ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Practical Privacy Primer – Elements of a Strong Privacy Program

Cyberinsurance: How to Make Sure You Have the Right Coverage

October 10, 2019

BARNES & THORNBURG LLP

Scott N. Godes

- 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 has assisted clients recover more than $1 billion in insurance coverage. In 2008, he focused his insurance recovery work on coverage for cybersecurity and privacy claims. He 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. One of those disputes spanned three different courts involving multiple parties, with the original action filed under seal, and all settled on terms favorable to his client. 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.

- Mr. Godes 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. Mr. Godes edits the BT Policyholder Protection blog and you can follow him on Twitter @scottgodes.

- Barnes & Thornburg is an AmLaw 100 law firm made up of more than 600 legal professionals throughout 14 offices in Atlanta, Chicago, Dallas, Delaware, Indiana, Los Angeles, Michigan, Minneapolis, Ohio, San Diego, and Washington, DC.

Laura H. Jones

Laura H. Jones, Senior Director, Associate General Counsel, Avaya Inc. | lhjones@avaya.com

Laura Jones is associate general counsel of Avaya and a leader of the ACC NCR Technology and IP Law Forum. She is an experienced commercial law generalist with particular emphasis on technology clients, and has been in-house for most of her career, with helpful interludes at large firms. She presently runs the US Commercial Law legal team for Avaya, a global communications solutions provider.

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).

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?

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 – 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?

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

Interplay of Risk Management & Insurance

"An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. **While it has been suggested that having insurance encourages companies to slack off on security, our research suggests the opposite.** Those companies with good security practices are more likely to purchase insurance."

Source: Ponemon Institute 2014 Research Report at 22

Risk Transfer Methods - Insurance

- Cyberinsurance, Tech E&O (that your company holds)
- Cyberinsurance, Tech E&O (that a vendor holds)
- Crime insurance
- Other policies?

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)

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?)

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")

Cyberinsurance: Coverage Checklist

- Spear phishing/spoofing
  - We were fraudulently induced to wire funds. (Social Engineering Fraud/Computer Fraud/Funds Transfer Fraud)
  - After someone hacked our email, our business partners paid fraudsters, and our business partners allege that we're responsible. (Multiple coverages)
  - Someone fraudulently induced us to send out sensitive data (Multiple coverages)
- Other third party liability claims
  - People say that we texted or faxed them without permission. (Exclusions?)
  - People say that we collected their information (*e.g.*, ZIP codes, PII) without permission (Affirmative coverage for wrongful collection? Exclusions?)

Cyberinsurance: Coverage Checklist

- Social engineering fraud endorsements
  - Defrauded employees
  - Defrauded vendors
- Lost revenues due to reputational harm
- Cloud-based triggers
- Business interruption
  - System failure triggers
  - Waiting period
  - Contingent business interruption
- Retroactive dates and full prior act coverage

Cyberinsurance: Coverage Checklist

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

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

Do My Other Insurance Policies Cover These Risks?

- CGL?
- Crime?
- E&O?
- D&O?
- First Party Property?
- KRE?

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. Proving losses?

a) Business income?

b) Extra expense?

ii. Resolutions with third parties?

iii. 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

a. Notice

b. Consent to settle / cooperation

c. Choice of counsel, vendors

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?