How to Prevent and Respond to Business Email Compromises

April 26, 2022

Presented by Christopher Hart and Yoni Bard

FOLEY HOAG LLP

Speakers

Christopher Hart
Partner and Co-Chair, Privacy & Data Security Group
Foley Hoag LLP
chart@foleyhoag.com

Yoni Bard
Associate
Foley Hoag LLP
ybard@foleyhoag.com

Agenda

- Business email compromise (“BEC”) overview
- BEC case studies
- Preventing and preparing for a BEC
- Responding to a BEC
- Claims and defenses
- Aftermath

The Scourge of Cyber Attacks

- Dozens of types of cyber attacks carried out against consumers, businesses, and governments.
  - March 2020 Solar Winds hack
  - May 2021 ransomware attack on Colonial Pipeline

- Cause profound business disruption and hefty monetary losses estimated at trillions in the aggregate.

- It’s only getting worse.

Business Email Compromises

- Sophisticated attacks conducted through social engineering, i.e., manipulating trust in human interactions.
- Difficult to identify and thwart because they rely on human error, not just exploitation of IT vulnerabilities.
- One kind of attack using social engineering is **business email compromise**, sometimes referred to as a “man-in-the-middle attack.”
- Involves impersonation of trusted individual and fraudulent wire instructions.
- In 2021, FBI received 19,954 business email compromise complaints.

Business Email Compromises: Step by Step

- **Step 1**: Attacker identifies target individual or organization.
- **Step 2**: Attacker studies business patterns.
  - Based on publicly available information and/or internal information obtained from cyber intrusion and lurking.
- **Step 3**: Attacker impersonates known individual, either using that individual's email address or spoofed email address.
- **Step 4**: Attacker uses fraudulent wire instructions to redirect payment.

Impact of Business Email Compromises

- **Financial loss**
  - FBI reported nearly $2.4 billion in losses in 2021 based on reported BECs.
- **Data loss**
  - Possibly involving sensitive information, triggering reporting obligations and creating liability.
- **Reputational harm**
  - To the entity and specific individual targeted.
- **Business relationship**
  - Can sour or destroy.
- **Litigation**
  - With payor or payee, third-party (e.g., over data loss), or insurer.

Case Study: *Arrow Truck Sales*

- *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment,* Inc., No. 8:14-cv-2052-T-30TGW, 2015 U.S. Dist. LEXIS 108823 (M.D. Fla. Aug. 18, 2015)
- Agreement for sale of trucks.
- Two sets of wire instructions, then a misdirected payment.
- Plaintiff (payor) sued and defendant counterclaimed for breach of contract (failure to make the required payment).
- Judgment for defendant because plaintiff was in best position to prevent the loss.

Case Study: *Bile*

- *Bile v. RREMC, LLC,* No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. Aug. 24, 2016)

- Transfer of funds pursuant to settlement agreement.

- Plaintiff (payee) had "actual knowledge" that "a malicious third party was targeting this settlement for a fraudulent transfer to an offshore account that did not belong to [the plaintiff]" and nevertheless failed to notify defendant.

- Judgment for defendant because plaintiff was in best position to prevent the loss.
  - "At the heart of this case is the simple fact that Bile's agent, Ubom, could have prevented the loss of $63,000.00 by notifying opposing counsel on July 27, 2015 when he had actual knowledge of an attempted fraud, the known purpose of which was to lay hands on the settlement funds."

Preventing Business Email Compromises

- **Authentication processes**
  - Have a multi-factor approach to payment changes that includes voice/video verification.
  - Build payment method into contracts.
- **Avoid unsecured email for payment purposes**
- **Basic cyber-hygiene**
  - Periodic review of audit logs.
- **Employee training**
  - When in doubt, pick up the phone.

Mitigating Fallout

- **Contractual protections**
  - Consider specific clauses to account for potential fraudulent payment, including “share the burden” clause.

- **Cyberinsurance**
  - Take care to determine scope of coverage.
  - Consider subrogation issues.

Responding to Business Email Compromises

- Rapid response strategies ASAP to avoid or mitigate loss
  - Notify payor's bank to stop payment.
  - Report to law enforcement by filing online complaint with FBI's Internet Crime Complaint Center (IC3).
- Incident review to understand nature and scope of attack
  - Engage digital forensic team (but be mindful of privilege).
- Provide any required notifications
  - Insurers, customers, etc.
- Dispute with counterparty

Claims and Defenses

- Imposter rule: party in the best position to prevent the loss must bear that loss.
  - *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc.,* No. 8:14-cv-2052-T-30TGW, 2015 U.S. Dist. LEXIS 108823 (M.D. Fla. Aug. 18, 2015)
  - *Jetcrete North America LP v. Austin Truck & Equipment, Ltd.,* 484 F. Supp. 3d 915 (D. Nev. 2020)
  - *Parmer v. United Bank, Inc.,* No. 20-0013, 2020 W. Va. LEXIS 828 (Dec. 7, 2020)

- Simple breach of contract for non-payment.
  - *Peeples v. Carolina Container, LLC*, No. 4:19-cv-21-MLB, 2021 U.S. Dist. LEXIS 176076, at *8-9 (N.D. Ga. Sep. 16, 2021) (finding that a defendant presented with fraudulent wiring instructions by a hacker who infiltrated the computer system of the plaintiff's attorney was liable for breach of contract because, despite its intentions, it paid the wrong party).

- Others? Get creative.

Aftermath

- Counsel should prepare written report, but watch out for privilege issues.
- Revisit IT security and controls.
- Retrain staff.
- Reconsider insurance coverage.

FOLEY HOAG LLP

Questions?

Thank You

Christopher Hart
Partner
Co-Chair, Privacy & Data Security Group
Foley Hoag LLP
chart@foleyhoag.com

Yoni Bard
Associate
Foley Hoag LLP
ybard@foleyhoag.com

For the latest developments in privacy and data security law, please subscribe to our blog.

https://www.securityprivacyandthelaw.com