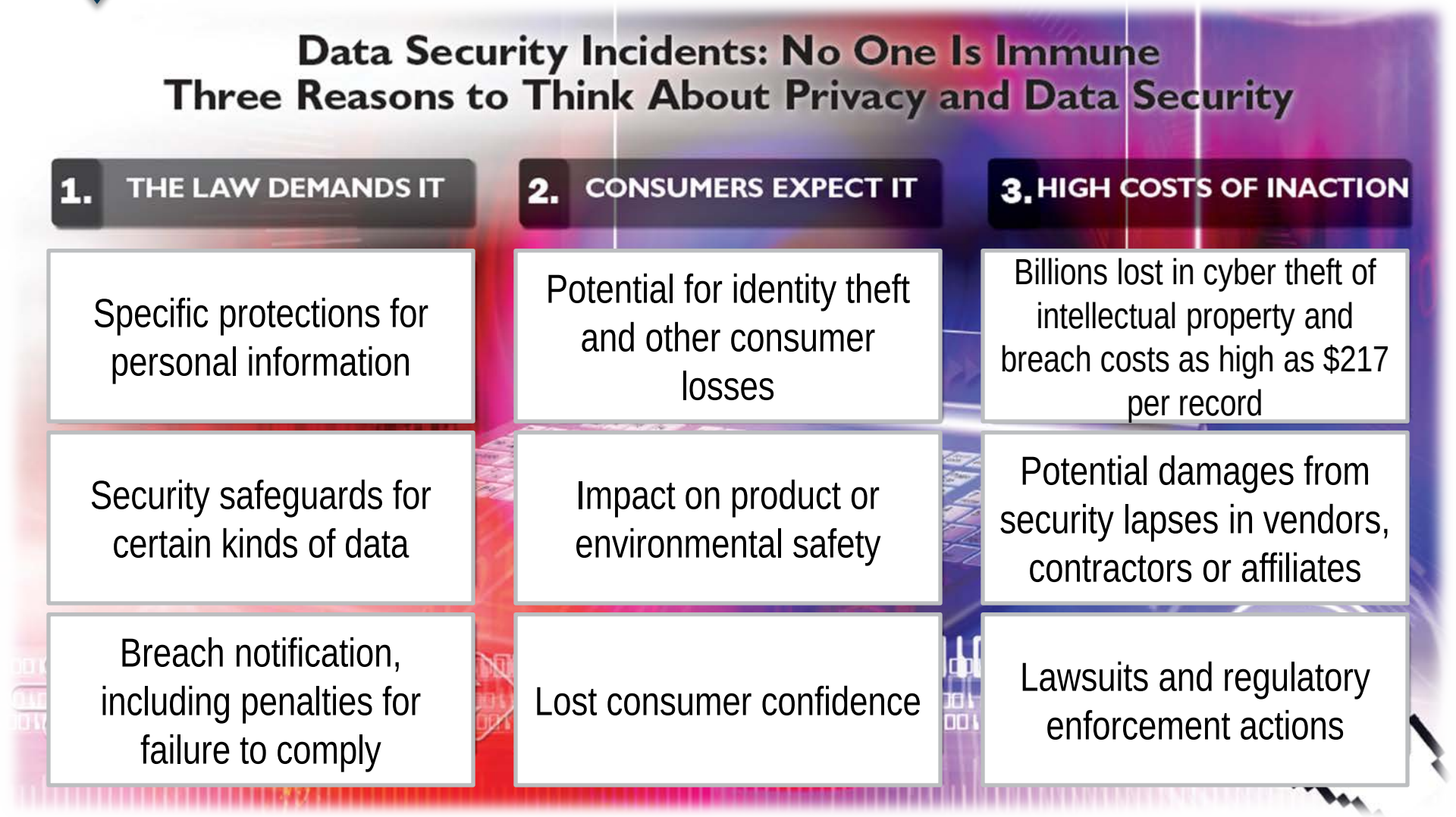
Cybersecurity: Minimizing the X-Factor

Kathleen Rice
Faegre Baker Daniels

NFI Insurance Forum
Indianapolis, IN
October 23, 2015

FAEGRE BAKER DANIELS

Data Security and Privacy Incidents Are on the Rise



Why More Companies are Paying Attention to Cybersecurity

Why More Companies are Paying Attention to Cybersecurity

In 2015, average cost for each lost or stolen record increased from $201 to $217.

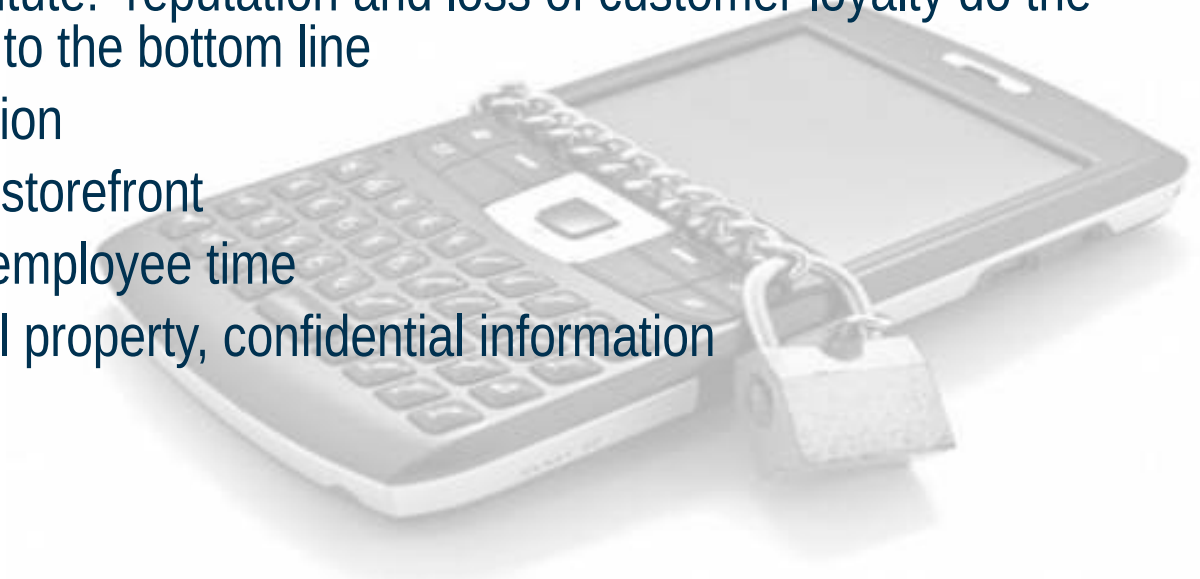
Total average cost paid by U.S. company increased from $5.9 million to $6.5 million.

Source: Ponemon Institute 2015 Cost of Data Breach Study: United States

Why More Companies are Paying Attention to Cybersecurity

- The legal costs
  - Data breach notification
  - Data breach litigation
  - Regulatory enforcement

- The non-legal costs
  - Loss of consumer/shareholder/employee confidence
    - Ponemon Institute: reputation and loss of customer loyalty do the most damage to the bottom line
  - Business interruption
    - Disabled web storefront
    - Demands on employee time
  - Loss of intellectual property, confidential information



Minimizing the X-factor: Understanding Data and Risk

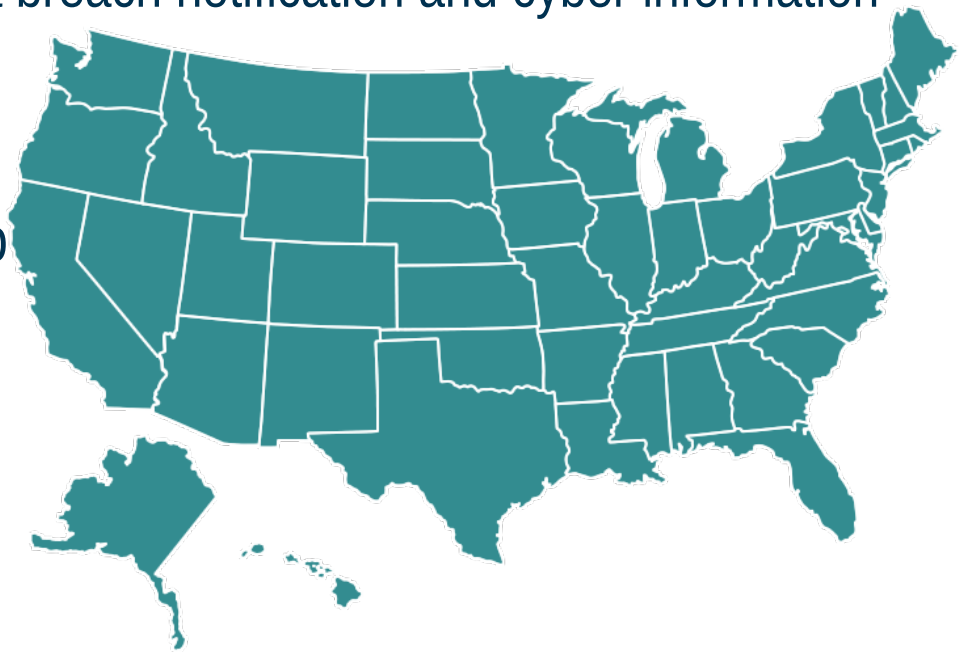
- Know your organization
  - Increased regulatory focus on “tone at the top”
  - Understand applicable laws and regulations
  - Implement data security and privacy policies, procedures, and training
- Know your data
  - e.g., personal, employee, consumer, proprietary
  - Understand and implement safeguards
- Know your risks
  - Insider threat (including inadvertent disclosure); vendors; suppliers; contractors; customers; and employees; bring your own device
  - Cyber attack
  - Physical threat and natural disasters

Minimizing the X-Factor: Navigating the Legal and Regulatory Landscape

- New laws; old proposals
- Regulatory enforcement
- Recent data breach court decisions
  - Split among courts as to whether there is actual injury/standing
  - Viability of state claims

U.S. Legislative Landscape

- Federal laws govern certain industries: e.g., HIPAA applies to healthcare sector
- Otherwise, no overarching federal cybersecurity/data breach notification law or cybersecurity standards
  - Congress considering data breach notification and cyber information sharing legislation
- Patchwork of 47 state laws, plus laws in DC, Guam, Puerto Rico, and the Virgin Islands



U.S. Legislative Landscape: State Laws

- In general, data breach = an event in which NAME + SS# or FINANCIAL INFO are accessible to unauthorized individual

- When a data breach occurs, data subjects must be notified and usually provided some explanation about incident
  - Notification to regulators: Indiana says notify AG
  - Most states require prompt notification: Indiana says without unreasonably delay (often interpreted as 30 days)

- The law that applies = law of the state where data subject resides
  - May or may not be state where company is headquartered
  - Often means company has to comply with 47+ different laws

U.S. Regulatory Landscape

- NIST Cybersecurity Framework
  - Not a regulation, but provides roadmap for regulators and industry to identify risk and defend against threats
- National Association of Insurance Commissioners
  - 12 cybersecurity principles for insurers to protect consumer information
- Securities and Exchange Commission
  - Issued guidance in 2011 on the disclosure of cybersecurity risks and incidents
- Federal Trade Commission
  - Has authority under Section 5 of FTC Act to investigate "unfair/deceptive acts or practices"
  - Pursues companies that don't keep promises made in privacy statements (this is deceptive)
  - Pursues companies that don't provide adequate security (this is unfair)

U.S. Regulatory Landscape: *FTC v. Wyndham*

- *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. 2015)
  - Arose out of security breach involving 619,000 customers, $10 million in fraudulent transactions
  - FTC sued Wyndham for failing to protect its customers
  - Wyndham moved to dismiss on ground that FTC failed to provide businesses with adequate notice of what constitutes "unfair" data security practices

  - Court: FTC has authority to take action against companies that employ poor IT security practices
  - FTC :
    - Every General Counsel should know what FTC is doing
    - Basic security deficiencies outlined in complaint—FTC guidance

U.S. Litigation Landscape

- Consumer class actions
- Suits by credit card companies, banks, and other issuing entities
- Shareholder derivative cases and securities litigation
  - Claims for breach of fiduciary duty, or even securities fraud; challenge conduct of officers/directors before & after breach
  - Lessons from case law
    - Regularly discuss data security/privacy at BoD meetings
    - Give BoD committee oversight of data security/privacy
    - Periodically have third-party consultants assess IT security; consider any deficiencies
    - Establish incident response team
    - Fully investigate any breach allegation

Minimizing the X-Factor: Incident Response

- Prepare
  - Engage management
  - Review/update policies and procedures
  - Develop incident response plan
  - Detection/prevention/insurance
  - Practice, Practice
- Respond
  - Execute response plan
  - Stop the bleeding
  - Take remedial action
  - Engage external experts—

  forensics, outside counsel, insurers

Minimizing the X-Factor: Incident Response

- Investigate
  - Find out who, what, how, when, and why
  - Identify compromised data
  - Determine obligation to notify
- Communicate
  - Internally—employees, management, advisors, affiliates, and BoD
  - Externally—insurance, law enforcement, regulators, elected officials, shareholders, affiliates, customers, and media
  - Assess potential liability, claims, or public safety issues
- Comply
  - Identify and comply with federal and state laws and regulations
  - Develop litigation response strategy

Minimizing the X-Factor: Review and Update Policies

- General Privacy
- Social Media
- Bring your own device
- Employee Monitoring
- Information Technology Usage
- Information and Physical Security
- Data Collection, Sharing, and Retention
  - Vendor agreements (e.g., data safeguards, responsibility to protect data, responsibility in event of a breach, compliance, liability considerations)
- Incident Response
- Training

Thank you!

Kathleen Rice, *Counsel*

+1 574-239-1958

kathleen.rice@FaegreBD.com

Leita Walker, *Partner*

+1 612 766 8347

leita.walker@FaegreBD.com

Rikke Dierrsen-Morice, *Partner*

+1 612 766 7655

rikke.morice@FaegreBD.com

Mike Ponto, *Partner*

+1 612 766 7420

michael.ponto@FaegreBD.com

FAEGRE BAKER DANIELS