UNDERSTANDING CYBER-RISK INSURANCE, THE MARKET, THE GAPS AND THE FINE PRINT

Webinar – September 25, 2018

McCARTER &ENGLISH
ATTORNEYS AT LAW

EPIC

NACD
NEW JERSEY CHAPTER

What Is Cybersecurity?

- The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation
- You need to understand the rules and regulations

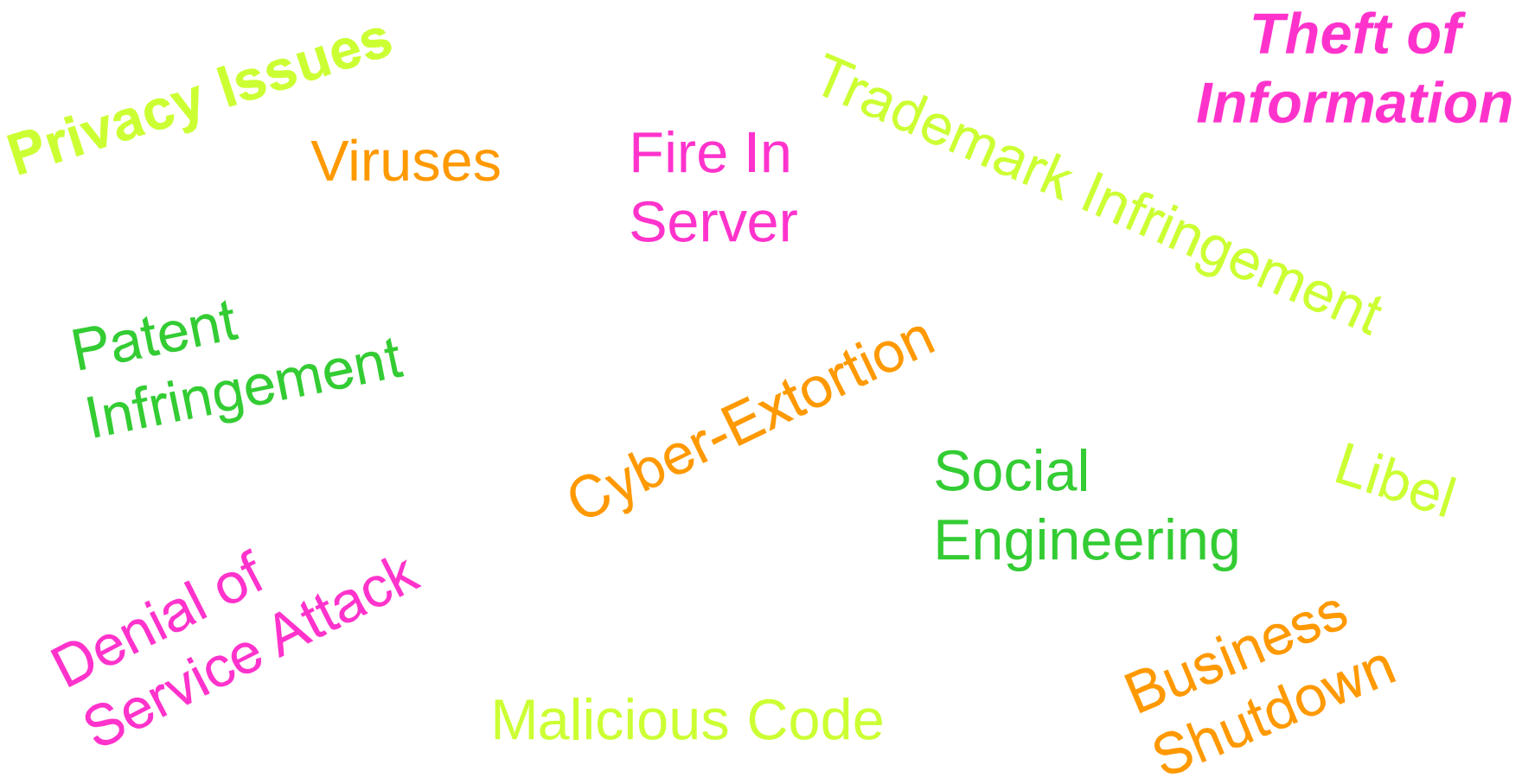
Understanding The Threat

- Types of Targets
  - Databases
  - File Servers
  - Mobile Devices
- The “Vectors”
  - Collaborative Tools
  - File Sharing Applications
  - Finance & Accounting Software/Applications
  - Emails
- The Spoils
  - Customer Data
  - Intellectual Property
  - Financial Data
  - Money

Potential Impacts of a Breach or Computer System Failure

- Data Leak/Breach
  - Customer Data (Personal and Commercial)
  - Identity Theft
  - Intellectual Property Loss
- Financial loss
  - Fraud
  - Ransomware
- Brand Damage/ Embarrassment
- Liability Risk
- Business Interruption
- Regulatory Action

Undifferentiated Cyber Risks



McCARTER &ENGLISH ATTORNEYS AT LAW EPIC NACD NEW JERSEY CHAPTER

Cyber Breach Costs

- The average total breach cost was $394K, the median $56K.
- Retail exposed 67% (420M) of the number of records in the total dataset.
- The largest Regulatory claim was upwards of $6M.
- Cyber Event Recovery expense was reported as high as $475K.
- The median cost of Third-Party breaches was comparable to in-house events, but exposed twice as many records.
- Wire Transfer Fraud & Theft of Money averaged $179K in breach cost.
- Ransomware/Cyber Extortion affected every sector with maximum breach costs in excess of $500K.
- Companies with revenues greater than $2B suffered an average breach cost of $3.2M.
- Companies with less than $50M in revenue were the most impacted, accounting for 47% of the claims.

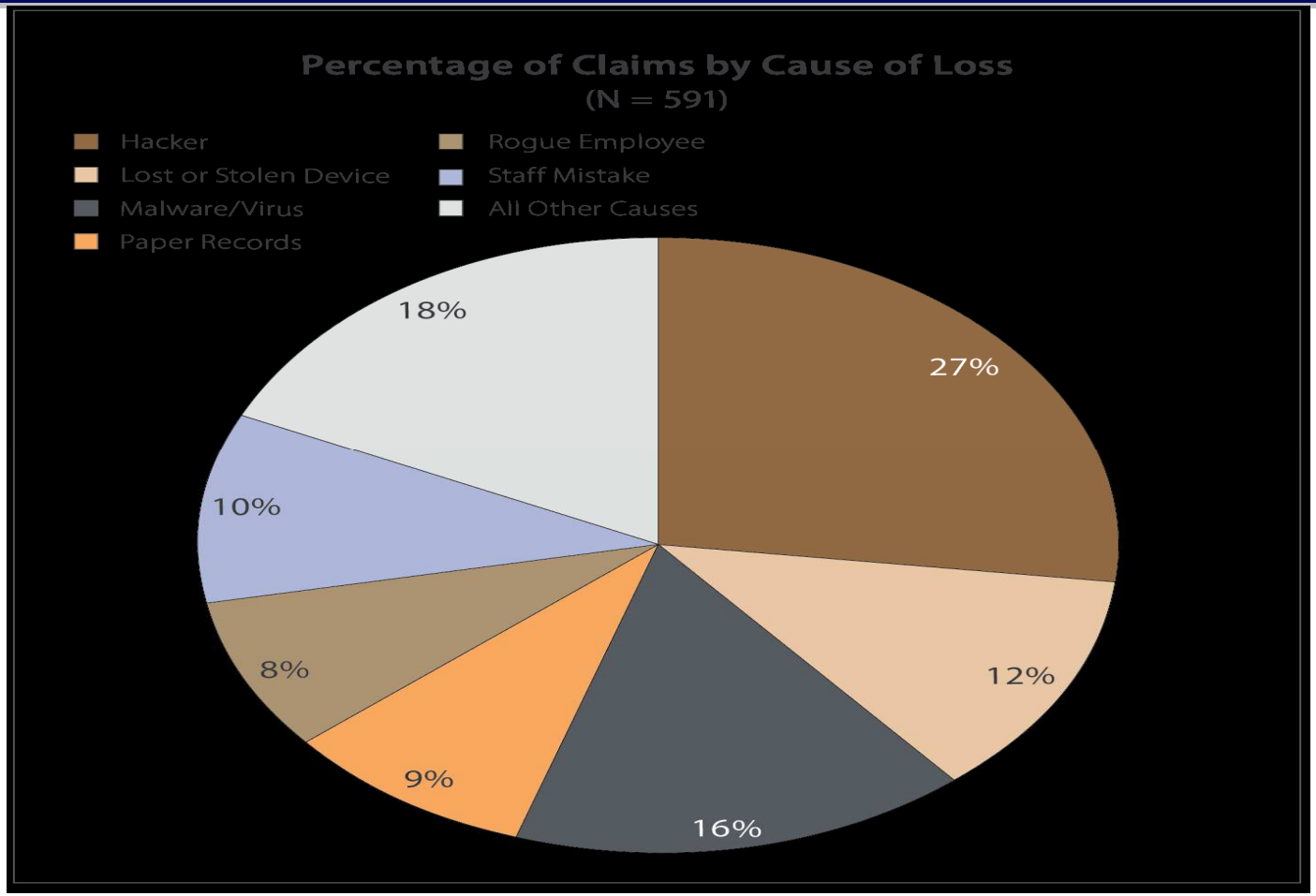
NetDiligence® 2017 CyberClaims Study Ver. 1.3

Cyber Breach Costs

- Breach costs were 20% higher when there was Cloud involvement.
- Trademark Infringement and/or the Loss of Trade Secrets averaged $865K, with a median of $182K and a maximum of $4.9M.
- PCI data was exposed in 16% of claims but accounted for 67% of records. PHI data represented 15% of claims and 17% of exposed records, while PII data accounted for 36% of claims but only 16% of exposed records. PCI, PHI and PII data accounted for 99% of all records exposed.
- The median payout ($64,324) for PCI Fines was similar to last year. The average of these fines was $389K. The maximum PCI fine paid was $3M.
- Maximum Notification cost, when compared to last year, increased 176% to $5.52M; average Notification cost was 39% higher.
- Hackers were identified as the most common Cause of Loss, followed by Malware/Virus, Ransomware/Cyber Extortion and Staff Mistake.

NetDiligence® 2017 CyberClaims Study Ver. 1.3

Claims By Cause of Loss



The Sony Pictures Hack – The Facts

- On November 24, 2014 – the Monday before Thanksgiving – Sony learned that it had been hacked when the following appeared on the computer screens of many Sony employees:

Primary Lessons Learned

- **Recognize and Protect Sensitive Information** – if the information is confidential and/or proprietary, treat it as such by ensuring that the files containing such data are encrypted and/or password-protected
- **Use and Maintain Antivirus Software** – think of antivirus software as a security fence that protects your company's data
  - If the perimeter is breached, serious problems may arise
  - Check for updates on a daily basis
  - When updates are identified, push them automatically to every user who has access to your company's internal systems
- **Conduct Periodic Penetration Testing** – at least every two weeks, have your system infrastructure tested to ensure its integrity

Primary Lessons Learned From LinkedIn® Breach

- **Take Password Security Seriously** – LinkedIn did not adequately protect the passwords of its users because it failed to use a "salt" (*i.e.*, random data inserted to scramble a password when encrypting it) for the passwords

- **Implement Policies Prohibiting The Cross-Pollination of Passwords** – Many LinkedIn users connected their LinkedIn accounts to other social media sites like Facebook or Twitter, such that access to one site meant access to all sites
  - This was problematic for the LinkedIn users that were hacked, and for the friends/followers of those users

Primary Lessons Learned (cont'd)

- **Implement A Breach Response Plan That Makes Sense** – LinkedIn implemented a "mandatory password reset" for the 6.5 million accounts they believed were compromised, but they did nothing for the other 400 million-plus users
  - If your company has been hacked, act as if no passwords are secure

“Insider Threat”

- A security threat (either intentional/malicious or unintentional) that originates from within the organization
  - Accomplished through abusing access rights, theft of materials, and/or the mishandling of physical devices/facilities
- Many lack procedures or controls to prevent/detect/deter insider attacks
- Threat hierarchy:
  - Privileged users with access to sensitive information
  - Contractors and consultants
  - Regular employees

"Insider Threat"

- "Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)."

"Roughly 80 percent of incidents in the cyber domain can be traced to three factors: poor user practices, poor network and data management practices, and poor implementation of network architecture."

Memorandum, Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I), September 30, 2015

Best Practices

- Goal should be security
- Know your business and your employees
- Baseline your systems' "normal" to spot "abnormal"
- Understand and moderate your data collection needs
- Wall it off: Insist on limited access to PCI, PHI and PII data
- Back it up: make sure data is securely backed up and available when/if needed
- Encrypt sensitive data

Best Practices

- Put Written Policies and Procedures in Place
  - Strong Passwords/Encryption Data Requirements
  - Controlling Access
  - Data Breach Protocol
  - Written Information Security Plan
- Provide Regular Employee Training Re Computer Security Best Practices
  - Avoid opening attachments to emails that look suspicious
  - Do not open executable files
  - Shut down computer at day's end
  - Change passwords regularly

Best Practices

- Use of Third Party Vendors
  - Due diligence on computer security capabilities
  - Due diligence on market cap/financial resources
  - Negotiate contractual indemnification provisions
  - Negotiate insurance requirements
  - Manage data access
- Best Practices will enhance ability to secure Cyber Risk Insurance on favorable terms, conditions and price.

And…

Insurance Coverage

Insurance Options

- Commercial General Liability Coverage
- Errors & Omissions Coverage
- Crime Policies
- Cyber Risk Insurance Policies
- Additional Insured coverage under a vendors' Technology Errors & Omissions policy
- First Party Property Insurance

CGL Coverage

- Coverage analyzed under "Coverage B" for personal and advertising injuries.
  - Definition of "personal and advertising injuries" will generally dictate whether there is coverage for a data breach.

    "Oral or written publication, in any manner, of material that violates a person's right of privacy."
  - Will have to consider policy's definition of "publication."
    - Does it require <u>publication</u> to a third party such that theft of the information is not a publication?

CGL Policy Exclusions

- This policy does not apply to:

  Electronic Data

  Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

  As used in this exclusion, electonic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

  ISO Form No. CG 00 01 12 04

Crime Policies May Also Be Necessary

- Considerations of coverage triggers
  - Computer Fraud?
  - Funds Transfer?
  - Social Engineering?

Crime Policies May Also Be Necessary

- As a general rule, crime policies cover direct loss of an insured's funds, whether through employee dishonesty or social engineering.

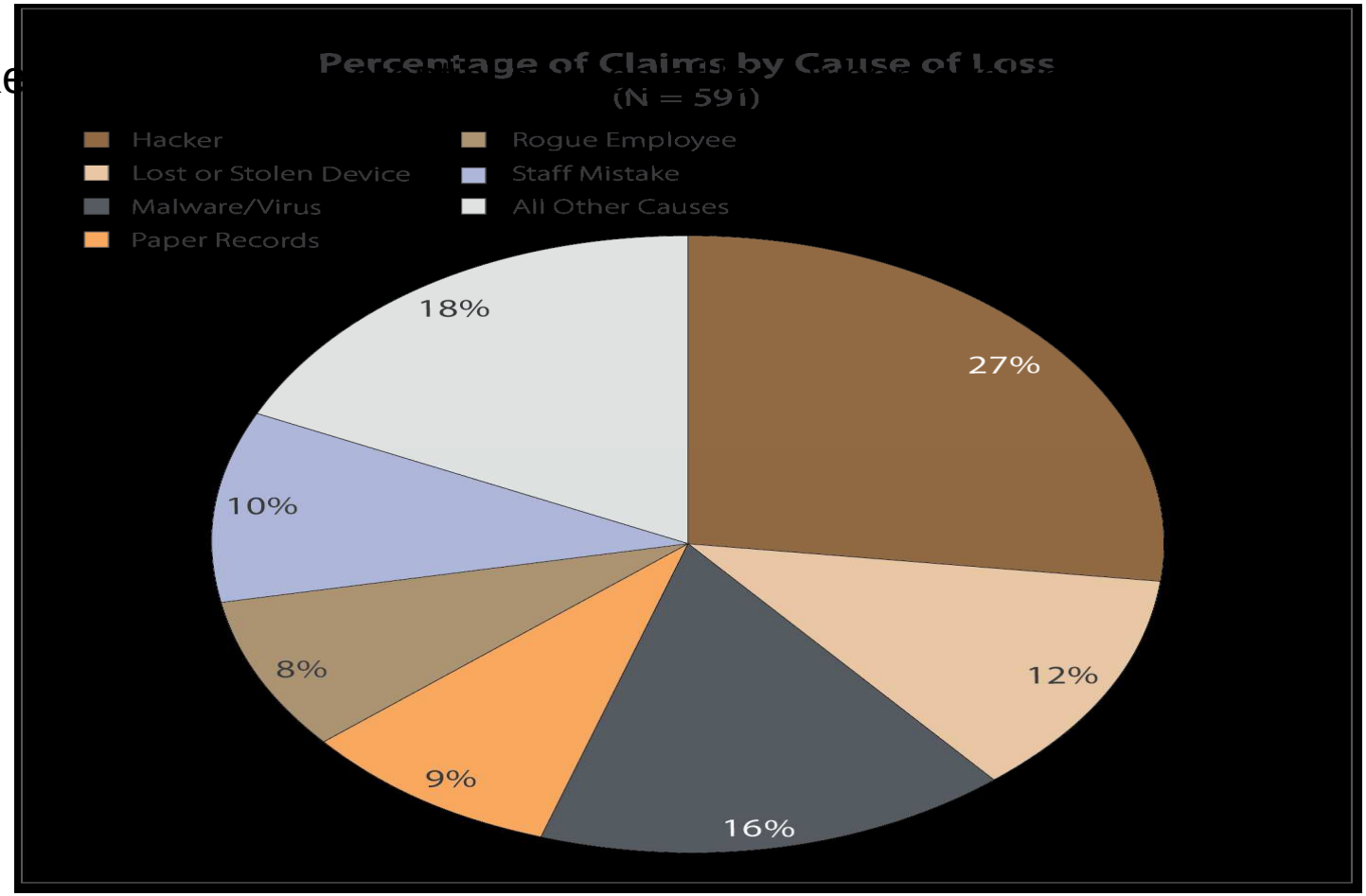
- Cyber policies cover economic damages arising through a failure of network security or privacy controls which may cause indirect losses.

Crime Policies May Also Be Necessary

- Claim example under a crime policy: Unknown party impersonates the insured's bank, contacts the insured's accountant, and convinces the accountant to activate a computer link back to the fraudulent bank. This then allows the impersonator to contact the insured's real bank, pretend to be the insured, and have wire transfers issued that ultimately ended up with a Chinese bank resulting in loss of $500,000.
- Claim could also result from an impersonator hacking into a third-party's email system to get information regarding an upcoming transaction, taking that information, spoofing the third-party's email address, and emailing fraudulent wire instructions which are acted upon by the insured.

Claims By Cause of Loss

Ke



Cyber Insurance 101: What may be covered?

- First-Party Coverage
  - Privacy breach response/notification expenses
  - Data Forensic Expenses
  - Computer funds transfer fraud
  - Business interruption
  - Cyber incident preparation and response
  - Computer disruption
  - Physical damage arising from computer disruption
  - Cyber/Network extortion
  - Network Asset Damage
  - Crisis Event Management

Cyber Insurance 101: What may be covered?

- Third-Party Coverage:
  - Media Liability/Website Media Content
    - Internet-related Defamation
    - Intellectual Property Violation
  - Information, Security and Privacy Liability
    - Theft, loss, unauthorized disclosure of PII
    - Theft, loss, unauthorized disclosure of confidential business information
    - Alterations, corruption, destruction, deletion or damage to data
  - Regulatory investigation and proceeding coverage

Cyber Insurance 101: What may be excluded?

- Traditional Exclusions
  - Contractual Liability
  - Certain Types of Conduct
  - War / Insurrection
  - Potentially, a prior acts exclusion
- Exclusions where Coverage Afforded by Other Lines
  - Bodily Injury and Property Damage
  - Employment-related claims
  - Patent, Copyright Infringement
- Cyber-specific Exclusions
  - Potentially, a failure to follow minimum required security practices

Broker's Role in Cyber Liability

- Advising on evolving risk, which is ever-changing
- Understanding the financial and reputational impact of a breach
- Managing detailed claims and underwriting history
- Having the best access points to insurers writing this type of risk

Cyber Policy Strategy

- Although market conditions continue to improve, a program is more easily built if the applicant can demonstrate by a Best-in-Class Information Security program and a Company-wide Commitment to Managing Cyber Risk.
- Some streamlined application processes, other applicants require greater underwriting scrutiny
- What are the premiums? the deductibles? The sublimits? The exclusions?
- Definitions - ensure broad definition of computer system to include a third party computer system/vendor

Scenario #1

- Employee inadvertently downloads destructive computer virus which spreads to other files on computer network.
  - Resulting in loss of data and shutdown of Company's computer network.
  - PII confidentiality of customers and clients compromised
  - Notification and credit monitoring required
  - Regulators begin investigation against the company
  - Coverage?

Scenario #2

- Ransomware event
  - Employee clicks on link contained in an email that downloads malware onto the company's server. The malware proceeds to encrypt all stored information. An email is then sent to the Employee demanding a ransom payment to unencrypt the information, to be paid in crypto currency.
  - Covered?

Scenario #3

- Internet Disparagement
  - Internal email making negative comments regarding a 3rd party vendor circulated within a company and eventually migrates outside the company, where the 3rd party vendor discovered the negative remarks. Vendor brings a disparagement suit against the company and employee alleging damages to reputation, disparagement, etc.
  - Covered?

When The Breach Occurs…

- Gather details of the incident immediately
- Determine what insurance policies are available, then look closely at insuring agreements, limits and retentions that will apply
- Determine what triggers a loss or claim under the policy
- What are the notice requirements in the policy (notice immediately, notice as soon as practicable, etc.)
- Timing around an upcoming policy renewal/expiring policy period that requires some type of expedited notice

The Take-Away

- Understand your risks and determine what coverage you need
- Carefully review the cyber policy:
  - All coverage grants
  - All definitions (*may narrowly define terms*)
  - All exclusions
  - All conditions
- Evaluate your whole program of insurance

Contact Us

Vincent G. Caracciolo
Managing Director of Claims and Coverage Advocacy
EPIC Insurance Brokers
646-452-4037 office
Vin.Caracciolo@epicbrokers.com

Louis A. Chiafullo, Esq.
Acres Land Title Agency, Inc.
55 Essex Street
Millburn, NJ 07041
973-376-4643 Ext. 185
973-315-9652 (Direct)
lchiafullo@acrestitle.com

Steven Weisman | Partner | Insurance Coverage and Cybersecurity & Data Privacy
McCarter & English, LLP
100 Mulberry Street, Four Gateway Center, Newark, NJ 07102
T: 973-848-5332
C: 862-371-3659
F: 973-297-3744
sweisman@mccarter.com | www.mccarter.com