

A Discussion with the CAE

ICFR AND CYBER EVENTS FOCUS



Your Panel



PANELISTS

- CJ Schneller, SVP, General Auditor | Bank of America Merchant Services
- Terri Rogers, Chief Audit Executive | United Community Bank
- Emily Ormsby, Vice President of Internal Audit | Cousins Properties

MODERATOR

- Bradley Carroll, Principal | Frazier & Deeter, LLC

Polling Question



Do you work for a public company subject to SOX 404 and ICFR requirements?

- Yes
- No



Internal Controls Over Financial Reporting



Internal Controls Over Financial Reporting



U.S. SECURITIES AND
EXCHANGE COMMISSION

SEC Charges Four Public Companies With Longstanding ICFR Failures

- settled charges against four public companies for failing to maintain internal control over financial reporting (ICFR) for seven to 10 consecutive annual reporting periods. Two of the charged companies also failed to complete the required evaluation of the effectiveness of ICFR for two consecutive annual reporting periods.

- cannot hide behind disclosures as a way to meet their ICFR obligations. Disclosure of material weaknesses is not enough without meaningful remediation. We are committed to holding corporations accountable for failing to timely remediate material weaknesses."

Internal Controls Over Financial Reporting



- **Grupo Simec S.A.B de C.V.** disclosed material weaknesses in its annual filings for 10 consecutive years, from 2008 to 2017. In both 2015 and 2016, its management failed to complete the required ICFR evaluation. The company did not make significant progress in devising a control structure and remediating material weaknesses until after the SEC staff contacted it. The company continues to have material weaknesses that are being addressed through remediation. The Commission's [settled order](#) includes violations of Exchange Act Section 13(b)(2)(B) and Rules 13a-15(a) and 13a-15(c), thereunder, payment of a \$200,000 civil penalty, and an undertaking requiring retention of an independent consultant to ensure remediation of material weaknesses, including those involving related party transactions.
- **Lifeway Foods Inc.** disclosed material weaknesses in each of its Forms 10-K for a period of nine years, from 2007 through 2015, and significant deficiencies that in the aggregate constituted a material weakness in 2016. In both 2013 and 2014, company management failed to complete the required ICFR evaluation. Lifeway did not fully remediate its material weaknesses and conclude that ICFR was effective until its fiscal year ended December 31, 2017. Lifeway's failure to address its material weaknesses was compounded by three announced restatements since fiscal 2012, including two restatements announced during fiscal 2016. The Commission's [settled order](#) includes violations of Exchange Act Sections 13(a), 13(b)(2)(A), 13(b)(2)(B), and Rules 13a-1, 13a-15(a) and 13a-15(c), thereunder, and payment of a \$100,000 civil penalty.

Internal Controls Over Financial Reporting



- **Digital Turbine Inc.** disclosed material weaknesses in each of its Forms 10-K over a period of seven years, from fiscal year 2011 through fiscal year 2017. The company did not fully remediate its material weaknesses until the end of fiscal year 2018, as disclosed in its Form 10-K for the year ended March 31, 2018. The Commission's settled order includes violations of Exchange Act Section 13(b)(2)(B) and Rule 13a-15(a), thereunder, and payment of a \$100,000 civil penalty.
- **CytoDyn Inc.** disclosed material weaknesses in each of its Forms 10-K over a period of nine years, from 2008 through 2016. CytoDyn included in its public filings the same, nearly boilerplate, disclosure of material weaknesses for nine consecutive years. CytoDyn remediated its material weaknesses and determined that ICFR was effective as of May 31, 2017. The Commission's settled order includes violations of Exchange Act Section 13(b)(2) (B) and Rule 13a-15(a), thereunder, and payment of a \$35,000 civil penalty.

Internal Controls Over Financial Reporting



SEC Charges Company and Executives for Faulty Evaluations of Internal Controls

- The SEC alleges that MHR and two senior officers – former CFO Ronald Ormand and former chief accounting officer David Krueger – failed to properly evaluate and apply applicable ICFR standards and improperly concluded that MHR had no material weaknesses. The SEC also charged former MHR consultant Joseph Allred, and former MHR audit engagement partner Wayne Gray, with improperly evaluating the severity of MHR's internal control deficiencies and misapplying relevant standards for assessing deficiencies and material weaknesses. Accordingly, the public was not told that MHR had a material weakness in its ICFR.

Polling Question



Who in your company is responsible for monitoring enforcement action related to ICFR?

- CFO/CAO
- Head of Internal Audit/SOX
- External Auditor
- Other
- I Don't Know



Internal Controls Over Financial Reporting



Pipeline Construction Company Settles Charges Relating to Internal Control Failures

- announced that Primoris Services Corporation has agreed to settle charges that it failed to devise and maintain a sufficient system of internal accounting controls, and failed to adequately evaluate these control deficiencies when assessing the effectiveness of its Internal Control over Financial Reporting ("ICFR").
- The SEC's order finds that Primoris violated the record keeping and internal controls provisions of Sections 13(b)(2)(A) and (B) of the Securities Exchange Act of 1934 and Rule 13a-15(c) thereunder. Without admitting or denying the findings, Primoris consented to the entry of a cease-and-desist order and agreed to pay a \$200,000 civil penalty.

Internal Controls Over Financial Reporting



SOX SECTION 404: MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

All annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management assertion that internal accounting controls are in place, operational and effective.

Cyber Defense





[Credit Cards](#) [Checking & Savings](#) [Auto Loans](#) [Business](#) [Commercial](#)

[Search](#) [Support](#) [Locations](#) [Sign In](#)

[Overview](#) [FAQs](#)

Information on the Capital One Cyber Incident

Updated 9:30 PM ET, Sun Aug 4, 2019

What happened

On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products.

What we've done

Capital One immediately fixed the issue and promptly began working with federal law enforcement. The person responsible was arrested. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.

Cyber Defense



| COMPANY | DATE | CUSTOMER EXPOSURE |
|-------------|-----------|-------------------|
| Capital One | July 2019 | 100 Million |
| Equifax | May 2017 | 143 Million |
| Marriott | 2014-2018 | 383 Million |
| Facebook | 2016-2018 | 87 Million |
| Anthem | 2015 | 80 Million |
| Yahoo | 2013-2014 | 3 Billion |

Polling Question



How confident are you that your audit program provides adequate coverage of cyber security risks?

- Very Confident
- Somewhat Confident
- Not Confident
- I Don't Know



Cyber Defense



LILY HAY NEWMAN SECURITY 04.23.18 08:55 PM

ATLANTA SPENT \$2.6M TO RECOVER FROM A \$52,000 RANSOMWARE SCARE

Attackers, who infected the city's systems with the pernicious SamSam malware, asked for a ransom of roughly \$50,000 worth of bitcoin.

Destructive Malware Attacks Up 200% in 2019

Organizations hit with destructive malware can lose more than 12,000 machines and face \$200 million or more in costs, IBM X-Force reports.

DARKReading

Polling Question



Are you using a cloud software that stores confidential or personal data for your company or clients?

- Yes
- No



What Risks Does the Cloud Add?





QUESTIONS?

