BakerHostetler

Ransomware: History, Histrionics, and "Honor"- The Intersection of Preparation and Prevention

February 24, 2017

Emily R. Fedeles
efedeles@bakerlaw.com

James A. Sherer
jsherer@bakerlaw.com

Breach Hotline: 855-217-5204
www.dataprivacymonitor.com

James Sherer, Partner

BakerHostetler

James Sherer is a partner in the New York office of BakerHostetler, where he chairs the Information Governance practice team and serves as part of the E-Discovery Advocacy and Management and Privacy and Data Protection groups. James assists with oversight of discovery and Electronically Stored Information issues for firm clients. James is also tasked with "deep dive" technological and case law-related assignments for omnibus motions and case strategy. James's work focuses on advising on merger & acquisition due diligence; information governance practices and policies for clients; and client corporate structure and business offerings regarding international data privacy requirements.

James holds an MBA, has CIPP/US, CIPP/E, CIPM, and FIP data privacy professional credentials, the CIP and IGP information governance designations, and the CEDS eDiscovery specialist credential. James is a member of The Sedona Conference® Working Groups One, Six, and Eleven and has served on Search, Achieving Quality, Data Privacy and Security, and Merger & Acquisition Drafting Teams. He is also a member of the New York State Bar Association EDiscovery Committee as well as the New York eDiscovery Counsel Roundtable.

Emily Fedeles, Associate

BakerHostetler

Emily Fedeles is an associate in the New York office of BakerHostetler, where she maintains a general litigation practice and serves as part of both the E-Discovery Advocacy and Management and the Privacy and Data Protection groups. Emily regularly works with clients across multiple industry sectors on a wide range of matters, including assisting with the oversight of discovery and Electronically Stored Information issues as well as developing litigation and regulatory responses to data breaches.

Prior to joining BakerHostetler, Emily practiced litigation in Geneva, Switzerland, where she developed a wealth of experience relating to cross-border litigation and discovery issues and data privacy and security considerations. She began her legal career as an associate in Florida, where she was a member of four trial teams for multi-million dollar cases in both state and federal court.

Emily attended Emory University for both undergrad and law school, where she held an internship with The Atlanta Spirit and served as a juvenile public defender under the Third Year Practice Act. She is a member of the International Association of Privacy Professionals (CIPP/E) and The Sedona Conference® Working Groups One, Six, and Eleven. Emily has written and spoken on e-discovery and privacy issues with a particular focus on the impacts of emerging technologies such as corporate "Bring Your Own Device" programs.

Agenda

- Ransomware Explained
- History of Ransomware
  - Ransomware as a Process
  - Ransomware as a Business
- Defending against and Responding to Ransomware
  - Ransomware's Direct Impact
  - Ransomware's Indirect Impact
  - Ransomware Response
    - Practical and Legal Challenges
- Future of Ransomware

What is Ransomware?

Ransomware Unpacked

- What is ransomware?
  - Malicious software that exploits or damages a target by infecting a computer or system
  - May be spread in a variety of ways
  - Attackers are getting smarter in delivery methods
- What forms does ransomware take?
  - Can be categorized based on the form of attack that ransomware takes
  - Locker ransomware, crypto ransomware, hybrid approaches

How Ransomware Works

- Encrypts or otherwise denies access to the data
- At next log-in, the victim gets a message that his data is being held hostage until a payment is made
- Typically includes a fast-approaching deadline, sometimes includes ancillary threats to disclose the data publicly

How Victims Pay

- Ransom payments generally must be made in a digital currency (Bitcoin)
- Attackers remain anonymous and transactions are virtually untraceable
- No middle-man involved
- Some even offer “customer service”
- Strategic decision whether to pay

How Organizations are Damaged

Monetary

- Ransom payment
- Lost profits while business operations halted
- Cost of engaging outside IT/forensics consultant
- Breach response costs if personal data accessed
- Potential regulatory fines or litigation costs

Non-monetary

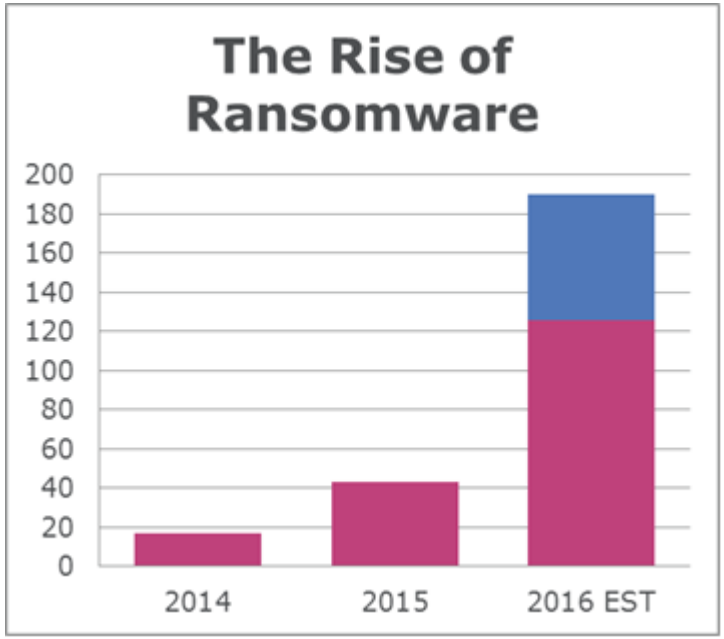
- Reputation damage
- Disruption of customer access to vital services
- Nightmare of potential breach if personal data accessed

Ransomware through the Decade(s)

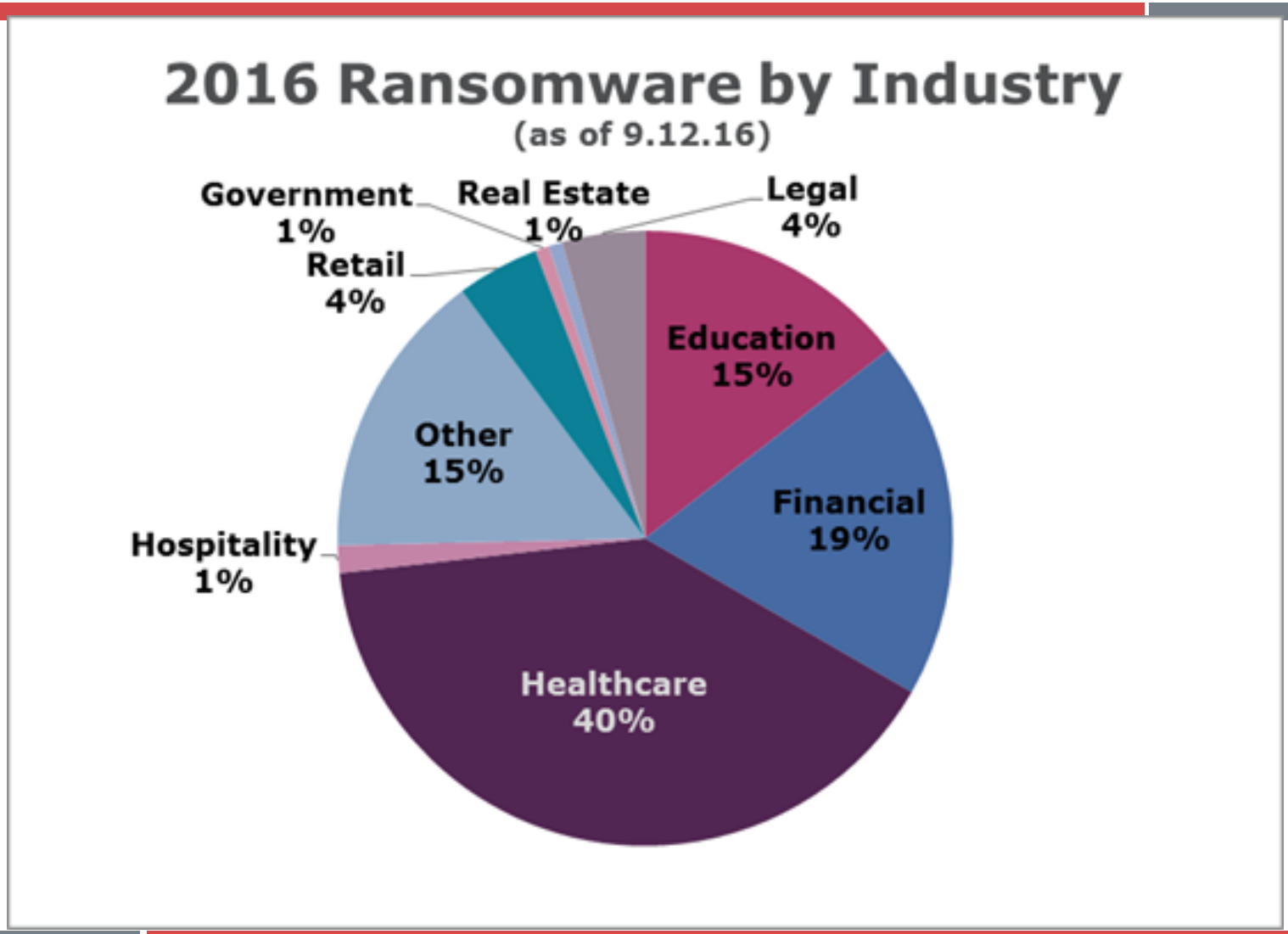
The Rise of Ransomware

- **Late 1980s - early 2000s**
  - Minor inconvenience
  - Payment largely unnecessary
- **2005 resurgence**
  - Actually successful in disabling machines
  - Precursor to what we see today
- **2013 - present**
  - Fast spreading
  - Growing exponentially in number and possible of devices it may effect
    - Emergence of smartphone variants

The Rise of Ransomware



Ransomware by Industry



Protecting Against and Responding to Ransomware

Ransomware Defense

- Implement robust backup and recovery policies and procedures
  - Backups to be maintained separate from the main network, preferably off-site
- Thorough data security training
- Workforce education
- Software solutions to block incoming malware
- Stay on top of the latest developments

Ransomware Defense

- Technical and administrative solutions
  - Disable use of vulnerable plugins
  - Deploy intrusion prevention
  - Utilize endpoint security software
  - Keep antivirus protection up-to-date
  - Ensure security patches are installed promptly

OCR Guidance

- July 2016 – the Department of Health and Human Services, Office for Civil Rights releases guidance on how the agency interprets ransomware attacks on HIPAA covered entities and business associates
  - "When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired….unless the covered entity or business associate can demonstrate that there is a '…low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule."

To Pay or Not To Pay?

- Will payment result in release of devices or a renewed demand for an increased payment?
- Law enforcement will not advise a company whether or not to pay, though may provide anecdotal evidence or information about a particular “brand” of ransomware
- May violate Office of Foreign Assets Control (OFAC) restrictions
- May result in further demands

Payment and Logistics

- Payment typically must be made in Bitcoin
  - Availability
  - Vulnerability and Victim Identification
  - Taxable status
- Ransom payments are not endorsed by the USA
- OFAC Restrictions
- Executive Order 13694 Cybercrime Restrictions

Questions?

BakerHostetler

James A. Sherer
Partner, BakerHostetler – New York
212.589.4279
jsherer@bakerlaw.com
@jamessherer

Emily R. Fedeles
Associate, BakerHostetler – New York
212.589.4202
efedeles@bakerlaw.com
@emilyrfedeles