About the Report

- Data breaches by industry and region
- Top cybersecurity causes and concerns worldwide
- Company and legal department budgets
- Cybersecurity insurance
- Lessons learned
- Managing vendors and outside risk
- Detailed glossary of information security terms
- Self assessment tool for benchmarking
- And much more…….

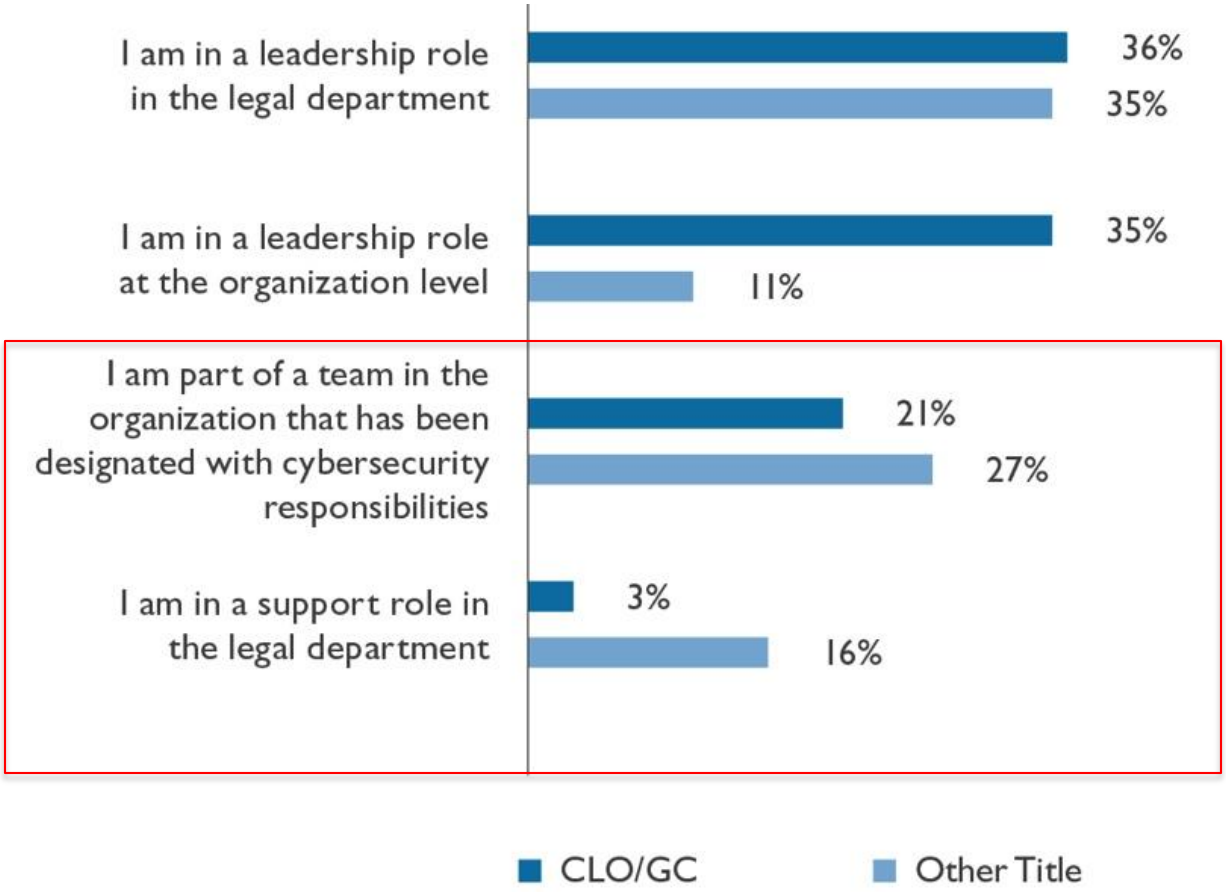
Source: *The State of Cybersecurity Report*

Ranking of Immediate Concerns Related to Data Breach

1. **Damage to reputation/brand**
2. **Loss of proprietary information**
3. **Economic damage**
4. Government/regulatory action
5. Business continuity
6. Litigation
7. Board (board of directors) concerns
8. Executive liability
9. Preservation of lawyer-client privilege
10. Media coverage
11. Shareholder activity

Source: *The State of Cybersecurity Report*

How Would You Characterize Your Responsibilities Regarding Cybersecurity in Your Company?



Source: *The State of Cybersecurity Report*

In-house Counsel Responsibilities Regarding Cybersecurity - Cyber Issues Generally

- **Understanding the importance of cybersecurity to your company:**
  - Use / storage of information regarding individuals – customers, vendors, employees
  - Importance of information security to your brand
  - Do you have valuable or sensitive proprietary data?
  - Are you a critical infrastructure provider or government contractor?
- **Assessment of the organizational structures and allocation of responsibilities**
- **Does the company have an adequate and appropriate incident response plan?**
- **Compliance with global privacy and data security laws, regulations and standards**
- **Does the company carry / need cyber risk insurance?**
- **Are the company's public disclosures on information risk appropriate?**
- **Do the company's internal and external privacy and information security policies and statements appropriately and adequately describe its information practices?**
- **Do the company's contracts with customers and vendors appropriately address cybersecurity?**

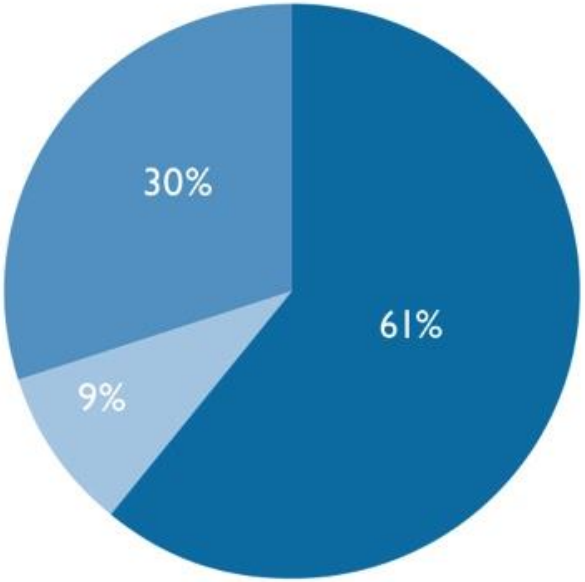
Source: Panelist perspective

In-house Counsel Responsibilities Regarding Cybersecurity - Incident Response

- **Incident Response Plan:**
  - Identify response team (internal and external) with contact list
  - Include provisions for consideration and invocation of privilege as appropriate
  - Incident identification and investigation procedures, including appropriate forensic processes
  - Process for determining if notifications are required
  - Notification plan
  - Communication plan
- **Understanding customer and vendor contract obligations**
- **Understanding security and notification compliance obligations:**
  - US Federal – GLBA, HIPAA, FTC, NRC, SEC
  - US State – privacy/consumer protection laws, breach notification laws
  - EU, Canada and other countries
  - Other – PCI, etc.
- **Establishing law enforcement contacts / relationships**
- **Invoking privilege / retaining outside counsel / litigation readiness**

Source: Panelist perspective

Member of the Legal Department on a Data Breach Team?



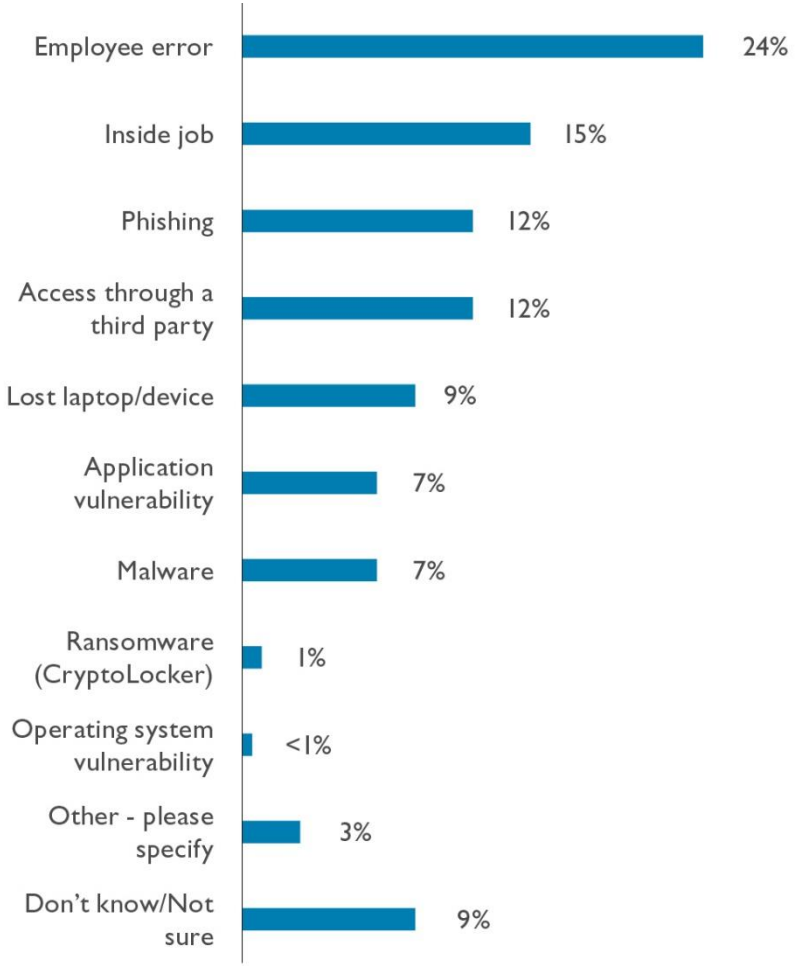
- Yes, I am or someone else is
- No department member on data breach response team
- Company does not have a formal data breach response team

Source: *The State of Cybersecurity Report*

31% of in-house counsel experienced a data breach

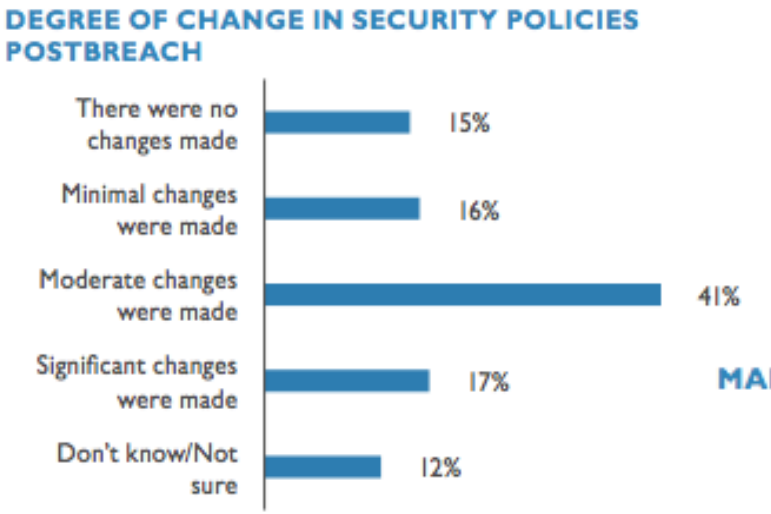
Source: *The State of Cybersecurity Report*

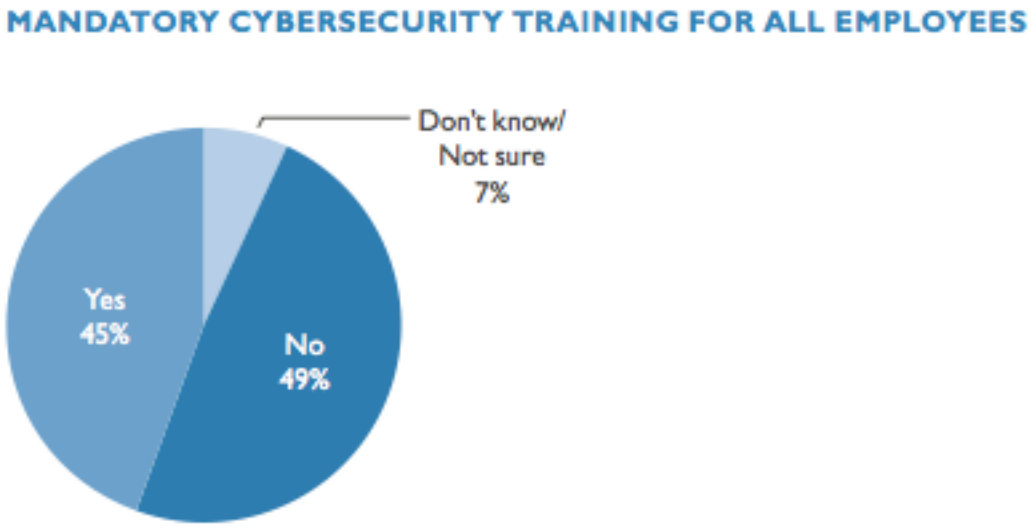
How Was the System Breached?



Source: *The State of Cybersecurity Report*

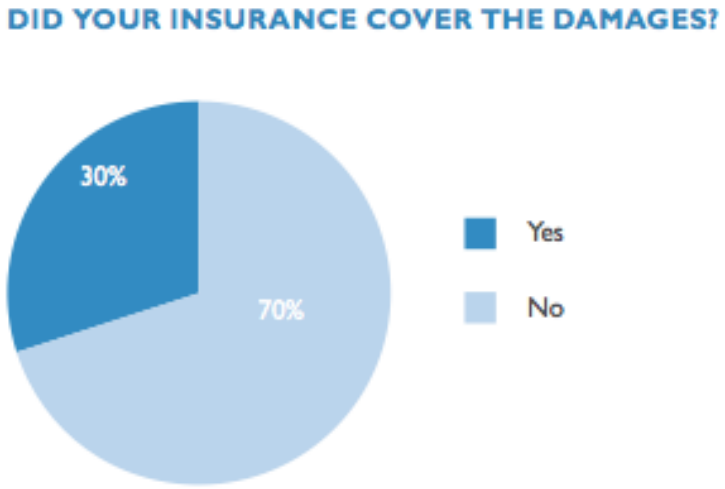
Key Trends Identified by the Report





Source: *The State of Cybersecurity Report*

Key Trends Identified by the Report



Source: *The State of Cybersecurity Report*

Highlight: Federal Trade Commission (FTC) Role in Cybersecurity

- **50+ enforcement actions in past 15 years relating to data security**
  - Mostly administrative actions
  - Mostly resolved through consent orders and long-term supervision
  - Other cases filed in federal court pursuant to injunctive authority
- **FTC enforcement authority primarily from Section 5 of FTC Act**
  - Also from Children Online Privacy Protection Act (COPPA); Gramm-Leach-Bliley (GLB) and Fair Credit Reporting Act (FCRA)
- **Section 5: "unfair" and "deceptive" trade practices**
  - **Deceptive** (historical & most common): challenge allegedly false data security representations (e.g. Fandango, Credit Karma)
  - **Unfair** (most recent): FTC's minimum cybersecurity standards for companies collecting personal information

Highlight: Federal Trade Commission (FTC) Role in Cybersecurity (Cont'd)

- **What's "unfair"**:
  - Failure to encrypt, establish log-in protocols, protect against commonly known attacks, and provide cybersecurity training…
- **Remedying violations through consent orders:**
  - Comprehensive information security program
  - Independent risk assessments
  - Periodic reporting back to FTC
- **Watch: Whether Third Circuit will curtail FTC authority**
  - *FTC v. Wyndham Worldwide Corporation*, et al., 2014 WL 2812049 (D.N.J.) – Interlocutory appeal before the Third Circuit

Highlight: Federal Trade Commission (FTC) Role in Cybersecurity (Cont'd)

- **FTC Recommendations -- 2012 Privacy Report**
  - Privacy by design
  - Simplified choice: Offer choices at a time and in the context in which consumer is making the decision
  - Transparency: Shorter, clearer privacy notices
- **Other recommendations –**
  - Use commonly used and readily available data security measures
  - Have a privacy policy in place
  - Review consumer assurances for alignment with actual security
  - Scrutinize data management often
  - Follow FTC complaints and consent decrees

Hypothetical

- FBI discovers personally identifiable information (PII) of your company's employees (including those in the UK) as well as 300,000 customers that has been posted on Pastebin
- FBI formally notifies your company and requests an on-site visit to further discuss the apparent breach
- On the same day the corporate anonymous hotline receives allegations of an insider possibly facilitating a data breach that may be linked to the FBI notification

What Should The Company Do To Prepare?

What do regulators expect?

- Cybersecurity Strategy and Framework
- Response Plan of Action
- Risk Management
- Continuous Monitoring
- Vigilance
  - Exercise
  - Incident Sharing

Source: Panelist perspective

What are some of the best practices of the companies represented on the panel and the audience?

Source: *© 2016 The Aerospace Corporation*

THANK YOU!

ACC FOUNDATION: THE STATE OF CYBERSECURITY REPORT

Price:

Members - $475

Non-Members - $595

www.acc.com/cybersecurity

Underwritten by:

Ballard Spahr LLP