# ANOTHER DAY AT THE BREACH:

## *Impact of Every Day Cyber Intrusions – Claims and Coverages*

*Presented by:*
**Robert H. Glasser**
**Verne A. Pedro**

MERLIN
LAW GROUP

BRG
Berkeley Research Group

# AGENDA

- What are cyber risks/intrusions
- Carry over between traditional and cyber claims
- Cyber insurance coverage/traditional coverages for cyber claims
- Cyber claim assembly and resolution

# I. WHAT IS CYBER RISK

# Traditional v. Cyber Claims

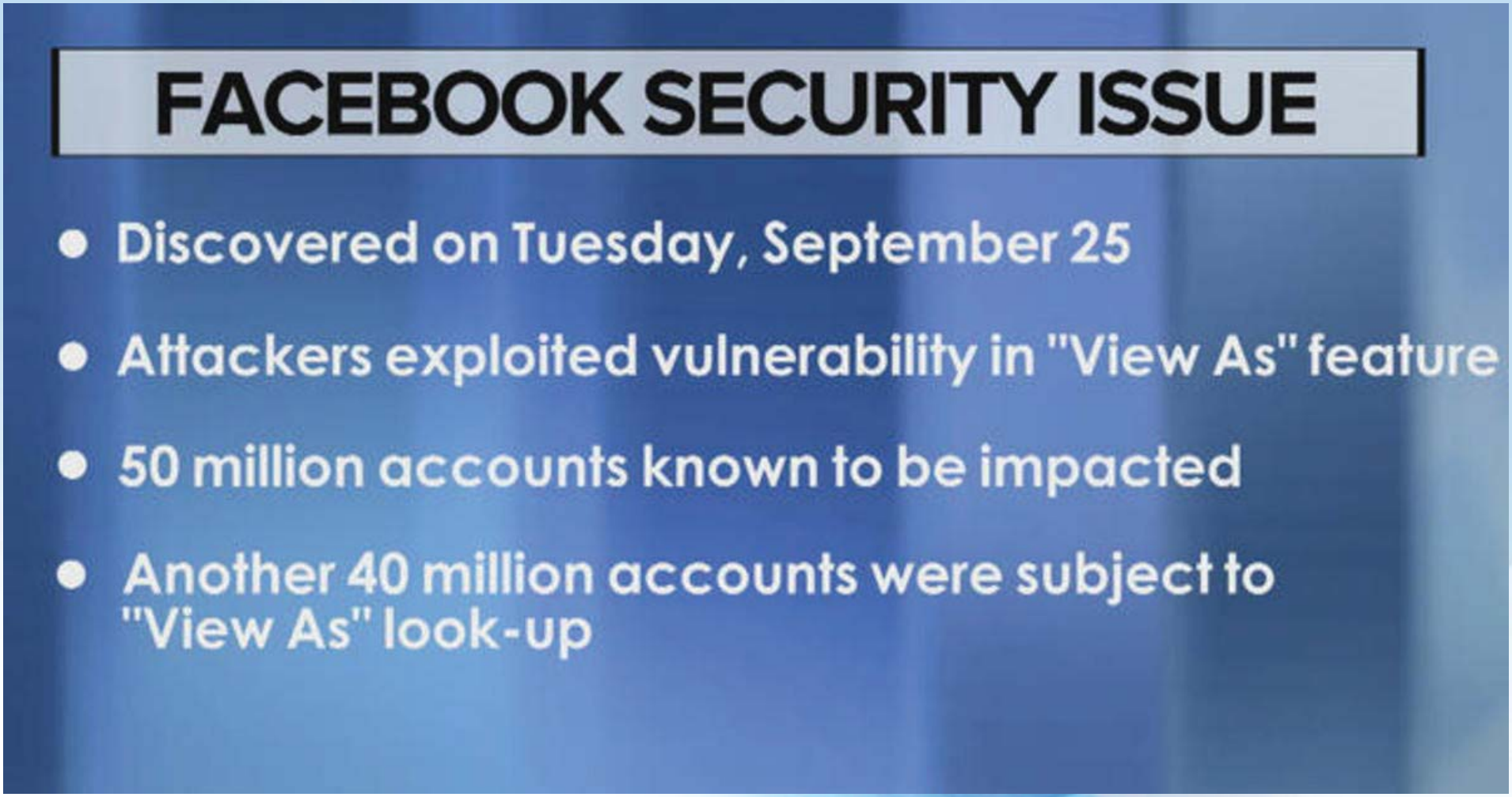
# Overview of Cyber Intrusion

- Cyber risk: Loss associated with the use of electronic devices, computers, IT, and virtual reality.

- 1 of out every 130 e-mails contains malware

- 4,000 ransomware attacks every day.

# So … What is an every day cyber intrusion?



# So … What is an every day cyber intrusion?

- **June 2018** - Washington Post report:

Chinese gov't hacked Navy contractor's computers, stealing massive amounts of highly sensitive data related to undersea warfare, incl. secret plans to develop a supersonic anti-ship missile for use on U.S. submarines by 2020.

# Deliberate Cyber Attacks Transcend Industries

- Utilities
- Manufacturing
- Healthcare
- Technology
- Transportation
- Hospitality
- Financial
- Law firms

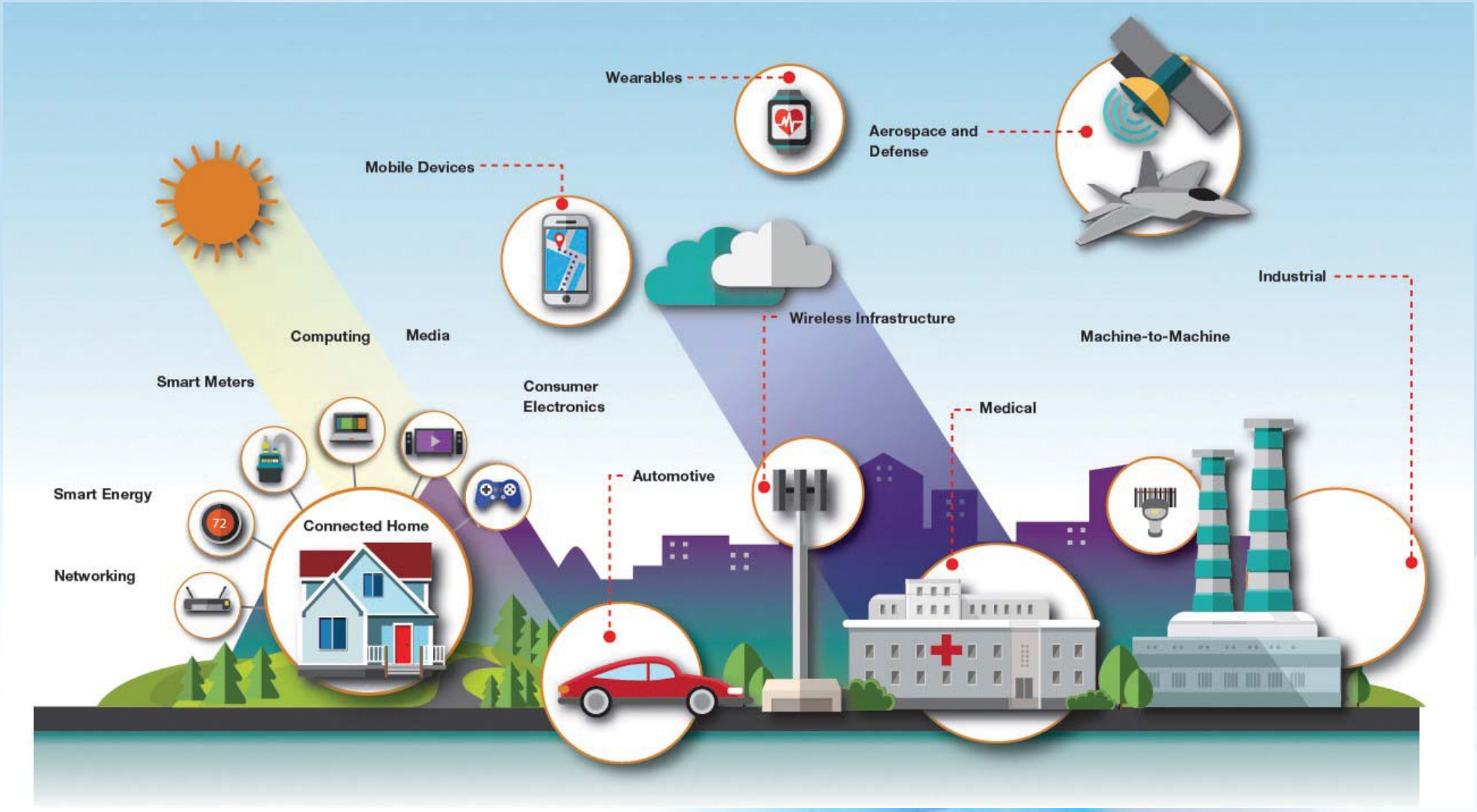
# Who are the Villains …

- Hackers
- Hacktivists
- Cyber terrorists
- Nation-state actors
- Organized criminal groups

# Cyber-Physical Attacks – Internet of Things

- ***"We are already the planet of the machines."*** **-- Keren Elazari, *Security Researcher***
- **The number of devices connected to the internet is 12 billion devices to 7.5 billion people – and within two years the ratio will be four to one.**
- **Cars, kitchen appliances, and heart monitors can all be connected through the IoT, and list of devices is growing every day.**
- **Devices generally built with poor defenses against malicious attacks.**

# Cyber-Physical Attacks – Internet of Things



# Cyber-Physical Attacks – Internet of Things

- September 28, 2018 – Calif. becomes first state with an IoT cyber-security law; security for connected devices.
- SB-327 Starting January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure.
- If it can be accessed outside a local area network with a password, it needs to either come with a unique password for each device, or force users to set their own password the first time they connect. That means no more generic default credentials for a hacker to guess.

# Cyber-Physical Attacks

- Security breach in cyberspace that adversely affects physical space, ex. Internet of Things
- Physical destruction by cyber means and acts of cyber warfare are serious emerging concerns.
- Ex. Dec. 2016, utilities in Ukraine were targeted by malware dubbed “CrashOverride” or “Industroyer”, which is designed to cause physical harm to infrastructure and disable power grids.

# So … What is an “every-day” cyber intrusion?

- **MALWARE –** Compromises system operation by performing unauthorized function or process. Attackers spy & steal private info
- **SOCIAL ENGINEERING –** non-technical manipulation to obtain information
- **PHISHING -** Digital form of social engineering to deceive individuals into providing sensitive information.
- **SPOOFING -** Attacker pretends to be someone else to enter a secure system.

# So … What is an “every-day” cyber intrusion?

- **RANSOMWARE**: Digital extortion; attacker demands on-line ransom to restore access

- **DENIAL OF SERVICE ATTACKS -** BOTS used to overload & temporarily disable websites (Ex. Draft Kings/Fan Duel).

# Defining the Risk

- **JUICE-JACKING:** stealing data or installing malware via a USB connection.
- **TRUST-JACKING:** When plugging a mobile phone or device into a new computer, you will be asked: Do you trust this Computer? Answering yes could expose the device to a remote attack; allows a cyber-attack to continue long after devices are physically disconnected.

# Defining the Risk
# INSIDER/ROGUE EMPLOYEES

- Unauthorized or malicious use of organizational resources.
- Insiders steal data hoping to convert into cash in the future.
- Human Error

# Defining the Risk – case law

- ***Medidata Solutions Inc. v. Federal Ins. Co.***, 1:15-cv-00907 (July 21, 2017, S.D.N.Y. 2017) –coverage found under computer fraud policy for insured spoofed via e-mail into wiring almost $4.8 million to an unknown overseas bank account.

- ***Medidata Solutions Inc. v. Federal Ins. Co.***, 2018 WL 3339245, docket number 17-2492-cv (July 6, 2018) – 2d Cir. affirmed District Court ruling.

# Defining the Risk – case law

- ***American Tooling Center v. Travelers Cas. & Surety,*** No. 5:16-cv-12108 (July 13, 2018) - U.S. Court of Appeals for the Sixth Circuit overturned a lower court ruling that exempted phishing scam losses from coverage under business insurance policy.

# Defining the Risk
# REGULATORY ENFORCEMENT

- NY Dept. of Financial Services cyber security regulation 23 NYCRR 500 (eff. March 1, 2017).
- Applies to all financial services companies in NY State (ex., banks, insurance companies, other financial institutions).
- Requires “covered entities” to establish cybersecurity program with minimum standards & requirements.
- General Data Protection Regulation (GDPR) – enacted 5/25/18 - General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas

# II. COVERAGE FOR EVERY DAY CYBER LOSSES; DOCUMENTING A CYBER CLAIM

# Cyber-Insurance Basics
# WHAT IS COVERED?

- ❑ Cyber incident response
- ❑ Security and privacy liability
- ❑ Network asset protection
- ❑ Multimedia Liability
- ❑ Post-Breach response costs
- ❑ Regulatory defense & penalties
- ❑ Payment Card Industry Data Security Standard (PCI DSS)
- ❑ Coverage for lost profits
- ❑ Cyber extortion
- ❑ Cyber terrorism
- ❑ Ransomware attacks
- ❑ System damage and business interruption
- ❑ Loss adjustment costs

# Cyber Claim Coverage Triggers and Initial Hurdles With a Cyber Loss

- **INCIDENT** - Event that compromises the integrity, confidentiality or availability of data.
- **BREACH** - Incident resulting in confirmed loss and disclosure of data.
- Ability to demonstrate the effect that a cyber incident has had on policyholder's business.
- Demonstrate the impact interruption had in terms of losing customers or profits.
- Steps taken to mitigate losses (quick response after a breach).
- What if there is no damage to so-called "physical" assets?

# Documenting the Claim
# OVERVIEW

- ❑ Notice issues
- ❑ Proof of security measures
- ❑ Policy compliance
- ❑ Regulatory compliance
- ❑ IT systems and steps taken to investigate the breach
- ❑ Identify data loss and physical damage to systems
- ❑ BI/CBI proofs
- ❑ Client/public response and notifications
- ❑ Vendor notifications
- ❑ Law enforcement involvement

# Documenting the claim
# NOTICE

# Documenting the Claim
# BUSINESS INTERRUPTION LANGUAGE

## ❑ First Party Network BI:

Business interruption Loss, in excess of retention, incurred by the Insured during the Period of Restoration as a direct result of the actual and necessary interruption or suspension of Computer Systems that first takes place during the Policy Period and is directly caused by a failure of Computer Security to prevent a Security Breach; provided that such Security Breach must first take place on or before the Retroactive Date and before the end of the Policy Period.


## ❑ Waiting Period:

Multiple Security Breaches resulting from a Failure of Computer Security shall be deemed to be a single BI Loss; provided, however, that a separate Waiting Period shall be applied to each Period of Restoration.

# Documenting the Claim
# BI LANGUAGE (cont.)

- **Income Loss** will be calculated on an hourly basis based on the Insured Organization's net profit (or loss) and fixed operating expenses.

- **Period of Restoration** begins on the specific date and time that the actual interruption first occurred; and ends on the specific date and time that the actual interruption of Computer Systems ends or would have ended had the Insured acted with due diligence and dispatch.

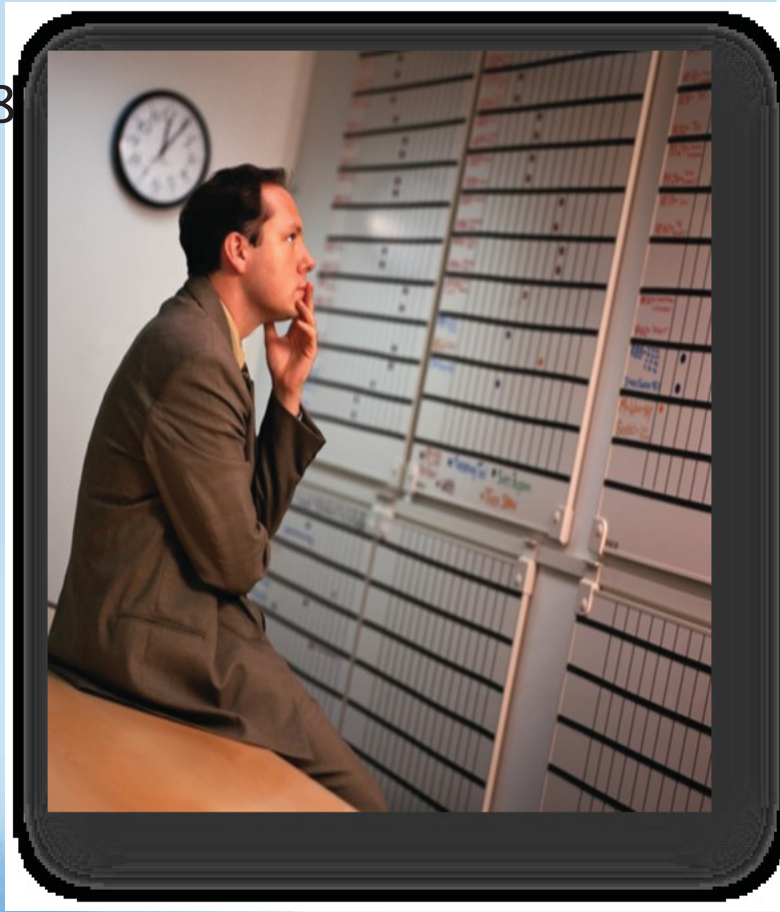
# Documenting the Claim
# BI LANGUAGE (cont.)

Most **Underwriters will pay for**: covered Income Loss per hour in the amount set forth in Item 2.A.6.(3) of the Declarations for Insuring Agreement I.I as the "Hourly Sublimit".

…with respect to covered Income Loss, the Retention shall be the greater of: (a) amount of any payments within the Retention for covered Loss under Insuring Agreement I.I. made in occurrence with Clause VII, or (b) the amount of Income Loss during the Waiting Period.

# Documenting the Claim
# CLAIM QUANTIFICATION COMPLEXITIES

1) Profits per hour
2) Hours of operation (internet 24 hours/stores 8 hours per day)
3) Deductible or waiting period by hour
4) Mitigation with store sales
5) Saved vs. continuing costs issues (margin issues)
6) Fill internet orders from physical store stock
7) Loss vs. deferral of internet sales
8) Reliability of historical data and trends
9) Time Zones



# Bridging the Gap Between Cyber and Traditional Insurance

- ❑ Directors and Officers
- ❑ Errors and Omissions
- ❑ Property
- ❑ Crime / Theft
- ❑ Commercial General Liability

# Nailing Down Responsive Cyber Coverage
# POTENTIAL CONCERNS

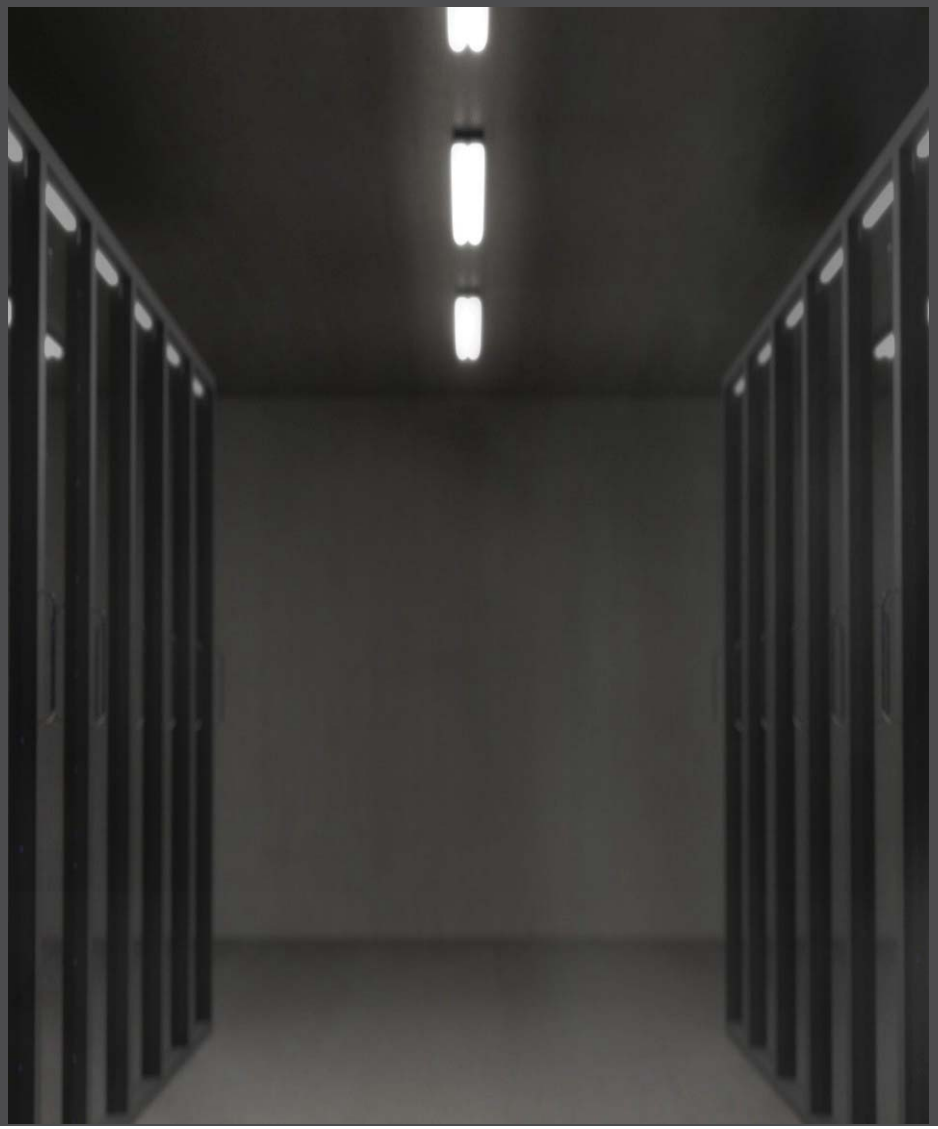
- Wild west: standardized language is still being developed so policies can vary greatly in what they expressly cover.
- WHAT ARE COVERAGE TRIGGERS, reimbursement vs. indemnification language
- Watch out for sub-limits on important lines of protection.
- Are property damage and bodily injury losses covered?
- Validate that coverage described on the Declaration page is reflected in the body of the policy.
- Understand exclusions that are narrow in scope; they are not supposed to remove what you have negotiated for, nor make coverage illusory.
- Verify that a cyber event did not take place before the policy issue or retro date or there might be a coverage fight.

# Nailing Down Responsive Cyber Coverage

- ❑ Ascertain unique cyber risks
- ❑ Insurance applications
- ❑ Retro dates
- ❑ Look for a clear policy structure: Modules and key coverage grants
- ❑ Symmetry with other insurance (*e.g.*, CGL and property insurance)
- ❑ Endorsements for special coverage needs when it comes to cloud providers and third-party vendors
- ❑ If you accept payment cards, PCI Issues and Card Brand fines and penalties
- ❑ Beware breach of contract exclusions (PCI coverage implications)
- ❑ Beware unencrypted mobile devices exclusion
- ❑ Beware conditions on "reasonable“ cyber security measures
- ❑ BI and “Reputation Damage” insurance—may be vague but becoming more relevant
- ❑ Policy may contain separate insuring clauses for each type of coverage

# Documenting the claim → RECAP

- ❑ Every “cyber” policy form is unique and requires careful review. (different insuring agreements, etc.)
- ❑ Coverage gaps/Consider other potential policies
- ❑ Pay attention to notice provisions & requirements
- ❑ Key concepts in cyber insurance coverage are evolving



# Q&A

# *Thank you!*

**For more info, visit our Websites:**

**MerlinLawGroup.com**
**PropertyInsuranceCoverageLaw.com**
**CondominiumInsuranceLaw.com**

**Robert Glasser, CPA, CFE, CIRA, CFF**
Managing Director, Berkeley Research Group
810 Seventh Avenue, Suite 600
New York, NY 10019
**rglasser@thinkbrg.com**
516-998-6310