

**4<sup>th</sup> Annual  
Government Enforcement Conference**

**Cybersecurity:  
Important Lessons in Breach Response**

**October 27, 2017**

**Sean B. Hoar, CISSP, GISP, CIPP/US, Lewis Brisbois  
Partner & Chair, Data Privacy & Cyber Security  
Practice**

**Andrew Valentine, Associate Managing Director,  
Cybersecurity and Investigations, Kroll**

**Allen Burzen, Referral Partner Manager, AllClear ID**

# Overview of discussion

---

- Reasons to be concerned
  - Current online threats
  - Regulatory environment
  - Reputational and economic cost
- Important lessons
  - Forensics investigations
  - Consumer remediation
  - Regulatory investigations

# Trends in Data Security

---

- Data breaches
  - Databases
  - POS systems
    - Technical subterfuge & social engineering
  - Data theft
    - Digital
    - Paper – most immediate impact
    - Mobile devices
- Extortionate attacks
  - Encryption (Ransomware)
    - Corrupted backups
  - Distributed denial of service (DDoS)
    - Often after failed ransomware attack



Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

Title search: Cybersecurity: Important Lessons in Breach Response

Also available as part of the eCourse

[2017 Government Enforcement eConference](#)

First appeared as part of the conference materials for the

4<sup>th</sup> Annual Government Enforcement Institute session

"Cybersecurity: Important Lessons in Breach Response"