GIBSON DUNN

Hot Topics in Securities and Governance

November 2017

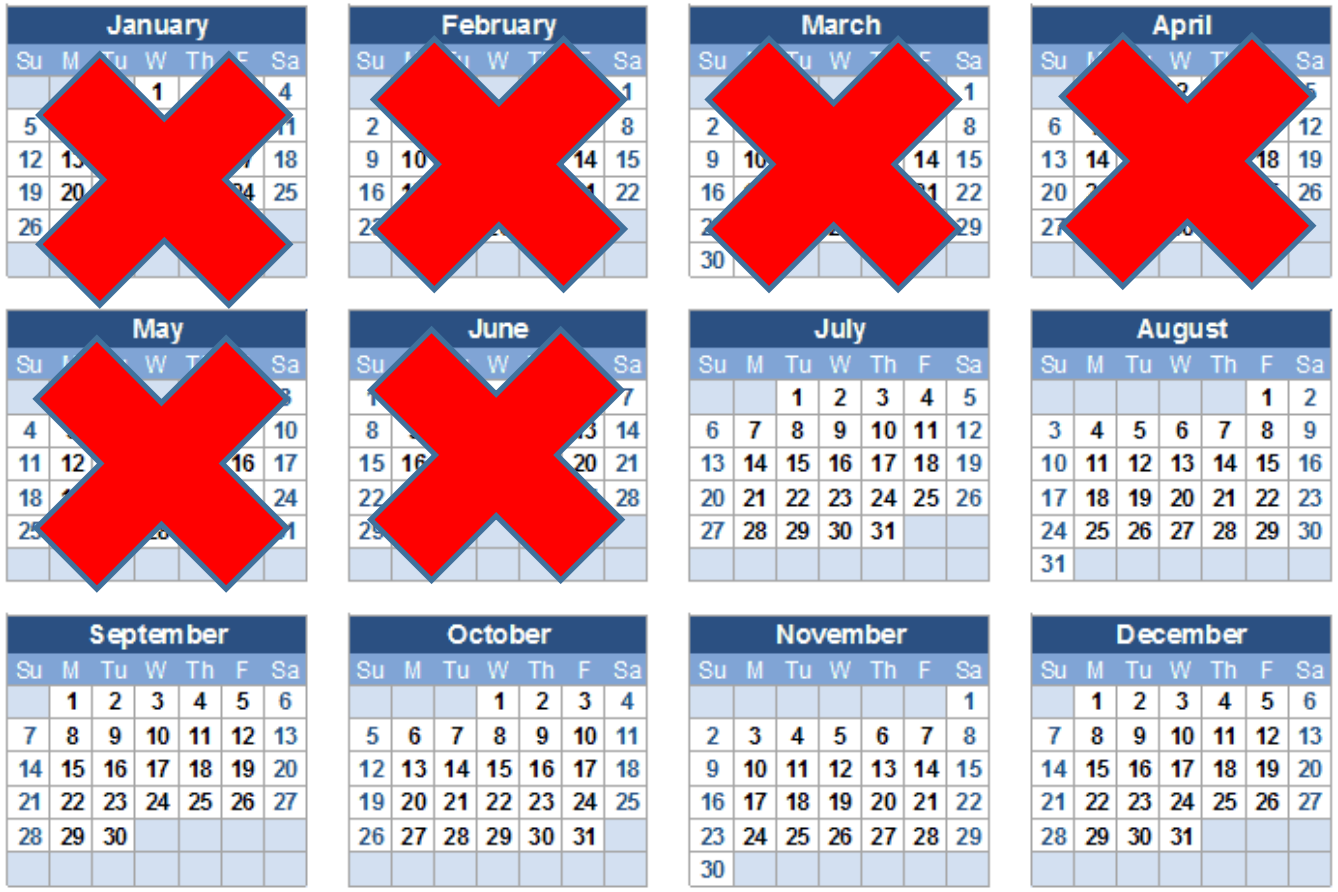
GIBSON DUNN

Cybersecurity Issues in an Evolving Landscape

In today's world, the question for companies
is not whether you have been hacked,
but whether you know that you have been or are being hacked.

Threat Landscape: Difficult to Detect

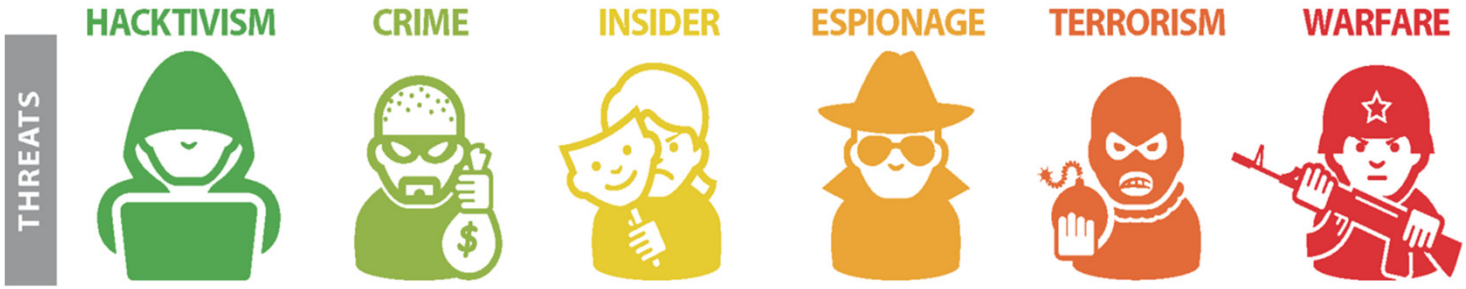
Average time for a breach to be detected in 2017: **191 days**



Source: Ponemon Institute - 2017 Cost of Data Breach Study

Threat Landscape: Varied Threat Actors

- Countries that pose the biggest threat:
  - Russia: most capable at hacking
    - Although Russian hacking efforts are focused on collecting military and diplomatic information, Russia remains committed to hacking business information that will enhance its competitive standing in the world.
  - China: very active in cyber realm
    - Key objective of Chinese cyber collection capability is to enable their state-owned enterprises to compete and dominate on a global economic level including through theft of intellectual property.
  - North Korea: growing player
    - May be hacking more to raise funds due to the depletion of funds from economic sanctions.



Threat Landscape: Insider Threat

- Nation-states aren't the only threat – 25% of data breaches in 2016 involved insiders.
  - 13% of 2016 breaches involved misuse of access privileges by insiders or trusted partners.
  - Employee training is key: 66% of malware infections in 2016 came from email attachments.
  - Data breaches caused by insiders are more likely to take months and years to discover.
- Third parties such as vendors and suppliers can be a significant source of risk.
  - A major retailer recently settled a class action related to a data breach that started when hackers used the retailer's HVAC vendor to access the retailer's internal network.
  - Limited oversight in this area: Only 38% of data risk managers in a 2016 survey agreed that the board was involved in ensuring vendor risk was assessed, managed, and monitored.

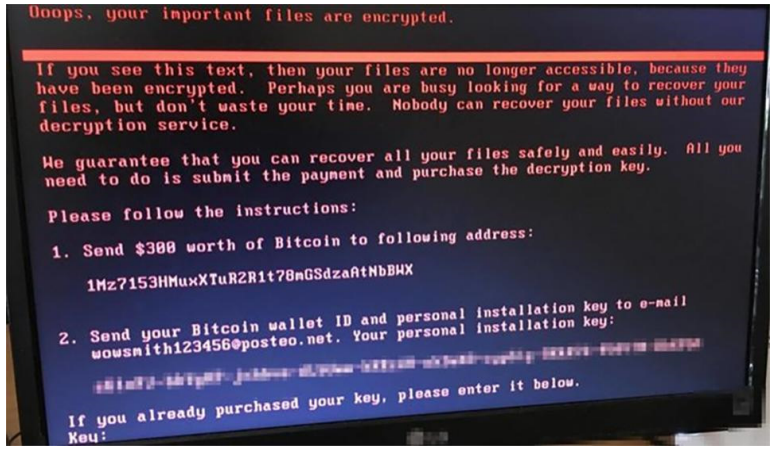
Threat Landscape: An Evolving Picture

- Likely continued focus on hacks to steal valuable information, such as intellectual property.
- As technology and security advance, countries will continue to devote resources toward cyber espionage and warfare.
- Increased focus in recent years on hacks using ransomware to raise money.
- More sophisticated tools and techniques, making breaches more difficult to detect.

THE WALL STREET JOURNAL.

High Petya Costs Will Catch Boards' Attention, Experts Say

Aug. 22, 2017 9:41 a.m. ET

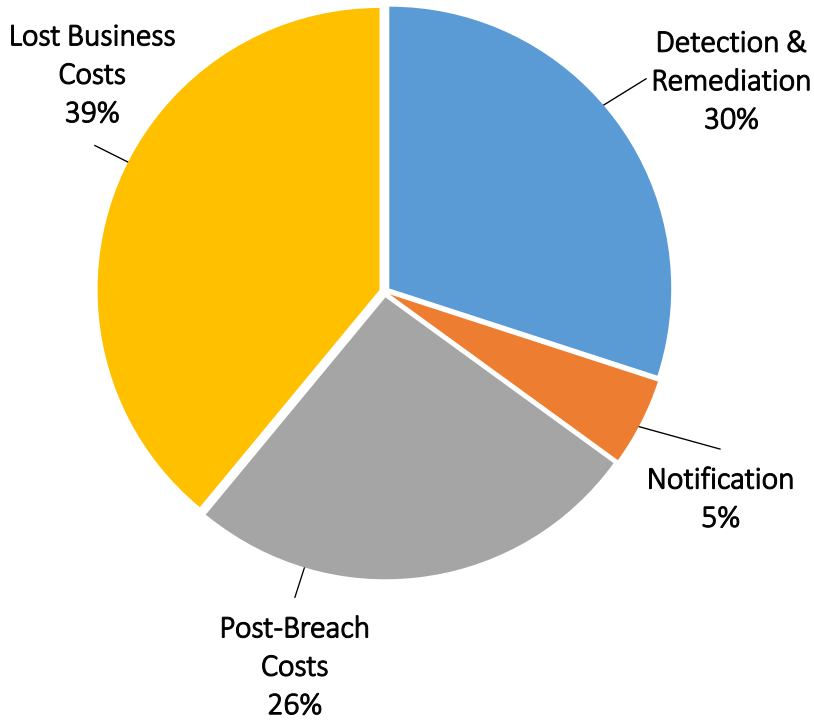


NotPetya Malware. Photo: Group-IB

Risks of Cyberattacks: Beyond Immediate Costs

- In a poll of consumers affected by data breaches, **11%** reported that they **stopped** dealing with the company who experienced the breach.
  - An additional **23%** reported giving **less business** to the company involved.
- Disruptive cyberattacks can cause ripple effects that **disrupt supply chains** for months.

Percentage of Data Breach Costs by Source, 2017



Ponemon Institute - 2017 Cost of Data Breach Study, Figures 14-17

Risks of Cyberattacks: Litigation and Investigations

- **Litigation:**
  - Consumer Class Actions
  - Lawsuits by financial institutions
  - Employee litigation
  - Derivative lawsuits
  - 10(b)(5) shareholder litigation
- **Broad and Far-Reaching Cybersecurity Investigations**

Case & Settlement Date	Settlement Details
Seagate Employee Class October 2017	**Up to $47.75 million** Up to $42 million for class member costs associated with the breach $5.75 million in identity theft protection Employee training
Anthem Consumer Class June 2017	**$115 million** paid into settlement fund Improvements to data security
Target Financial Institution Class May 2016	**Reportedly up to $125.5 million** Reportedly up to $67 million for Visa's claims Up to $20.25 million for class claims $19.108 million to MasterCard $19.189 in fees and costs

Average cost of settling class-action data breach litigation in 2016: **$44.7 million**, up from $5.8 million in 2015 → almost **8-fold increase**

Risks of Cyberattacks: Federal and State Enforcement

August 2017 settlement with a transportation company, requiring the company to strengthen its privacy and data security practices. The settlement includes audits by an independent expert for the next 20 years.

The SEC will likely refresh its 2011 guidance on disclosing cybersecurity incidents in the near future, potentially including a prohibition on officers and directors trading stock between discovering and disclosing a breach.
SEC Division of Corporation Finance Director William Hinman, 11/2017

"[T]he enforcement division [would not] 'rule out' bringing a case finding an issuer liable under circumstances where the company knew it had vulnerabilities and failed to disclose that to the public."
Co-Chief of SEC Enforcement Division Stephanie Avakian, 7/2017

Target: 5/2017, $18.5 million settlement with 47 AGs, including $1.4 million to California

Nationwide Insurance: 8/2017, $5.5 million settlement with 32 states & D.C.

Cybersecurity and Fiduciary Responsibilities: Overview

- Fiduciary duties are a fundamental principle of corporate law.
- Directors (and officers) owe duties of loyalty and care to the corporation.
- Under the *Caremark* principle, applicable law sets a high threshold for finding that directors breached their fiduciary duties by not providing adequate oversight.
  - Directors are liable only if plaintiffs can demonstrate "sustained or systematic failure of the board to exercise oversight."
    - *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959, 971 (Del. Ch. 1996).
- Most corporate decisions will be assessed under the business judgement rule:
  - Courts presume that the board's business decisions were made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company."
    - *Smith v. Van Gorkom*, 488 A.2d 858, 872 (Del. 1985).

Cybersecurity and Fiduciary Duties: Derivative Lawsuits

- The high standard for director liability under *Caremark* has not prevented derivative lawsuits against directors and officers following cyberattacks: at least six since 2015.
- Data breach derivative lawsuits naming directors and officers have alleged breaches of fiduciary duties and mismanagement based on a *failure to oversee* company policies and procedures.
- More recent cases against Equifax and Yahoo focus on alleged *disclosure* deficiencies.
  - Some plaintiffs have alleged failure to disclose cybersecurity risks prior to a cyberattack, as well as failure to timely disclose cyberattacks themselves.
  - Having policies regarding disclosure before a cyberattack and documenting disclosure-related decisions afterwards could help companies prepare for potential legal challenges.

Cybersecurity Best Practices: Benchmarking

- According to 2017 BDO USA Cyber Governance study:
  - 79% of directors are more involved in cybersecurity efforts this year than the last.
  - 78% of public company directors have increased company investments to defend against cyberattacks, with a 19% increase in budgets, on average.
  - 61% of companies have a cyberbreach or incident response plan in place.
  - 91% of directors are briefed on cybersecurity at least once a year.

Cybersecurity Best Practices: Lessons from Recent Litigation

- In a recent derivative litigation settlement, a major retailer agreed to change its cybersecurity corporate governance practices by implementing the following measures:
  - A Chief Information Security Officer with defined duties;
  - Cyber tabletop exercises;
  - Monitoring key indicators of compromise on computer network endpoints;
  - Searching for confidential company information via a dark web mining service;
  - An executive committee on data security;
  - Management reporting regarding IT spending on cybersecurity;
  - An Incident Response Team and Incident Response Plan; and
  - Participating in information-sharing agreements.

Cybersecurity Best Practices

- Additional best practices include:
  - Developing a business continuity plan to mitigate disruptive cyberattacks.
  - Building relationships with local and federal law enforcement.
  - Using a dashboard of quantitative metrics for the board to measure progress.
  - Adopting the NIST Framework for assessing cyber risk.
  - Commissioning an independent legal assessment of cybersecurity governance including a review of:
    - Cybersecurity response plans;
    - Board and management reporting procedures;
    - Employee training materials;
    - Third-party vendor assessment processes; and
    - Other aspects of cybersecurity governance.

GIBSON DUNN

Changes in Audit Reporting Model

PCAOB Audit Reporting Standard: *Background*

- On June 1, 2017, PCAOB adopted new standards for audit reports.
- SEC approved the new standard on October 23, 2017.

PCAOB
Public Company Accounting Oversight Board

The new standard (AS 3101) requires:

- Disclosures about Critical Audit Matters ("CAMs");
- Disclosure of the length of auditor tenure;
- A statement regarding auditor independence; and
- Disclosures intended to clarify the auditor's responsibilities.

PCAOB Audit Reporting Standard: *Background*

- CAM related disclosure requirements will become effective:
  - For large accelerated filers, for fiscal years ending on or after June 30, 2019
  - For all other companies, for fiscal years ending on or after December 15, 2020.
- The non-CAM related disclosure requirements will become effective for fiscal years ending on or after December 15, 2017.

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- CAMs are defined as:
  - matters arising from the audit of the financial statements that were communicated or required to be communicated to the audit committee and that:
    1) relate to *accounts* or *disclosures* that are material to the financial statements, and
    2) involve especially challenging, subjective, or complex auditor judgment.

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- PCAOB provided a non-exhaustive list of factors to consider in determining whether a matter involves challenging, subjective, or complex judgment, including:
  - The risk of material misstatement;
  - The application of significant judgment or estimation;
  - The nature and timing of unusual transactions;
  - The extent of specialized skill or knowledge needed in conducting the audit; and
  - The nature of audit evidence obtained regarding the matter.

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- Under the standard, if an auditor identifies a CAM, it must provide disclosure in the audit report that:

- Identifies the CAM;
- Describes the principal considerations that led to the determination;
- Describe how the CAM was addressed in the audit;
- Identify relevant financial statement accounts and disclosures that relate to the CAM.

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- CAM reporting presents challenges to companies, their audit committees, and their auditors, including:
  - Subjective determinations as to whether a matter qualifies as a CAM;
  - Potential disclosure of original information by auditors;
  - Concerns regarding timing – completion of the audit and review of draft CAM disclosures; and
  - Potential chilling in auditor/audit committee communications.

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- CAM disclosures may require an auditor to disclose original information that has not previously been disclosed by the issuer.

- PCAOB says that auditors should work with issuers to address matters without making original disclosures, but the standard permits original disclosures where it is "necessary to describe the principal considerations that led the auditor to determine that a matter is a critical audit matter or how the matter was addressed in the audit."

PCAOB Audit Reporting Standard: *Critical Audit Matters*

- Audit committees should engage with their auditors to prepare for the CAM reporting requirements.
  - Consider asking auditors about issues that have arisen in prior audits and that may be considered CAMs under the new standard;
  - Consider asking for draft disclosure or prepare draft disclosure and present it to them; and
  - Outline expected "ground rules," including timing.

GIBSON DUNN

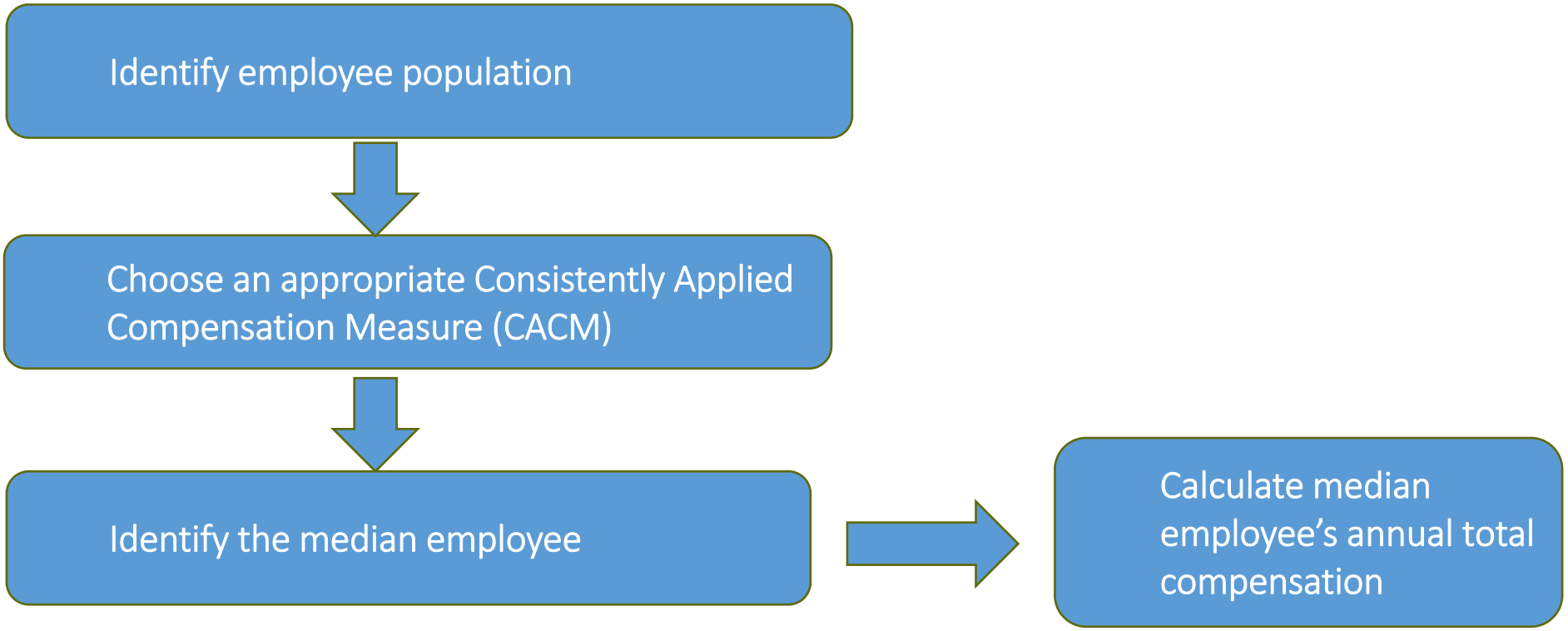
Pay Ratio Disclosure Requirements for 2018 Proxy Season

Pay Ratio in 2018 Proxy Statements

- The pay ratio rule was mandated by Section 953(b) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which became law in 2010.
- In 2015, the SEC adopted the pay ratio rule in Item 402(u) of Reg. S-K.
  - The rule requires the pay ratio to be disclosed in filings where Item 402 information is required for compensation in the first fiscal year beginning on or after January 1, 2017.
  - This means that for calendar year end companies, the pay ratio disclosure will first be required in their upcoming 2018 proxy statements. Companies with a fiscal year end other than December 31 have a delayed compliance date.
  - The pay ratio rule does not require disclosure for emerging growth companies, smaller reporting companies and foreign private issuers.
- In September 2017, the SEC issued interpretative guidance.
  - At that time, the Staff updated its C&DIs (first issued in October 2016).
  - The Division of Corporation Finance also provided guidance focusing on reasonable estimates, methodologies and statistical sampling.

Practical Application of the Rules

- In general, the pay ratio rule requires disclosure of: (1) the annual compensation of the median compensated employee, (2) the annual compensation of the CEO, and (3) the ratio of these two amounts.
- In order to provide this disclosure, companies engage in a step by step process:



Issues in Application

- Step 1: Identify the employee population
  - Determine employee population determination date
  - Address any independent contractors, furloughed employees
  - Decide whether to use exemptions to exclude employees(de minimis, acquisitions)
- Step 2: Choose an appropriate CACM
  - Consider which internal records to use
  - Determine which measure will reasonably reflect annual compensation and provide a reasonable alternative to annual total compensation
  - Determine which time period to choose
- Step 3: Identify the median
  - Determine how to gather compensation data for employees
  - Address outliers
  - Decide whether to annualize
  - Determine which estimates are reasonable and appropriate
  - Decide whether to use the cost of living adjustment
- Step 4: Calculate Annual Total Compensation for the Median Employee and the Pay Ratio
  - Consider whether to include health and other non-discriminatory benefits
  - Confirm documentation of important decisions in process and compliance with SEC guidance

How to Approach Disclosure

- Disclosure requirements
  - Annual total compensation of median employee, CEO, ratio
  - Date for employee population
  - CACM used
  - Brief description of methodology
  - If use exemptions, additional requirements
- Emphasize uniqueness of disclosure
- Importance of describing methodology
  - Statement that the pay ratio is a reasonable estimated calculated under SEC rules
  - Determine which assumptions and estimates should be disclosed
  - Reliance on internal records
  - Opportunity to distinguish your disclosure from other companies' disclosures
  - Consider describing aspects of median employee's annual total compensation and the median employee

Pay Ratio on the Board and Committee Agendas

Provide overview of what the pay ratio rule requires

- Explain the flexibility in the rule and the ability for the company to choose its own methodology

Explain the Company's methodology and the uniqueness of the Company's disclosure

- Explain which variables will cause median employee's pay to be higher or lower than peers' pay ratio

Provide overview of employee communications strategy

- Consider having HR present on this strategy and potential employee reaction

Explain how proxy advisory firms and key investors will view the pay ratio disclosure in 2018

- Focus on the Company's key investors and identify their approach to pay ratio

Employee Communications

Preparation of appropriate FAQs

- Consider describing the median employee and how you identified the median employee

Be ready to explain median employee's annual total compensation and meaning of ratio

- Consider explaining any health, 401(K), benefits for median employee

Coordinate with existing employee communication strategies

- Consider timing of disclosure, coordination and organization with HR

Shift focus *away from* pay ratio number itself and *to* your overall compensation practices and strategies to foster career growth

Investor Aspect – Separate Pay Ratio from Say on Pay

- Pay ratio adopting release states that the pay ratio "provides new data points that shareholders may find relevant and useful when exercising their [say on pay] votes".
- Recent de-emphasis on connection between pay ratio and say on pay
  - Say on pay vote is a vote on executive compensation – not on the gap in pay between the CEO and median employee
  - Emphasize disconnect through placement of disclosure in proxy statement outside of executive compensation sections
- Proxy advisory firm and investor views
- Importance of describing methodology and uniqueness of disclosure

GIBSON DUNN

Revenue Recognition Standard

Revenue Recognition Standard: *Background*

- In 2014, FASB and IASB jointly set out to develop a common revenue recognition standard across regions and industries.
- In May 2014, FASB released Accounting Standards Update No. 2014-09, Revenue from Contracts with Customers (Topic 606).
- The new revenue recognition standard will be effective for public companies for annual reporting periods beginning after December 15, 2017.

Revenue Recognition Standard: *The New Standard*

- The core principle of the new revenue recognition standard is that revenue should accurately depict the transfer of goods or services to customers in amounts corresponding to the consideration expected in exchange.
- Industry-specific standards will be eliminated, and all companies will be subject to the same uniform standar

Revenue Recognition Standard: *The New Standard*

- Companies are expected to follow a five step process:

  1) Identify the contract;

  2) Identify the obligations in the contract;

  3) Determine the transaction price;

  4) Allocate the transaction price to the obligations in the contract; and

  5) Recognize revenue when the obligations are satisfied.

Revenue Recognition Standard: *Transitional Considerations*

- SEC has required registrants to make disclosures regarding the process of transitioning to the new revenue recognition standard.
    - Companies should consider disclosing any issues arising during the implementation of the new standard as well as the expected impact of the new standard.
    - Most companies have not provided quantitative estimates of the impact of the new standard, but according to an October 2, 2017 Audit Analytics study, more than one-quarter of Russell 3000 companies have disclosed that at least one area of accounting is likely to change under the new standard.

Revenue Recognition Standard: *Important Considerations*

- Adoption of the new standard may require the implementation of new internal control processes and accounting systems, potentially triggering disclosure obligations under Item 308 of Reg. S-K.

- Implementation of the standard may result in meaningful changes to performance measures, especially in transitional years, which may impact debt covenants and compensation targets established prior to the implementation of the new standard.

- To the extent that implementation results in material changes to results of operations, the changes will need to be discussed in MD&A.

Revenue Recognition Standard: *PCAOB Guidance*

- PCAOB issued Staff Audit Practice Alert No. 15 in October of 2017 to provide guidance to companies and auditors in the process of implementing the revenue recognition standard.

- PCAOB reminded auditors that the new standard will require a deeper understanding of contractual arrangements and a close review of new controls and changes to existing controls.

- In particular, companies should be prepared to explain to their auditors any short-term processes implemented as stopgap measures before automated processes and controls can be fully implemented.

Recent Developments

SEC Releases New Shareholder Proposal Guidance.

On November 1, 2017, the staff of the Securities and Exchange Commission published

Staff Legal Bulletin No. 14I.

This was a significant development that we discuss in our recent client alert, available at: http://www.gibsondunn.com/publications/Pages/SEC-Staff-Issues-New-Guidance-on-Shareholder-Proposals.aspx

The Staff Legal Bulletin is available at: https://www.sec.gov/interps/legal/cfslb14i.htm

MCLE Information

- **The Handout.** Participants must download the PowerPoint as the handout for this webinar to comply with MCLE requirements. Click on "File" in order to "Save As" to your computer.
- **Sign-In Sheet.** Participants should download the MCLE Sign-In Sheet, complete it and email it to Jeanine McKeown.
- **Certificate of Attendance.** Most participants should anticipate receiving their certificate of attendance in 3 to 4 weeks following the webcast. (Virginia Bar members should anticipate receiving it in ~6 weeks following the webcast.)
- **NY Compliance.** Individuals seeking credit in New York can expect to hear the key word during the webinar.
- **Questions.** Direct MCLE questions and forms to Jeanine McKeown (her contact information is found on all MCLE forms provided):

Jeanine McKeown at 213-229-7140 or
jmckeown@gibsondunn.com

GIBSON DUNN

Professional Profiles

Lori I. Zyskowski

200 Park Avenue, New York, NY 10166-0193
Tel: +1 212.351.2309
LZyskowski@gibsondunn.com

Lori Zyskowski is a partner in Gibson Dunn's New York office and a member of the Firm's Securities Regulation and Corporate Governance Practice Group. Ms. Zyskowski advises public companies and their boards of directors on corporate governance matters, securities disclosure and compliance issues, executive compensation practices, and shareholder engagement and activism matters.

Ms. Zyskowski advises clients, including public companies and their boards of directors, on corporate governance and securities disclosure matters, with a focus on Securities and Exchange Commission reporting requirements, proxy statements, annual shareholders meetings, director independence issues, and executive compensation disclosure best practices. Ms. Zyskowski also advises on board succession planning and board evaluations and has considerable experience advising nonprofit organizations on governance matters.

Before joining Gibson Dunn, for over a decade Ms. Zyskowski served as internal securities and corporate counsel at several large publicly traded companies, including most recently at General Electric Company. Her in-house experience provides a unique insight and perspective on the issues that her clients face every day.

Ms. Zyskowski is a frequent speaker on governance, proxy and securities disclosure panels and is very active in the corporate governance community. She is a former member of the board of directors of the Society for Corporate Governance and served as the President of its New York Chapter from 2016-2017.

She graduated from Columbia University School of Law in 1996 and was a Harlan Fiske Stone Scholar. Ms. Zyskowski received her undergraduate degree from Harvard University.

Caroline D. Krass

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306
Tel: +1 202.887.3784
CKrass@gibsondunn.com

Caroline Krass, former Central Intelligence Agency (CIA) General Counsel, is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is Chair of the National Security Practice Group, and focuses on advising clients on the most complicated and sensitive matters involving national security, intelligence, cybersecurity, data privacy, government investigations, and regulatory issues. Ms. Krass served as a senior national security lawyer in the Obama and George W. Bush Administrations and is widely recognized for her expertise, both in Washington and abroad.

Ms. Krass is one of the most experienced national security lawyers in the United States. She has particular expertise in intelligence, privacy, surveillance, national security, economic sanctions, the Committee on Foreign Investment in the United States (CFIUS), cybersecurity, and government investigations.

Before joining Gibson Dunn in May 2017, Ms. Krass was appointed to be the General Counsel of the CIA by President Obama, and she served in that position from 2014 to 2017. In her role as General Counsel, she served as the agency's Chief Legal Officer, principal legal advisor to the CIA Director, and a trusted member of the Senior Leadership Team. Ms. Krass oversaw more than 150 attorneys and advised on complex, highly sensitive legal and policy issues, including cybersecurity and privacy, foreign investment in the U.S. and export controls, government investigations and litigation, crisis management and congressional relations. She served as the primary liaison with the White House Counsel and general counsels across the Executive Branch, as well as counterparts abroad, on national security legal and policy issues. From 2011 to 2014, Ms. Krass served as Acting Assistant Attorney General, and before that, Principal Deputy Assistant Attorney General, in the Office of Legal Counsel (OLC) in the Department of Justice. In these roles, she provided legal advice to the Attorney General, the White House Counsel, the National Security Council Legal Adviser, and senior officials at other executive branch agencies on a wide range of complex and significant constitutional, statutory, and regulatory questions relating to national security, cybersecurity, privacy, and foreign affairs, including matters involving foreign sovereign immunity, CFIUS, export control, economic sanctions, surveillance and use of force. At the President's request, Ms. Krass also led OLC in 2011.

Ms. Krass served as Special Assistant to the President for National Security Affairs in the Office of White House Counsel from 2009 to 2010. During this time, she dually served as the Deputy Legal Adviser to the National Security Council. She provided advice on a broad range of pressing and complicated domestic and international legal matters and interacted frequently with the general counsels and other senior lawyers in the Departments of Justice, Defense, State, and Homeland Security, the CIA, and the Office of the Director of National Intelligence. From 2007 to 2009, she served as a prosecutor in the U.S. Attorney's Office for the District of Columbia in the National Security Section.

Before that, she served as Special Assistant to the Department of the Treasury's General Counsel, as an Attorney-Advisor in the Office of the Legal Adviser at the State Department and as a Senior Counsel and Attorney-Advisor in OLC.

Ms. Krass received a BA with Honors from Stanford University in 1989, where she was elected to Phi Beta Kappa, and graduated in 1993 from Yale Law School, where she served as a Senior Editor of the *Yale Law Journal* and as a Coker Fellow. She clerked for Judge Patricia M. Wald of the U.S. Court of Appeals for the District of Columbia Circuit.

Michael J. Scanlon

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306
Tel: +1 202.887.3668
MScanlon@gibsondunn.com

Michael J. Scanlon is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. He is a member of the Firm's Securities Regulation and Corporate Governance, Securities Enforcement, and Corporate Transactions Practice Groups, and has an extensive practice representing U.S. and foreign public company and audit firm clients on regulatory, corporate governance, and enforcement matters.

Mr. Scanlon advises corporate clients on SEC compliance and disclosure issues, the Sarbanes-Oxley Act of 2002, and corporate governance best practices, with a particular focus on financial reporting matters. He frequently represents both accounting firms and public company clients on SEC and PCAOB accounting and auditing matters, including financial statement materiality and restatement issues, internal control issues, auditor independence, and other accounting-related disclosure issues. Mr. Scanlon has represented large accounting firms in enforcement investigations conducted by the SEC, PCAOB, and state accountancy boards. He also is experienced in conducting internal investigations involving accounting irregularities for management, audit committees, and other Board committees, and represents clients on these matters before the SEC. Mr. Scanlon also represents several public company boards of directors and audit committees, as well as not-for-profit organizations, with respect to corporate governance and other compliance matters.

Mr. Scanlon has served as Chair of the ABA's Law and Accounting Committee, Business Law Section, and as Chair of the DC Bar's Law and Accounting Committee. Mr. Scanlon currently serves as one of eight lawyers nationwide on the National Conference of Lawyers and Certified Public Accountants, a joint ABA-AICPA standing task force. He also is a member of the Society of Corporate Secretaries and Governance Professionals.

Mr. Scanlon also is a frequent speaker and author on securities regulatory and enforcement matters and corporate governance matters. In addition, he also appears as a speaker at continuing legal education programs for various clients. Mr. Scanlon has authored or co-authored more than thirty articles on securities regulatory, corporate governance, and enforcement-related matters.

Mr. Scanlon is admitted to practice in the District of Columbia and he is a member of the American Bar Association. He served as a law clerk to Judge Richard W. Goldberg of the U.S. Court of International Trade from 1997 to 1999. He received his law degree *cum laude* from the Georgetown University Law Center in 1997, where he was a member of the *Tax Lawyer*. He received his Bachelor of Arts degree from Middlebury College in 1992.

Maia R. Gez

200 Park Avenue, New York, NY 10166-0193
Tel: +1 212.351.2612
MGez@gibsondunn.com

Maia Gez is of counsel in Gibson Dunn's New York office and a member of the Firm's Securities Regulation and Corporate Governance Practice Group. Ms. Gez advises public companies and their boards of directors on a wide range of corporate law matters, including corporate governance, compliance with U.S. federal securities laws and the requirements of the major U.S. stock exchanges, board and executive compensation and pay ratio disclosure, and shareholder engagement and activism matters. Ms. Gez regularly assists in-house counsel, management, boards of directors and board committees on director independence, conflicts of interest, proxy statements and periodic reports, SEC and stock exchange reporting and disclosure requirements, disclosure controls and procedures and internal controls, auditor independence, insider trading and other company policies, shareholder proposals and responses to SEC inquiries. Her practice also focuses on new developments and evolving best practices in governance matters, as well as advising newly public companies on their public company obligations.

Prior to joining Gibson, Dunn & Crutcher, Ms. Gez was a member of the Public Company Advisory Practice at Simpson Thacher & Bartlett in New York. Ms. Gez is a member of the Society for Corporate Governance. She earned her Juris Doctor cum laude in 2007 from the New York University School of Law and her undergraduate degree magna cum laude and Phi Beta Kappa from Columbia University. Prior to law school, Ms. Gez was a journalist who reported for various publications from Israel.

Ms. Gez is admitted to practice in New York and California.

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2100 McKinney Avenue
Suite 1100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt am Main
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
1221 McKinney Street
Houston, TX 77010-2046
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0) 1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
São Paulo 04551-060
Brazil
+55 (11) 3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500