.)

- Cyber Crime ***Business Email Loss**
  - Cyber Extortion
  - Computer Fraud
  - Funds Transfer Fraud

Cyber/Privacy Insurance Coverage

Liability Coverage

- Privacy Liability
  - Covers defense costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to the failure of network security.
  - May include unintentional violations of the insured's privacy policy and actions of rogue employees.
- Security Liability
  - Covers defense costs and damages suffered by others resulting from a failure of computer security.
  - Includes liability caused by theft or disclosure of confidential info, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus.

Cyber/Privacy Insurance Coverage

Liability Coverage (cont.)

- Regulatory Proceedings
  - Covers defense costs for proceedings brought by a governmental agency in connection with a failure to protect private info and/or a failure of network security.
- Payment Card Industry Fines and Assessments
  - Covers fines and penalties assessed against the insured (to the extent such fines/penalties are insurable by law) and defense costs incurred in conjunction with a proceeding brought by a credit card company alleging the insured failed to comply with payment card industry data security standards.
  - Claims typically arise in connection with a wrongful act covered under security/privacy liability coverage.

Technology E&O Insurance

- Combines multimedia insurance and professional liability insurance.
- Covers providers of technology services or products for financial loss.
- Applies to errors and omissions and liability assumed by contract.

Cyber/Tech E&O Insurance Developments

- Standard forms yet to be developed.
- Cyber policies typically exclude bodily injury and property damage.
  - But some insurers are now marketing cyber policies that more clearly afford coverage for bodily injury and property damage losses.
- Numerous exclusions that limit coverage.
- Policies are complex and there are few court decisions interpreting them.
- It is therefore critical for a company seeking cyber insurance to not assume protection for all IoT/data breach-related losses, to carefully identify gaps in existing coverage, and proactively work with insurers to obtain coverage for potential risks.

Cyber Case Law – Few Reported Decisions

PF Chang's China Bistro, Inc. v. Fed. Ins. Co., 2016 U.S. Dist. LEXIS 70749 (D. Arizona 2016)

- PF Chang's entered into an agreement with Bank of America Merchant Services ("BAMS") for BAMS to process credit card payments. PF Chang's agreed to reimburse BAMS for fees and penalties imposed on BAMS by credit card issuers.
- BAMS also had an agreement with MasterCard requiring BAMS to pay certain fees and assessments to MasterCard in the event of a data breach.
- Hackers obtained and posted on the internet 60,000 credit cards belonging to PF Chang's customers.
- BAMS was required to pay MasterCard nearly $2 million in fees and other expenses related to the data breach, and sought reimbursement from PF Chang's. PF Chang's reimbursed BAMS and then sought coverage under its CyberSecurity policy through Federal Insurance.

Cyber Case Law – Few Reported Decisions

- ***PF Chang's China Bistro, Inc. v. Fed. Ins. Co.*, 2016 U.S. Dist. LEXIS 70749 (D. Arizona 2016) (cont.)**
  - The court found that the insuring agreement for Privacy Notification Expenses (costs of notifying affected consumers) was implicated. The Privacy Injury insuring agreement was not triggered because the records belonged to the issuing credit card companies and not BAMS.
  - However, the policy contained a **contractual liability exclusion** for losses "assumed by an Insured under any contract or agreement," as well as costs "incurred to perform any obligation assumed by, on behalf of, or with the consent of any Insured."
  - **Result = no coverage.** The court turned to a traditional CGL analysis of the contractual liability exclusion, holding that such an exclusion "appl(ies) to the assumption of another's liability, such as an agreement to indemnify or hold another harmless." The court rejected a "reasonable expectations" argument made by the insured.
  - Note: No PCI assessment carve-back was discussed.

Cyber Case Law – Few Reported Decisions

***Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs.*, 103 F. Supp. 3d 1297 (D. Utah 2015)**

- Travelers issued a CyberFirst Policy to two electronic data storage providers.
- The policy contained a Technology Errors and Omissions Liability Form, which provided that Travelers would pay damages the insureds incurred on account of an "errors and omissions wrongful act."
- A fitness chain owner entered into an asset purchase agreement pursuant to which it would transfer its member account data to the purchasing entity.
- The insureds refused to transfer the data until the owner satisfied several demands for compensation.
- **Result = no coverage.** The insureds' knowing withholding and refusal to return the data was not an error, omission, or negligent act. Traditional analysis.

Coverage Issues

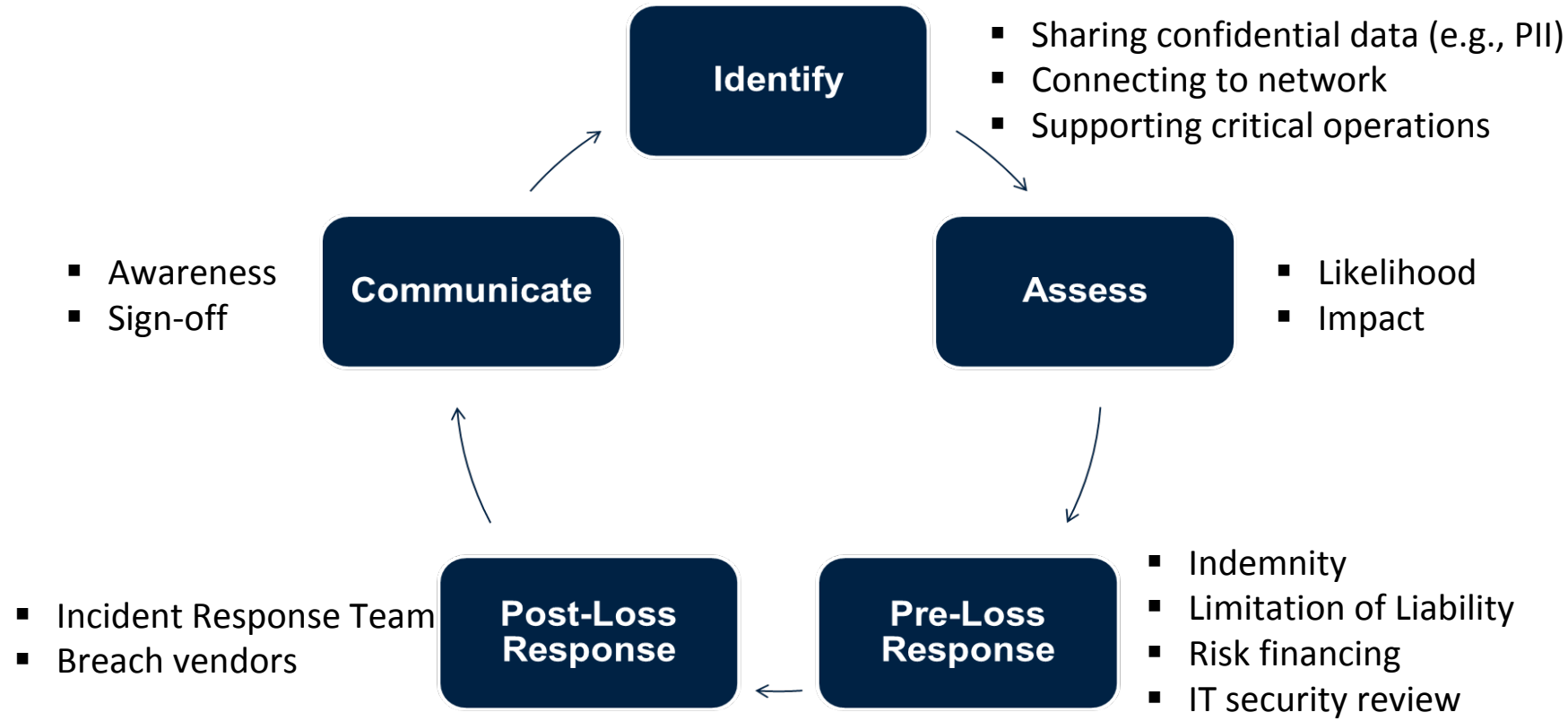
- Is the defendant an insured?
- Fall within insuring agreement(s)?
- Waiting periods?
- Sublimits?
- Compliance with Conditions?

Coverage Issues

- Claim first made prior to retroactive date?
- Prior knowledge not disclosed in application?
- When was claim "first made"?
- Actionable claim or notice of circumstance to trigger policy?

Risk Transfer – Vendor Contracts

Risk Management Process for third party contract IT risk exposures



Risk Transfer – Vendor Contracts

- Risk Transfer Fundamentals
  - When you contract with a vendor, you potentially become liable for their work.
  - Party best able to control the risk should be responsible, *i.e.*, the vendor
    - The proper use of contractual agreements can transfer risk from your business to the responsible party, *i.e.*, the vendor or the vendor's subcontractors doing the work and causing the risk.
  - Two principal ways to transfer risk:
    - Indemnity – vendor agrees to assume the liability of the business (this may be insured by contractual liability coverage).
    - Insurance – vendor includes your business on its cyber/privacy policies as an additional insured.

Risk Mitigation Strategies

Avoid	Are there cost-effective options to: - not outsource? - not share sensitive data? - not provide connection to systems?
Mitigate	Notify IT Security, Legal Data protection standards, encryption Breach response planning
Retain	Who pays? (i.e., approver's cost center)
Transfer	Insurance or non-insurance (contractual transfer)

Risk Transfer – Vendor Contracts

- What to consider when contracting with your vendor:
  - Data at issue
  - Information Security Programs
  - Industry Standards
  - Privacy
  - Subcontractors
  - Termination and Transition
  - Insurance

- Ability to control risk decreases throughout the procurement process

- Risk should be a key consideration early and at every phase of the contracting process

Risk Transfer – Vendor Contracts

- Contractual agreements with outside vendors should:
  - Warrant no known security defects in products
  - Require vendor to provide notice of any subsequently discovered security vulnerabilities or defects
  - Require vendor to timely update, replace and remove vulnerabilities
  - Require vendor to name company as additional insured, covering loss of data policyholder is storing for others and loss caused by a breach of a third party's data as a result of the policyholder's misconduct

Third-party cyber risk assessment template

Background:
- Vendor name and services provided, etc.

Inherent Risk Description:
- How many customer and/or employee records could be impacted and what types of data (credit card numbers, personal health data, social security numbers, passport numbers, passwords, or answers to security questions, etc.)?
- Will supplier be connecting to Company's systems – which ones and how critical are they?
- What is the maximum plausible loss to Company if the supplier's controls fail (describe and / or use table below)?

Risk Assessment:

Inherent Risk Rating			Risk Mitigation	Residual Risk	
	Sensitive PII records	Exposure	**Examples:**		**Examples:**
High	i.e., xxxK+ records	$xxM+	▪ Contractual indemnity, limitation of liability ▪ Vendor's insurance ▪ Company size, balance sheet ▪ Vendor's reputation ▪ Meets or exceeds industry IT security standards ▪ Company's insurance may provide some coverage[1]	High	▪ Vendor meets relevant IT Security standards, but a breach remains plausible ▪ Contractual indemnity covers ~X% of total exposure ▪ Company's residual risk is ~$XM
Med	i.e., xxK-xxxK records	$xxM-xxM		Med	
Low	i.e., <xxK records	$xM		Low	

1. Company carries $xxxM+ of cyber insurance, but this is intended to provide coverage for Company's risks, not vendors'. If Company makes a significant cyber claim, the coverage will likely no longer be available or become cost prohibitive.

Strategy Recommendation:
- Example 1: Recommend seeking lower risk vendors with more favorable indemnity, etc.
- Example 2: Due to importance of vendor capabilities and lack of alternative providers, we recommend proceeding with agreement.

Third-party contractual cyber risk mitigation

1. Assess and negotiate risk early

a. Indemnity section is critical
b. Financial strength / insurance to finance risk

2. Manage the business's expectations

3. Create leverage with multiple vendors

4. If can't get appropriate risk transfer…

a. Consult SMEs
b. Document risk-benefit trade-offs
c. Make sure decision made at appropriate level
d. Document the decision, the reason(s), and who signed off

Procurement is a front line defense to prevent vendors from inappropriately transferring risk to your company

What can we expect in the future?

Questions?

John D. Hackett
Margaret A. Shipitalo
Cassiday Schade LLP

Kenneth K. Suh
Technology, Media, and Business Services
Beazley Group

Neil Blauvelt
Enterprise Risk Management
United Airlines