ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

ACC NCR Fall Conference – Advanced Topics for the In-House Attorney

Cyberinsurance: How I Learned to Stop Worrying and Love the Policy

September 29, 2021

BARNES & THORNBURG LLP

BARNES & THORNBURG LLP

Scott N. Godes

Partner Insurance Recovery, Co-Chair Data Security & Privacy
Barnes & Thornburg LLP | Washington, DC | (202) 408-6928 | sgodes@btlaw.com

Described as the "most interesting insurance lawyer in the world," **Scott Godes** is a Chambers-rated insurance recovery attorney who has assisted clients recover more than $1 billion in insurance coverage. He is a co-chair of his firm's insurance recovery and counseling practice. Scott focused his insurance recovery work on coverage for cybersecurity and privacy claims in 2008 and is one of the few lawyers in the country who has litigated the scope of insurance coverage available for data breach claims under cyberinsurance policies. He also has helped clients recover millions for data privacy incidents and cyberattacks under cyber, crime, CGL, first party property, and Tech E&O insurance policies, as well as in connection with professional liability claims. He has provided strategic coverage advice for companies that have had cloud-based privacy and cybersecurity events.

Scott served as co-chair of the Cyber Risk & Data Privacy Subcommittee of the American Bar Association Section of Litigation Insurance Coverage Litigation Committee for several years. He has also been a co-chair of the American Bar Association's Computer Technology Subcommittee of the Insurance Coverage Litigation Committee. He frequently is quoted in industry publications regarding insurance for cybersecurity and privacy risks. You can follow him on Twitter @scottgodes.

BARNES & THORNBURG LLP

Imani Barnes

Imani Barnes, Senior Analyst, Cyber Technology Practice, Lockton Companies
Lockton Companies| New York, NY| (646) 572-7300| ibarnes@lockton.com

Imani Barnes is a Senior Analyst in Lockton's Cyber Technology Practice for the Northeast. In this role, she is responsible for engaging with insurance carriers for program design, negotiation, and renewal placement for cyber and professional liability coverage. Imani also services clients in identifying and quantifying their cyber and professional liability exposures. Imani has a Master of Business Administration in Enterprise Risk Management from St. John's University and brings her years of experience in property management to Lockton. Her primary industry area focus is Real Estate and Construction.

Imani has been a principal presenter in the 'Managing Risk Through Turbulent Times' webinar for the NY Bar Association and the 'Cybersecurity Risk Management for Construction Projects' webinar for construction leaders. Her ransomware whitepaper (May 2019) can be viewed on the Lockton website.

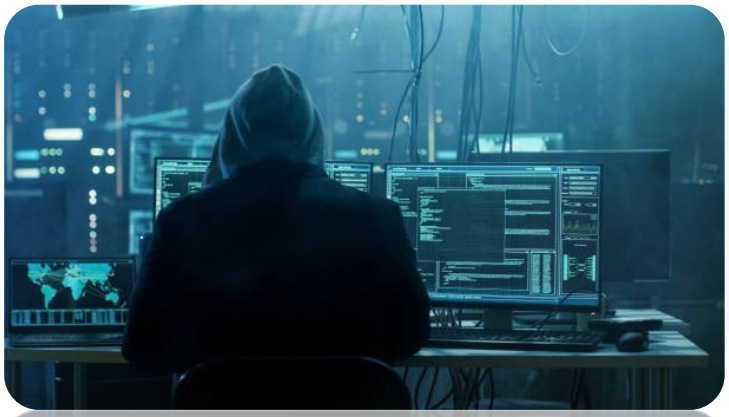
BARNES & THORNBURG LLP

Michael Catina

Assistant Vice President & Assistant General Counsel at Zurich North America
Zurich North America | Schaumburg, IL| (800) 382-2150 | michael.catina@zurichna.com

Michael Catina is Assistant General Counsel within the Corporate Law Department of Zurich North America providing legal and regulatory counsel to various business units throughout the country. In this role he advises business clients on the implications of internal and external business decisions as well as company-wide initiatives. Mr. Catina's areas of expertise include cyber and data privacy risks, New York free trade zone issues, surplus lines issues and insurance product drafting and review. Mr. Catina is a graduate of the St. John's University School of Law and has over fifteen years experience in the insurance industry. Prior to joining Zurich North America Mr. Catina was a senior associate for a large international law firm as well as Assistant Division Counsel within the Corporate Law Department for AIG. Mr. Catina is currently a member of the Board of Directors for both the Insurance Federation of New York and the Insurance Regulatory Forum of Greater New York.

Business Email Compromises - Scenario



- "Don Hinds Ford agreed to purchase twenty Ford Explorers from Beau Townsend Ford for about $736,225. When it came time to close the deal, Beau Townsend's commercial sales manager asked, via email, that Don Hinds pay via wire transfer to an out-of-state bank. Don Hinds agreed, wired the money, and picked up the Explorers.

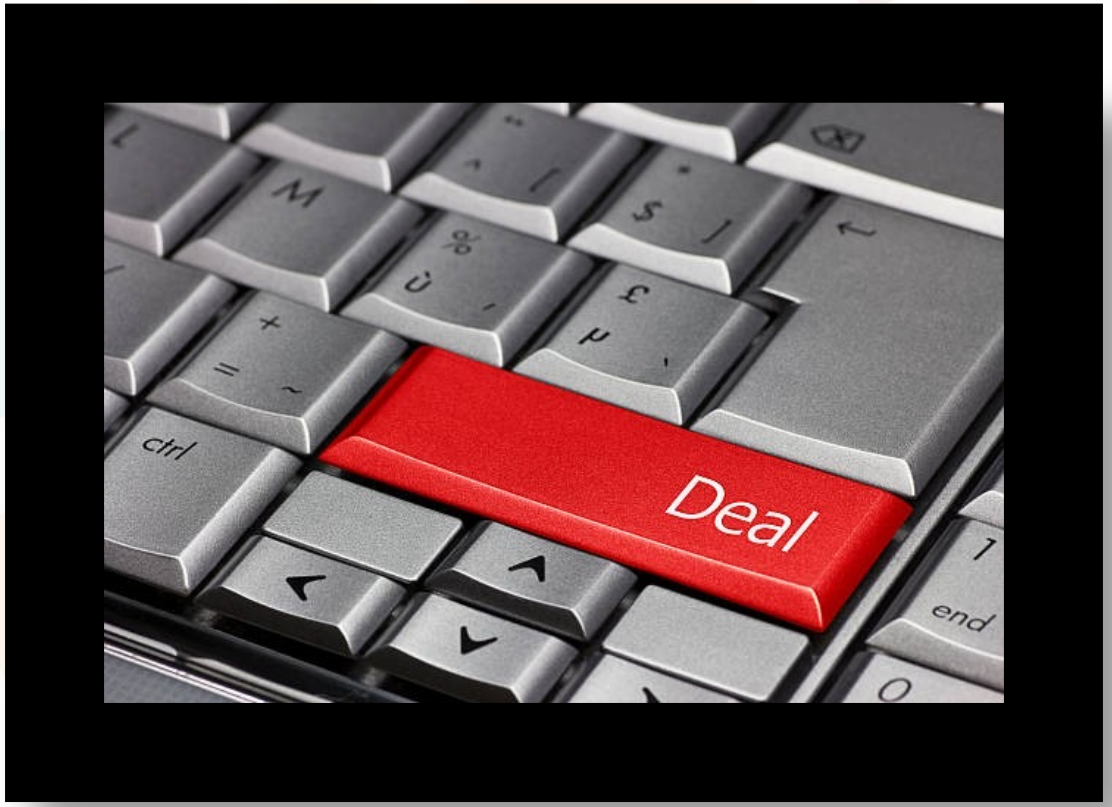
- Just one problem—a hacker had infiltrated the email account of the Beau Townsend manager and sent Don Hinds fraudulent wiring instructions. Although Don Hinds thought it had paid Beau Townsend for the Explorers, it had actually wired the $736,225 to the hacker, who quickly drained the bank account and made off with the money. This case is about who must bear that loss."

Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc., 759 F. App'x 348, 349 (6th Cir. 2018).

BARNES & THORNBURG LLP

Business Email Compromises – Losses and Liabilities?

- Responsibility for payment?
  - Entity that was hacked?
  - Entity that wired the money?
  - Entity that could have stopped the transaction? Or snapped the money back?
  - Causes of action?
    - Negligence? Or other torts?
    - Contract?



BARNES & THORNBURG LLP

Ransomware – What Happens?

- "OCTA was allegedly damaged when a third-party hacker launched a ransomware attack. According to the complaint, this affected numerous OCTA servers, which had to be rebuilt and restored, and caused the loss of OCTA's data . . . ." *Nat'l Union Fire Ins. Co. v. Sharepoint360, Inc.*, No. 18-249 (S.D. Cal. Mar. 27, 2019)

Ransomware – What's Changing?

1. Amounts of demands
2. Second bite at the apple by threat actors
3. Second attacks
4. PII and corporate secret breaches

BARNES & THORNBURG LLP

OFAC Guidance

1. OFAC overview
2. Recent guidance: https://bit.ly/39IkwAx
3. Potential liabilities for OFAC violations

BARNES & THORNBURG LLP

Ransomware – Losses and Liabilities?

- Amount of ransom (in bitcoin)?
- Forensic investigator?
- Legal counsel / breach coach?
- Lost revenues?
- Extra expenses to stay in business?
- Customer claims?
- Replacement servers?

BARNES & THORNBURG LLP

Payment Card Issues – Potential Losses

- What losses result from a hack of payment card data?
  - Amounts taken by card brands
  - Bank class actions
  - Consumer class actions
  - Regulatory investigations
  - Forensics
  - Notifications and credit monitoring

BARNES & THORNBURG LLP

Risk Transfer Methods - Insurance

- Cyberinsurance, Tech E&O (that your organization holds)
- Cyberinsurance, Tech E&O (that a vendor holds)
- Crime insurance
- Kidnap, Ransom, & Extortion
- Property insurance
- Liability policies (D&O, E&O, CGL)
- Other policies

BARNES & THORNBURG LLP

Cyberinsurance: Coverage Checklist

- **In the beginning (forensics)**
  - Did something go wrong? ("First Party Breach Response")
- **Initial obligations under privacy laws**
  - Something went wrong…or maybe it did…and do we need to do something about it…or we should send out notices, offer credit monitoring, and set up a call center? ("First Party Breach Response")
- **Business impact, lost sales**
  - Our reputation has been harmed. (Reputational harm coverage; "First Party Breach Response"/PR)

BARNES & THORNBURG LLP

Cyberinsurance: Coverage Checklist

- **Third party lawsuits, regulatory investigations, and claims**
  - Someone's accusing us of doing something wrong. ("Third Party Liability Coverage")
  - Business customers think that we did something wrong. ("Tech E&O"; Network Security Liability; Privacy Liability)
  - Regulators want to determine if we did something wrong. ("Regulatory Investigation," "Regulatory Claim," "Regulatory Action," etc.)
  - Payment card brands and/or processors think that we did something wrong. (Network Security Liability? Privacy Liability? PCI DSS liability?)
  - Someone alleges that we infringed on their copyright, impacted their advertisements, or made other errors or omissions in our media. ("Media Liability")

BARNES & THORNBURG LLP

Cyberinsurance: Coverage Checklist

- **Impact on the ability to conduct business**
  - Our business has been interrupted or it's more expensive to stay in business. ("Business Interruption," "Extra Expense," "Contingent BI/EE")
  - Our data is gone. ("Data Restoration")
- **Threats to expose or delete data**
  - Someone is threatening to expose our data if we don't pay a ransom. ("Cyber Extortion")
  - Someone has locked up our data and/or network and only will unlock if it if we pay a ransom. ("Ransomware/Cyber Extortion")
  - Customers and business partners are making demands against us because ransomware took our business down (Multiple coverages)

Cyberinsurance: Coverage Checklist

- **Spear phishing/spoofing**
  - We were fraudulently induced to wire funds, and our vendor didn't receive payment. (Multiple coverages)
  - After someone hacked our email, our business partners paid fraudsters, leading to our business partners alleging that we're responsible and refusing to pay our invoices. (Multiple coverages)
  - Someone fraudulently induced us to send out sensitive data (Multiple coverages)

Cyberinsurance: Coverage Checklist

- **Other third party liability claims**
  - People say that we texted or faxed them without permission. (TCPA coverage/exclusions?)
  - People say that we collected their information (*e.g.*, ZIP codes, PII) without permission (Affirmative coverage for wrongful collection? Exclusions?)

BARNES & THORNBURG LLP

Cyberinsurance: Coverage Checklist

- **Social engineering fraud endorsements**
  - Defrauded employees (money sent out)
  - Defrauded vendors (money not received)
  - Call back requirements?
  - Voluntary payment language?
- **Lost revenues due to reputational harm**
- **Cloud-based triggers**
- **Business interruption**
  - System failure triggers
  - Waiting period
  - Contingent business interruption
  - Bricking coverage
  - Betterment coverage
- **Retroactive dates and full prior act coverage**
- **Preferred law firm and vendors?**
- **BYOD and work-from-home**
- **Non-litigated resolutions with customers and SLA-based resolutions?**
- **Liquidated damages and fee-based resolutions of claims (including under government contracts)**

BARNES & THORNBURG LLP

Cyberinsurance: Coverage Checklist

- **Non-claim based additional services and benefits**
  - Discounted cybersecurity services
  - Table top exercises
  - Breach coaching

BARNES & THORNBURG LLP

Cyberinsurance: Players List

- **Privacy / cybersecurity / defense counsel**
  - Usually recommended by or agreed to by the insurer; paid by the insurer
  - Directs investigation; analyzes privacy laws; and defends claims and lawsuits against the insured
- **Forensic firms**
  - Technology forensics usually recommended by or agreed to by the insurer; paid by the insurer
  - Forensic accountants (for business income losses) might be paid by the insurer
- **Insurance broker**
  - Often has "claim advocates" who should push for coverage
  - Note insurance company positions regarding privilege and brokers
- **Coverage counsel**
  - Not recommended by the insurer; not paid by the insurer
  - Provides advice as to how coverage should apply to the claim and losses

BARNES & THORNBURG LLP

What Are Best Practices To Secure Better Coverage?

- **Multi Factor Authentication (MFA)**
  - Is this enabled for all remote access, administrator accounts, RDP, emails, back-ups, and any other area in which this can be applied?
- **Behavioral analysis and/or machine learning endpoint protection (EPP) software**
  - Do we have safeguards in place for detection and response to unusual behavior and malicious attacks on laptops, phones etc.?
- **Server segmentation and air gapping**
  - Are we segmented in a way to stop cyber criminals from being able to move horizontally within our network?
- **Server backups to the cloud and offsite locations**
  - Do we have back-ups that are saved offline and regularly tested to allow our company to have something to fall back on in case of severe data encryption?

What Other Steps Can An Entity Take Regarding Cyber Risk?

- **Breach Response and ransomware preparedness**
  - Do we have a plan in place for when a breach occurs and/or a ransomware attack?
- **Frequent training of employees**
  - Do our employees know how to spot a phishing/fraudulent email and what to do if they encounter one?

Coverage Trapdoors

1. **Business email compromise coverage issues**
    a. Which policies provide coverage for “first party” vs. “third party” loss?
    b. What exclusions and limitations do insurers raise?
        i. Exclusions from “damages” or “loss”?
        ii. Actual liability?
        iii. Contractual liability?
        iv. Was there a “claim”?
        v. Was the loss “direct”?
        vi. Limits and sublimits (particularly in crime policies)?
        vii. Failure to follow call-back or other procedures?

Coverage Trapdoors

2. Ransomware issues

a. Which policies provide coverage for “first party” vs. “third party” loss?

b. What exclusions and limitations do insurers raise?

i. Sanctions check?

ii. Proving losses?

a) Business income?

b) Extra expense?

iii. Resolutions with third parties?

iv. Statements in application?

v. Employee costs?

vi. War exclusions?

Coverage Trapdoors

3. PCI issues

a. Which policies provide coverage?

b. What exclusions and limitations do insurers raise?

i. Retroactive date?

ii. Scope of coverage available for amounts owed to card brands?

a) Affirmative grant of coverage?

b) Limits and sublimits?

c) Exclusions?

Coverage Trapdoors

4. Issues Not Specific to Type of Claim - Notice

Maryland

An insurer may disclaim coverage if: (1) the insured provides **late notice** of a claim; and (2) if the insurer establishes by a preponderance of the evidence that the late notice resulted in **actual prejudice.** *St. Paul Mercury Ins. Co. v. Am. Bank Holdings, Inc.*, 819 F.3d 728, 730 (4th Cir. 2016) (applying Maryland law); Md.Code Ann., Ins. § 19–110.

District of Columbia

Strict notice requirement.

"[W]here compliance with notice provisions is a contractual precondition to coverage, a failure to timely notify releases the insurer from liability." *Nat'l R.R. Passenger Corp. v. Lexington Ins. Co.,* 445 F. Supp. 2d 37, 43 (D.D.C. 2006), *aff'd sub nom. Nat. R.R. Passenger Corp. v. Lexington Ins. Co.*, 249 F. App'x 832 (D.C. Cir. 2007).

Virginia

"[I]n order for untimely notification to constitute a breach the policy, such that the insurer no longer bears the duty to defend the insured, the failure to notify must be **substantial and material**." *State Farm Fire & Cas. Co. v. Wallace*, 997 F. Supp. 2d 439, 446 (W.D. Va. 2014).

"Three factors bear upon the materiality of a breach of the notice provision of a policy: (1) the reasonableness of the delayed notice, (2) the amount of prejudice suffered by the insurer as a result of the delay, and (3) the length of time that elapsed before notice was given." *Id.* at 447.

Coverage Trapdoors

4. **Issues Not Specific to Type of Claim – Consent to settle / cooperation**
   a. What rights does your insurer purport to have regarding settlement?
   b. What's a best practice for resolving a claim when your carrier says, "We haven't completed our coverage evaluation, and can't give you a position"?

Coverage Trapdoors

4. **Issues Not Specific to Type of Claim – Choice of Counsel / Vendors**
    a. Can you pick the law firm and vendor to work on your matter?
    b. Should you use the tech firm that you use for other work?
    c. What if the carrier reserved its rights?
        i. Privilege?
        ii. Control over the investigation and defense?

Best Practices At The Time Of Claim

1. Notice
2. “Claim Handling Counsel”
3. Resolving “other insurance” questions
4. Addressing third party liabilities
5. Privilege and the tri-partite relationship

BARNES & THORNBURG LLP

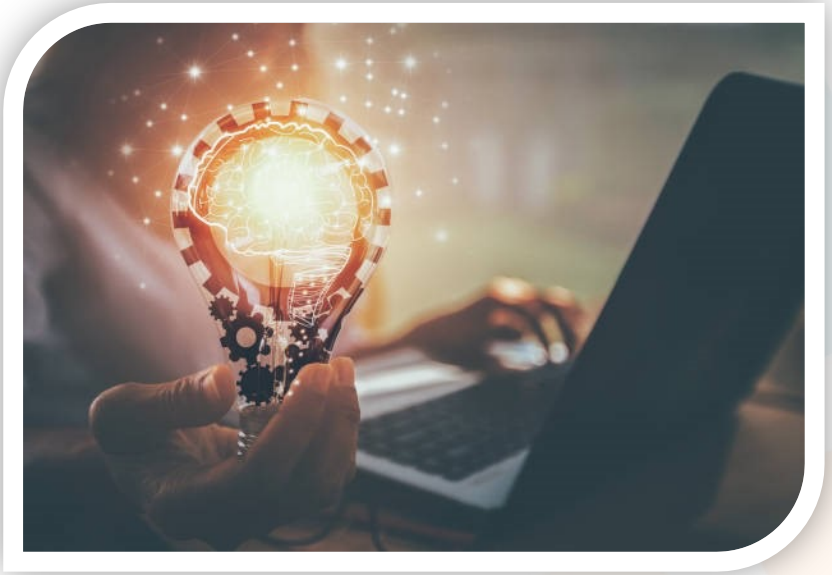
Best Practices At The Time Of Claim

5. Business Interruption and Extra Expense
   a. Forensic Accountants
      i. Covered?
      ii. Scope?
   b. Proof of loss
   c. Lost income
   d. Extra expense
   e. Categorizing losses

Final Insurance Best Practices

1. **When buying insurance:**
    a. Consider whether the types of coverages you have are sufficient or have trapdoors specific to your risks.
    b. Scrutinize exposures to match evolving risks and terms of cyber coverage.
    c. Coverage terms and parameters are beginning to be litigated in early disputes about the application of cyber policies.
    d. Understand where insurance fits into your incident response plan.
    e. Consider your entity's pre-existing relationships and partners.

Final Insurance Best Practices



2. **When there's been an event or incident:**
    a. Notice, notice, notice!
        i. Cyber program?
        ii. Other policies?
    b. Insurer engagement for:
        i. Counsel and vendor retentions?
        ii. Course of action?
        iii. Customer and third party claim defense and resolution?
    c. Pay close attention to the insurance company's position letters and consider carefully your next steps.
    d. Is your counsel engaged?

BARNES & THORNBURG LLP

Questions?

Thank you for your time.