Cybercriminals, Data Breaches & Regulatory Requirements:

A look into the increasingly challenging world of privacy and data protection

July 13, 2017

Doron S. Goldstein

Co-Head, Privacy, Data & Cybersecurity Practice
Katten Muchin Rosenman LLP

Katten
Katten Muchin Rosenman LLP

Background

- ***Data***
  Collection, analysis and use of personal and other information

Background

- ***Data***
  Collection, analysis and use of personal and other information

    - ***Cybersecurity***
      Protection of information systems, business information and personal data.

Background

- ***Data***
  Collection, analysis and use of personal and other information

    - ***Cybersecurity***
      Protection of information systems, business information and personal data.

        - ***Privacy****:*
          Protection of personal data

Overview

- **Technology & Data**
- **Cybersecurity**
  - Ransomware
  - Data Breach
- **Privacy**
  - GDPR
- **Addressing Current (and Future) Realities: Protecting Your Ass(ets)**

Technology and Data

Hospitality Technology Landscape - Mobile

- **Mobile is ubiquitous**
  - Reviews and Comparisons
  - Booking
  - Check-in
  - Room Access
  - Guest Services

Hospitality Technology Landscape - Guests

- **Guests expect in-room technological conveniences**
  - High bandwidth WiFi
  - On-demand entertainment
  - Integration of personal mobile
  - Voice activation
  - Coming Soon: Internet of Things (IoT)

Hospitality Technology Landscape - Data

- **Data is cross-platform and integrated**
  - Online (hosted) platforms
  - Property management systems (PMS)

Powered by **handy** OS

handy OS is the world's first mobile operating system tailored for the hospitality industry. We've carefully listened to the needs of hoteliers and travelers to design a service that provides hotels with increased revenue opportunities and guests with seamless connectivity and content.

Powered by **handy** OS

handy OS is the world's first mobile operating system tailored for the hospitality industry. We've carefully listened to the needs of hoteliers and travelers to design a service that provides hotels with increased revenue opportunities and guests with seamless connectivity and content.

Hospitality Technology Landscape

- **Technology and data use and analysis offers significant value**
  - Understanding and addressing guest needs
  - Engaging in behaviour analytics (bookings, cancellations, maintenance)
  - Enhancing revenue generation
- **There are also significant challenges**
  - Cybersecurity Risks
  - Privacy and Data Protection Requirements

Cybersecurity

Hospitality Industry Data Security - Overview

- **Valuable target, with significant amounts of useful data**
- **Multiple Vulnerabilities/Risks:**
  - POS
  - Guest (open) WiFi
  - Room keys
  - Hosted PMS/CRM systems
  - Often limited internal information security support
  - Vendors and service providers
  - Personnel with significant access

Hospitality Industry Data Security - Vulnerabilities

- **Phishing/Social Engineering**
  - Targets known individuals and departments
  - Tricks individuals into harmful acts
- **Malware**
  - Unauthorized malicious code
  - Exploits individuals or known vulnerabilities
- **Ransomware**
  - Most profitable form of malware
  - Holds data hostage, and demands payment to unlock it
- **(Personal) Data Breaches**

Ransomware

Ransomware – Recent Developments

- **Ransomware**
  - "Romantik Seehotel Jägerwirt, had its electronic key system compromised by hackers, which locked management out of its computer system…Guests were unable to access their hotel rooms…"

    – SAS Americas April, 2017

Ransomware – Recent Developments

- **Ransomware**
  - "Romantik Seehotel Jägerwirt, had its electronic key system compromised by hackers, which locked management out of its computer system…Guests were unable to access their hotel rooms…"
    – SAS Americas April, 2017
  - *Why 'WannaCry' Malware Caused Chaos for National Health Services in the U.K*
    - NBC News
  - *The Ransomware Meltdown Experts Warned About is Here*
    - Wired

Ransomware – Recent Developments

- **Ransomware**
  - "Romantik Seehotel Jägerwirt, had its electronic key system compromised by hackers, which locked management out of its computer system…Guests were unable to access their hotel rooms…"

    – SAS Americas April, 2017
  - *Why 'WannaCry' Malware Caused Chaos for National Health Services in the U.K*

    - NBC News
  - *The Ransomware Meltdown Experts Warned About is Here*

    - Wired
- **Faux Ransomware**

Ransomware – Recent Developments

- **Ransomware**
  - "Romantik Seehotel Jägerwirt, had its electronic key system compromised by hackers, which locked management out of its computer system…Guests were unable to access their hotel rooms…"
    – SAS Americas April, 2017
  - *Why 'WannaCry' Malware Caused Chaos for National Health Services in the U.K*
    - NBC News
  - *The Ransomware Meltdown Experts Warned About is Here*
    - Wired
- **Faux Ransomware**
  - *Petya or NotPetya: Why the Latest Ransomware is Deadlier than WannaCry*
    - Forbes
  - *New computer virus spreads from Ukraine to disrupt world business*
    - Reuters

Ransomware - Costs

- 2016 losses estimated to exceed $75 billion
- Experts disagree on the amount of ransomware paid out in 2016, with estimates ranging from hundreds of millions of dollars to approximately $1 billion
- The FBI reported that an average of more than 4,000 ransomware attacks were recorded each day in 2016 (up from about 1,000 daily attacks in 2015)
- Average ransom demand mid-2016 was $679; in October, Beazley reported an average of $1,000
- Targeted attacks can demand significantly more

Ransomware - Targets

- **Study of 165 US organizations**
  - 79% had a malware attack in the prior 12 months;47% had ransomware attack
  - Of the ransomware attacks, 37% paid a ransom; 72% of those who didn't lost some data.
- **Study of 305 large UK organizations**
  - 44% were infected by ransomware (27% more than once)
  - An average of 33 man hours spent to remediate

Ransomware - Defenses

- **Survey of 60 companies that suffered ransomware attacks:**
  - 100% ran antivirus software
  - 95% had firewalls
  - 77% of the attacks got through email filtering
  - 52% of the attacks bypassed anti-malware software
  - 33% were infected despite security awareness training

Data Breach

Data Breach - Recent Developments

- **Data Breach**
  - "IHG's Americas division confirmed food-and-beverage outlets at 12 U.S. hotels were hit by a data breach between August 1 and December 20, 2016."
    – SAS Americas April, 2017

Data Breach - Recent Developments

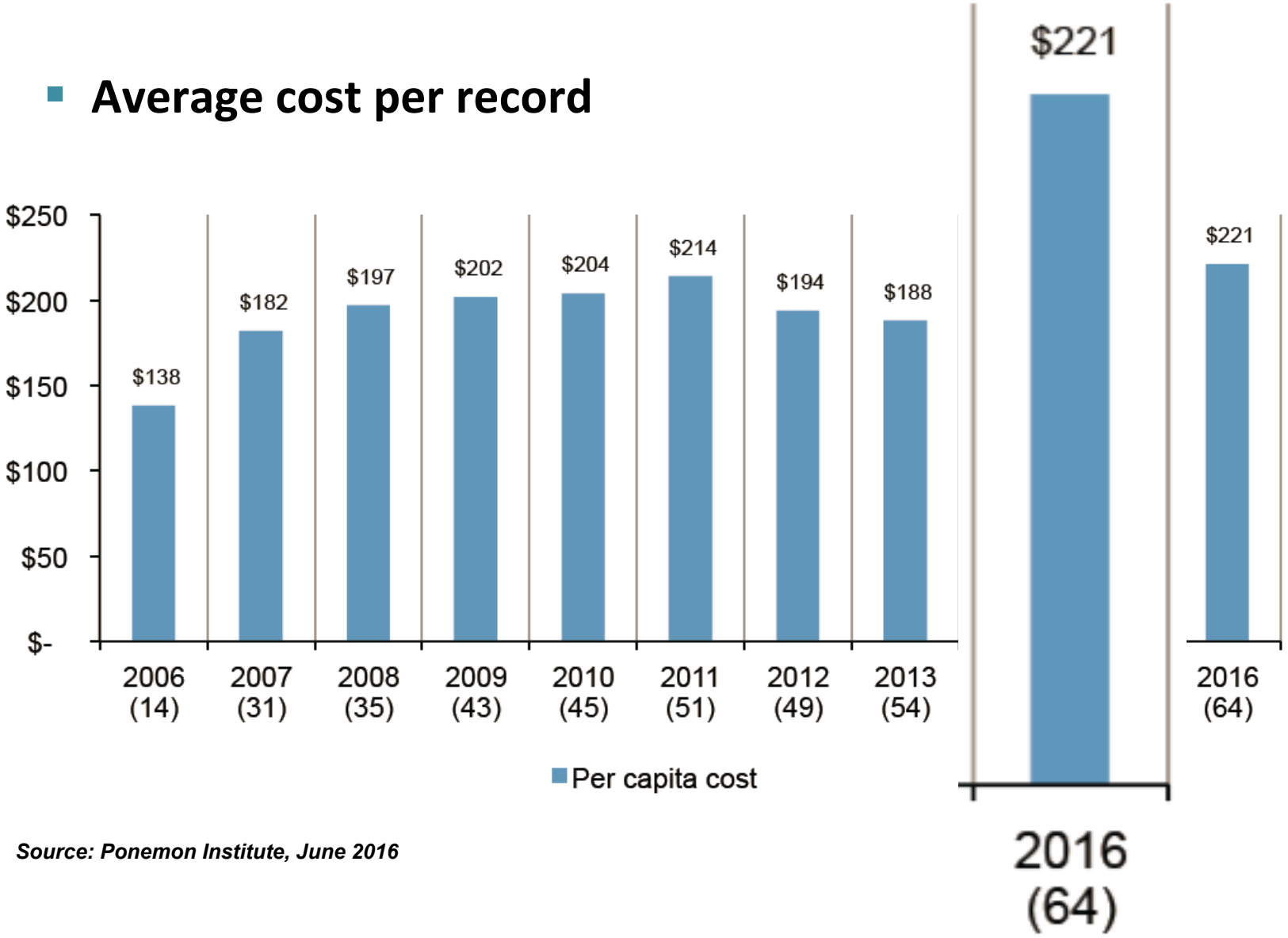
- **Data Breach**
  - "IHG's Americas division confirmed food-and-beverage outlets at 12 U.S. hotels were hit by a data breach between August 1 and December 20, 2016."
    – SAS Americas April, 2017
  - *InterContinental data breach expands from 12 to 1200 hotels*
    - ZDNet
  - *Credit card breach at InterContinental affects 1000 hotels*
    - Fox News

Data Breach - Recent Developments

- **Data Breach**
  - "IHG's Americas division confirmed food-and-beverage outlets at 12 U.S. hotels were hit by a data breach between August 1 and December 20, 2016."
    – SAS Americas April, 2017
  - *InterContinental data breach expands from 12 to 1200 hotels*
    - ZDNet
  - *Credit card breach at InterContinental affects 1000 hotels*
    - Fox News
- **Vendor Data Breach**
  - *Sabre Rattled by Breach Affecting Card Data at 36,000 Locations*
    - CU Times
  - *Hard Rock, Loews hotels admit data breach*
    - ZDNet

Data Breach - Costs

- **Average cost per record**



Source: Ponemon Institute, June 2016

Data Breach – Sabre/SynXis

- **Vendor data breach**
- **Multiple parties**
  - Properties/operators
  - OTAs
  - Intermediaries
- **Complex data sets**
- **Multinational**

Privacy

Privacy - Current Issues

- **New European Regulations**
  - General Data Protection Regulation
  - Cookie (ePrivacy) Directive (updated)
  - NIS (Network and Information Systems)/Cybersecurity Directive

Privacy - Current Issues

- **New European Regulations**
  - General Data Protection Regulation
  - Cookie (ePrivacy) Directive
  - NIS (Network and Information Systems)/Cybersecurity Directive
- **EU Regulators Issuing Larger Fines**
  - Facebook – €122 million fine for "incorrect or misleading" information relating to personal account linking in WhatsApp acquisition
  - Google – €2.42 billion for directing search traffic to its shopping services

Privacy – Examples

- **Payment Card Industry Data Security Standards (PCI-DSS)**
  - Technical and operational protections for cardholder data
  - Noncompliance Fines: $5,000 to $500,000.
  - Potential Breach Consequences: $50-$90 fine/card; suspension of credit card acceptance

Privacy – Examples

- **Payment Card Industry Data Security Standards (PCI-DSS)**
  - Technical and operational protections for cardholder data
  - Noncompliance Fines: $5,000 to $500,000.
  - Potential Breach Consequences: $50-$90 fine/card; suspension of credit card acceptance
- **US Federal & State Requirements**
  - FTC consent decrees/fines for exposing personal data, as an unfair or deceptive trade practice
    - Examples include Wyndham Hotels
  - 48 states, plus DC and US territories have data breach notification laws

Privacy - GDPR

- **Effective**: May 2018
- **Replaces the Data Protection Directive & current national laws**
- **Maximum Fines**:
  - Greater of €20 million or 4% of global turnover for violation of principles, data subject rights, international data transfers, member law obligations, SA orders.
  - Greater of €10 million or 2% of global turnover for other violations

Privacy - GDPR

- **Data Privacy Principles:**
  - Lawful, Fair and Transparent Processing
  - Purpose Limitation
  - Minimization and Proportionality
  - Quality and Accuracy
  - Data Retention
  - Data Security (Integrity and Confidentiality
  - Accountability

Privacy - GDPR

- **Some Operational Issues:**
  - Complexity of “consent”
  - Data subject right to obtain a copy of the personal data
  - Right of Erasure (Right to be Forgotten)
  - Data Portability
  - Limited Retention
  - Breach Reporting: 72 hours
  - Vendor Management

Protecting Your Ass(ets)

Implementing Technologies and Protecting Data

- **Consider the implications of technologies before implementation**
  - Convenience vs. risk
  - Conduct PIAs/DPIAs
- **Manage Risks**
  - Understand data flows
  - Manage vendors
  - Implement appropriate information security practices
  - Train personnel
  - Consider Insurance

Implementing Technologies and Protecting Data

- **Information Security**
  - Updates/patch management
  - Lock down/limit known vectors
    - Disable scripts, spam filters
  - Encryption where appropriate
  - Intrusion detection and prevention
  - Multifactor authentication
  - Least privilege access
  - Device/equipment management

Implementing Technologies and Protecting Data

- **Planning**
  - Risk assessment
  - Appropriate policies
  - Business continuity plan
  - Personnel training and education
    - Involve vendors as appropriate
  - Cyberliability insurance
    - Consider appropriate coverage amounts and types
  - Tabletop exercises/wargames

Implementing Technologies and Protecting Data

- **Incident Response Plan**
  - Crisis management
  - Key internal and external contacts
    - Include back-ups
    - Define authority/decision-making
  - Communications plans (both internal and external)
  - High-risk (based on likelihood and/or severity) scenarios
  - Consider vendor breach
  - Consider pre-engagement of forensics and other response providers

Katten Muchin Rosenman LLP Locations

AUSTIN
One Congress Plaza
111 Congress Avenue
Suite 1000
Austin, TX 78701-4073
+1.512.691.4000 tel
+1.512.691.4001 fax

CHARLOTTE
550 South Tryon Street
Suite 2900
Charlotte, NC 28202-4213
+1.704.444.2000 tel
+1.704.444.2050 fax

CHICAGO
525 West Monroe Street
Chicago, IL 60661-3693
+1.312.902.5200 tel
+1.312.902.1061 fax

HOUSTON
1301 McKinney Street
Suite 3000
Houston, TX 77010-3033
+1.713.270.3400 tel
+1.713.270.3401 fax

IRVING
545 East John Carpenter Freeway
Suite 300
Irving, TX 75062-3964
+1.972.587.4100 tel
+1.972.587.4109 fax

LONDON
Paternoster House
65 St Paul's Churchyard
London EC4M 8AB United Kingdom
+44.0.20.7776.7620 tel
+44.0.20.7776.7621 fax

LOS ANGELES – CENTURY CITY
2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012
+1.310.788.4400 tel
+1.310.788.4471 fax

LOS ANGELES – DOWNTOWN
515 South Flower Street
Suite 1000
Los Angeles, CA 90071-2212
+1.213.443.9000 tel
+1.213.443.9001 fax

NEW YORK
575 Madison Avenue
New York, NY 10022-2585
+1.212.940.8800 tel
+1.212.940.8776 fax

ORANGE COUNTY
100 Spectrum Center Drive
Suite 1050
Irvine, CA 92618-4960
+1.714.966.6819 tel
+1.714.966.6821 fax

SAN FRANCISCO BAY AREA
1999 Harrison Street
Suite 700
Oakland, CA 94612-4704
+1.415.293.5800 tel
+1.415.293.5801 fax

SHANGHAI
Suite 4906 Wheelock Square
1717 Nanjing Road West
Shanghai 200040 P.R. China
+86.21.6039.3222 tel
+86.21.6039.3223 fax

WASHINGTON, DC
2900 K Street NW
North Tower - Suite 200
Washington, DC 20007-5118
+1.202.625.3500 tel
+1.202.298.7570 fax

Katten
Katten Muchin Rosenman LLP
www.kattenlaw.com