Cyber-*Liability for the* C-Suite:

Mitigating the Risks of Senior Management (and Potentially Directors) Being Held Personally Accountable for Data Breach Incidents

*By Charles R. Ragan and Martin T. Tully**

Introduction

In the field of data protection and cybersecurity, there are Givens and there are Probabilities. Among the Givens are that information has value and that bad actors will continue to attack organizations that are rich in data. Another Given is that laws and regulations that set penalties for organizations and individuals if personal data is lost in a cyberattack have expanded recently, and it is probable that litigation stemming from and relating to data breaches will escalate in this and coming years.

In 2022, two cases eliminated all doubt that the C-suite was not exempt from personal accountability for inadequate data protection and security measures. And it is highly probable that regulators and counsel for consumers will target and seek to hold senior management accountable for security lapses that expose personal information.

There are a variety of tactics and techniques to reduce (but not eliminate) the probability and impact of a successful cyberattack. This article discusses a different issue – the evolving risks to senior management and potentially even directors of being held personally accountable in the event of a successful cyberattack – and explores some strategies to mitigate those risks.

I. Recent Cases Assessing Personal Responsibility for an Organizational Data Breach

The Cover-up Is Sometimes Worse Than The Crime

In October 2022, a federal jury convicted Joseph Sullivan, the former Chief Security Officer of Uber, of obstructing Federal Trade Commission (FTC) proceedings and misprision of felony. The facts were extreme, and some might be inclined to dismiss the case as one of bad facts making sensationalized law.

The evidence at trial established that Sullivan participated in a presentation to the FTC in March 2016 about a then-recent hack and testified in November 2016 before the FTC about that incident and Uber's data security practices. Ten days after that testimony, Sullivan learned of another hack of Uber involving

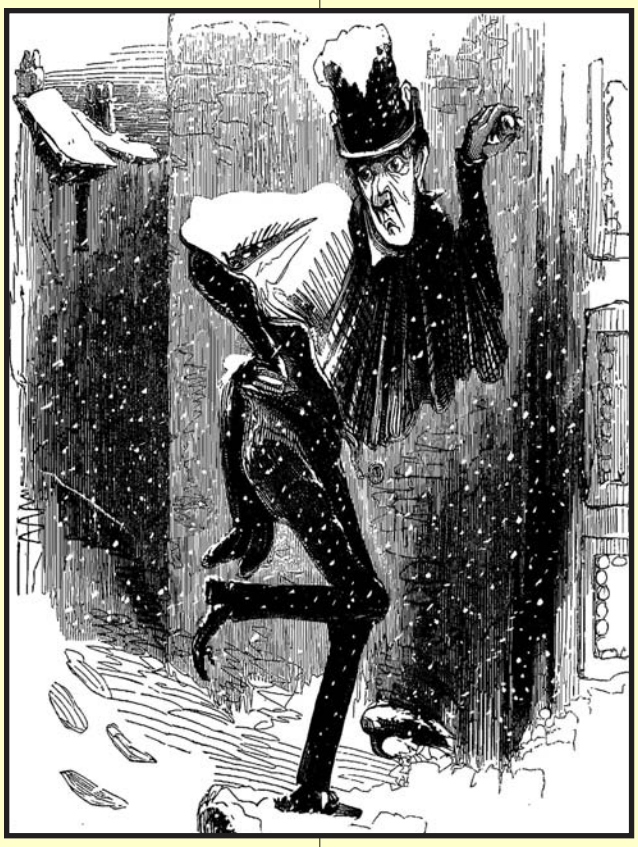
Continued on page 29

* *Charles R. Ragan is Of Counsel with Gunster, a Florida-based law firm. Martin T. Tully is a Partner with Redgrave LLP in its Chicago office.*

Cyber-*Liability for the* C-Suite

Continued from page 28

records of approximately 57 million Uber users. In response to the second hack, Sullivan, who was an attorney, had served as a federal prosecutor, and was a founding member of the Computing Hacking and IP Unit in the Northern District of California, did not alert federal authorities as required. Instead, while Sullivan's team's analysis of the second breach included a comment that it "may also play very badly based on previous assertions" to the FTC, Sullivan told his team that they needed to keep information about the second hack tightly controlled and that they should act as if their investigation did not exist.



Sullivan also arranged to pay the hackers a $100,000 ransom and have them sign nondisclosure agreements promising that they had not and would not disclose anything about the company's technology vulnerabilities. The court in January 2023 denied Sullivan's motion for acquittal or a new trial.[1] He faces a maximum of five years in prison for the obstruction charge, and a maximum three years in prison for the misprision charge.[2]

A Sobering Outcome For Drizly's CEO

The second recent case involving personal accountability in the C-suite was the FTC proceeding involving Drizly, LLC, an online company that facilitates the delivery of alcohol from local retailers to customers, and its CEO, James Cory Rellas ("Rellas"). In that proceeding, the FTC alleged that the company's security failures led to a data breach exposing personal information of about 2.5 million consumers, and that Rellas "formulate[d], direct[ed], or control[led]" the policies and practices of Drizly.

The matter concluded in January 2023 with the entry of a consent Decision and Order with the usual non-admissions but imposing extensive obligations requiring the company to maintain a comprehensive information security program, have biennial information security assessments from an independent third party, limit data retention, file periodic compliance reports and annual certifications, and keep certain records for 20 years.

The consent decree also requires Rellas to file compliance reports – even if he leaves Drizly. Moreover, the consent decree obligates Rellas for 10 years to ensure that any business of which Rellas is a majority owner, or functions as a CEO or other senior officer with direct or indirect responsibility for information security have a comprehensive information security program equivalent to that mandated in the decree.

Ill Winds Blow For Some Officers and Directors

A third recent case seeking to hold officers and directors liable stemmed from the cyber breach at SolarWinds Corporation that occurred when the Russian Foreign Intelligence Service injected a malicious code into the company's software, which impacted approximately 18,000 Solar Winds customers. The breach was discovered in late 2020. Securities class actions alleging fraud and naming CEO Kevin B. Thompson and Chief Information Security Officer (CISO) and VP for Security Architecture Timothy Brown ensued and were consolidated in the Western District of Texas. The complaint alleged that defendants made materially false and misleading statements about SolarWinds' cybersecurity measures, including the company's efforts to ensure the security of its software products and customers' data.

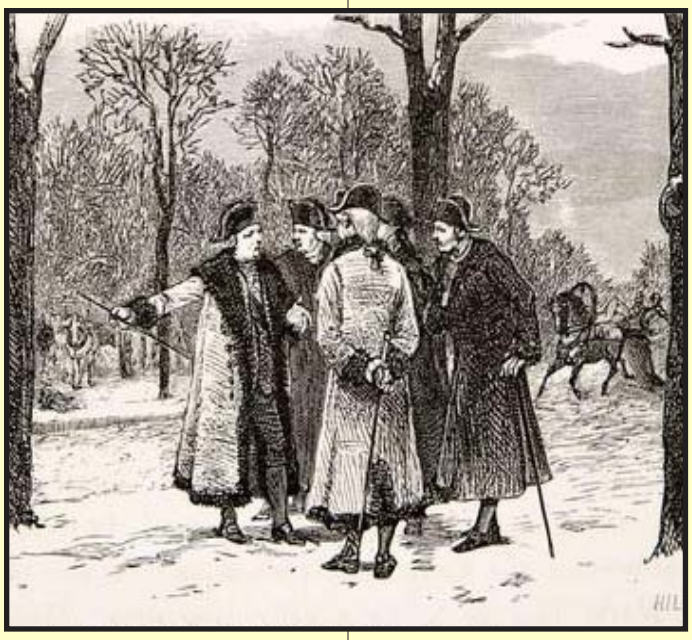
In March 2022, the court found that plaintiffs had failed to allege Thompson's scienter but allowed the case to proceed against other defendants, including the CISO. A proposed $26 million settlement

Continued on page 30

Cyber-*Liability* *for the* C-Suite

Continued from page 29

has been preliminarily approved with a final hearing scheduled for July 28, 2023.[3] In an 8-K filing with the SEC filed November 3, 2022, the company stated its expectation that the settlement payment would be funded entirely by applicable directors' and officers' liability insurance.



In the same 8-K filing, however, the company announced that, on October 28, 2022, the enforcement staff of the SEC provided SolarWinds with a "Wells Notice," stating that the staff had made a preliminary determination to recommend an enforcement action against the company alleging violation of the securities laws with respect to its cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures.

Also, a separate derivative action was filed in Delaware state court naming Thompson and 12 SolarWinds directors, alleging they failed to exercise their oversight duties so as to avert the breach – a so-called *Caremark* claim, stemming from a 1996 Delaware case.[4] The Vice Chancellor dismissed the SolarWinds derivative complaint in September 2022, finding that plaintiffs had failed to present credible allegations that defendants allowed the company to violate the law or ignore any red flags indicative of scienter. Rather, the court noted that the company had established two subcommittees of the board of directors with responsibility for overseeing corporate governance risks including cybersecurity, one of which received a cybersecurity briefing in February 2019.[5]

The derivative plaintiffs have appealed to the Delaware Supreme Court, arguing in part "[t]he nominal delegation to board committees of oversight concerning a 'mission critical' risk does not constitute a 'reporting system' if neither of those committees actually do anything for years on end" and that the board as a whole "did absolutely nothing to monitor or ensure reporting on cybersecurity issues."[6]

In support, they relied upon the 2019 Delaware Supreme Court opinion in *Marchand v. Barnhill,* which stemmed not from a cybersecurity incident but from a listeria outbreak at an ice cream company. There the Supreme Court reversed a Chancery Court dismissal, stating that a *Caremark* claim could succeed "when 'the directors [completely] fail[ ] to implement any reporting or information system or controls[,] or … having implemented such a system or controls, consciously fail[ ] to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.'" 212 A. 3d 805, 821.

Similar arguments led to a 2021 Delaware court-approved settlement requiring Boeing to make a $237.5 million payment and adopt corporate governance enhancements. In that case, the claim was that the Boeing board of directors had failed in its oversight responsibilities regarding the mission-critical aircraft design and development aspects of Boeing's business.[7]

* * *

These recent cases heighten the probability that future cases will allege boards should be held accountable for failure to perform appropriate oversight responsibility over mission-critical cybersecurity measures, and the possibility that courts may impose such liability.

Perhaps more significant, given the extent to which imminent new state and federal regulations and newly revised international standards (which we discuss below) increase senior management's responsibility for adequate cybersecurity protections, it is possible that courts may look to the recent developments as establishing a standard of care and impose liability based on failure to meet legal obligations and not the higher burden required to prove a *Caremark* claim.

Continued on page 31

Cyber-Liability for the C-Suite

Continued from page 30

II. New Regulations and International Standards Present New Risks for Organizations and Senior Management

State Legislation and Regulations

We have written elsewhere about comprehensive data protection and cybersecurity legislation enacted in five states and corresponding regulations taking effect at different times during 2023.[8] More states are expected to follow suit. Some of these statutes include rights of private action, so litigation alleging failure to meet the requirements of these laws and the regulations adopted under them – and naming senior management – is possible if a cyber incident results in the exposure of personal information.

At least one of the regulations expected to take effect in 2023 will increase the scope of an organization's required cybersecurity oversight. Specifically, California's Privacy Protection Agency will require that an organization enter into new agreements – having specific provisions – with service providers and contractors to which personal information the organization collects is disclosed and take reasonable and appropriate steps to ensure that those providers and contractors adhere to the revised act, which may include permitting scans of the provider's systems, assessments by an independent third party, and operational testing every 12 months.[9] In February 2023, the agency requested public comment on content to be included in further regulations it may issue regarding such monitoring activities.

NYS Department of Financial Services Regulation

Among regulations of administrative agencies scheduled to take effect this year are those of the New York State Department of Financial Services, whose authority extends broadly to all entities with a New York state license under banking, insurance, or financial services laws. As proposed, the regulations would require each covered entity to implement and maintain a written policy or policies, approved at least once annually by a senior officer or the company's board or an appropriate committee thereof, setting forth the entity's policies and procedures for the protection of its information systems and nonpublic information stored on those systems. The policies and procedures must be based on the entity's risk assessment covering more than a dozen specified items.

Specific duties are imposed on a CISO (*see* 23 NYCRR 500, section 500.4) and, if the entity has a board of directors or equivalent, the board (or an appropriate committee) must exercise oversight of and provide direction to management on the entity's cybersecurity risk management, require the development, implementation, and maintenance of a cybersecurity program, and have sufficient expertise and knowledge (or advice from qualified persons) to exercise oversight over cybersecurity risk management.

Cybersecurity programs must ensure a complete, accurate, and documented asset inventory to include a method to track information for each asset covering owner, location, classification of sensitivity, support expiration date, and recovery time requirement (section 500.13), a detailed business continuity and disaster recovery plan (section 500.16(a)(2)), and notification of certain cybersecurity events which must be given **no later than 72 hours** from determination of the occurrence (section 500.17(a)). Some observers have posited that other agencies will issue similar regulations.

SEC Regulations

The most highly anticipated (and broadly applicable) regulations to take effect in 2023 are the SEC's revised regulations regarding cybersecurity disclosures required of public companies. The SEC proposed those rules in March 2022 (and in February 2022 published rules applicable to registered advisers and funds). Final action on both of these proposals is expected in April 2023.[10]

Some early articles about the proposals pertaining to public companies focused on the requirement to file an SEC Form 8-K **within four business days** after a company determines that it has experienced a material cybersecurity incident (where cybersecurity incident is broadly defined). Public companies will also have to submit an 8-K if and when cybersecurity incidents become material in the aggregate.

More pertinent for current purposes, the proposals expand on the substance of cybersecurity disclosures that an organization must make in 10-Ks and 20-Fs, to include (among others):

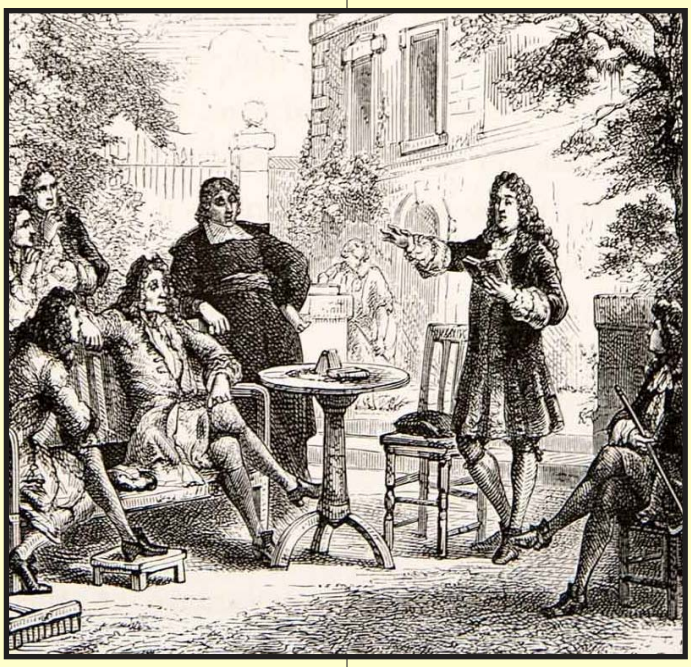
- Whether the company has policies and procedures: to identify and manage cybersecurity risks and threats (including operational risk,) and for risk assessment

Continued on page 32

Cyber-*Liability* *for the* C-Suite

Continued from page 31

of third-party service providers (including cloud providers), incident response, disaster recovery, and improvements in response to incidents;



- Whether the company engages assessors or other third parties in connection with any cybersecurity risk assessment program and whether it has policies and procedures to oversee and identify cybersecurity of third-party providers that have access to the organization's employee or customer personal information;
- Management's expertise in cybersecurity issues, including its role in assessing risk and implementing appropriate policies and procedures;
- Details on the organization's chief information security officer and internal lines for communications with the CISO;
- Whether, how, and how frequently the board is informed of and considers cybersecurity risks, and how those risks relate to or may impact the organization's business strategy, financial outlook, or financial planning; and
- Identification of board members with cybersecurity expertise with "such detail as necessary to fully describe the nature of the expertise." The proposed rules also include factors potentially applicable regarding whether a board member has cybersecurity expertise.

These revised regulations clearly portend that the agency will scrutinize the roles of senior management – including particularly the CISO if there is one – with regard to cybersecurity protections when it investigates a company following a cybersecurity breach that exposes personal information of the company's customers or employees.

Updated ISO 27001 regarding Information Security Management Systems

One final recent development that may have considerable impact on future court and regulatory actions seeking to hold senior management (and board members) accountable for inadequate data protection and cybersecurity policies and procedures was the October 2022 update to ISO 27001. While companies seeking ISO 27001 certification need not have in place until 2025 all the new controls included in this standard, it is probable that the adequacy of cybersecurity oversight will soon be measured against the standard if for no other reason than that ISO "was founded with the idea of answering a fundamental question: 'what's the best way of doing this?'"[11]

The revised standard adds controls for managing data in the cloud, data masking, enhanced monitoring, and deleting information to align with data minimization requirements. As with its predecessor, revised ISO 27001 requires top management, which the parent ISO 27000 defines as the "person or group of people who directs and controls an organization at the highest level," to review the organization's information security management system (ISMS) at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.

The revision adds a requirement that top management's review include consideration of changes in the needs and expectations of interested parties relevant to the ISMS, which the parent ISO 27000 defines as persons or organizations "that can affect, be affected by, or perceive [themselves] to be affected by a decision or activity."[12]

I. Takeaways from Recent Developments

The new state and agency regulations, and the revised ISO 27001 align around an important phenomenon: the evolution and explosion of organizational use of cloud service providers to store important personal information that organizations collect.

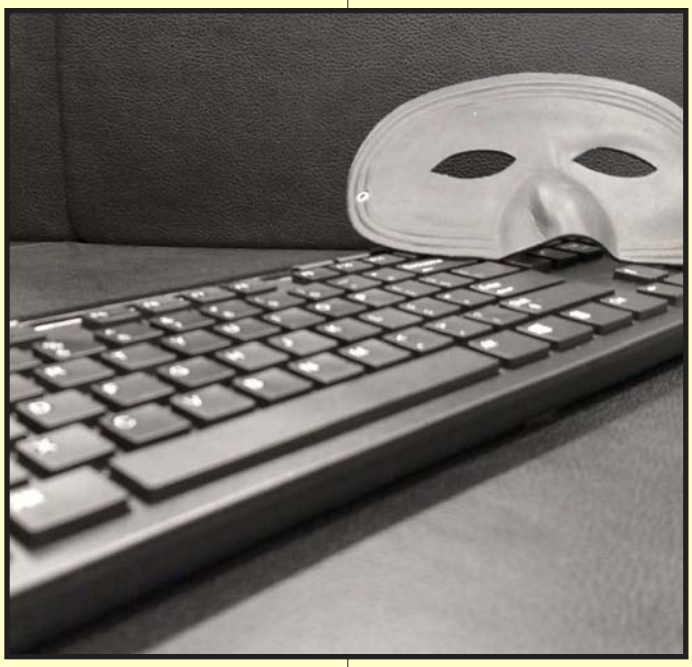
All these recent pronouncements recognize and require that an

Continued on page 33

Cyber-*Liability* *for the* C-Suite

Continued from page 32

organization's data protection and cybersecurity policies and procedures should be extended to cloud service providers and third parties holding the personal information an organization collects. They also dictate data minimization, and expect that senior management (including boards of directors) will take steps to ensure the organization implements, monitors, and maintains a comprehensive data protection and security program with appropriate improvements over time.



These expectations are extensive. If a cyber incident results in exposure of customer or employee personal information, members of senior management and in some cases directors may expect that private parties or regulators will seek to hold those senior personnel accountable for the security failures. And, as the *Drizly* order demonstrates, the remedies imposed may follow the executives for many years. Lastly, officers and directors should not assume insurance will cover such risks: As the CEO of Europe's Zurich Insurance recently observed, as cyberattacks grow, they will become "uninsurable."[13]

II. Strategies to Mitigate the Increasing Risks of Personal Liability

There are several strategies an organization may consider and pursue now to mitigate these risks. For example, to achieve compliance with the recent spate of state legislation and prepare to make rapid notifications regulators will require, an organization could:

- Conduct an **assessment** to determine the systems (on-premises and in the cloud or with other contractors) that hold personal information the organization collects and evaluate vulnerabilities and controls of those systems;
- Evaluate the organization's current state of its data protection and security policies and procedures in comparison to what these recent developments require, and the comprehensive program mandated in the *Drizly* order;
- Update policies and procedures as appropriate in light of the evaluative comparison; and
- Provide cybersecurity awareness training for all personnel as well as training about the organization's data protection and security.

To prepare to meet the quick-notification requirements of the new regulations, an organization could:

- Develop (or update as appropriate) a Playbook for responding to a cybersecurity incident, and include among other things clear duties and responsibilities, decision and notification trees, and timelines for all steps in the response; and
- Provide enhanced training including tabletop exercises for all personnel with responsibilities for responding to a breach, including senior management.

To help mitigate the risk of senior management or directors being held individually accountable for the consequences of data breaches, the organization should:

- Identify who among senior management and on the board of directors (or equivalent) has expertise in cybersecurity measures or look to add or affiliate with a resource with such expertise;
- Clearly define within the organization which individuals have what responsibilities for developing, implementing, monitoring, and maintaining the information security system, and who has oversight responsibilities;

Continued on page 34

Cyber-*Liability* *for the* C-Suite

Continued from page 33

- Ensure that the board of directors (or equivalent) receives regular briefings on cybersecurity risks and requirements and the organization's policies and procedures for meeting its legal obligations with respect thereto;

- Task one or more board committees with responsibility for overseeing the organization's data protection and cybersecurity policies and procedures, and for reporting to the board as a whole periodically on cybersecurity issues;

- Stay abreast of relevant trends and developments in the cybersecurity space with an eye toward reasonably tracking to industry standards; and

- Review directors' and officers' insurance policies to ensure that cyber risk exposure is adequately addressed. Insurers can also incentivize better cybersecurity measures by pricing policies based on the effectiveness of cybersecurity programs.

* * *

For more information on the matters discussed in this article, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.

Notes:

[1] 3:20-cr-00337-WHO, Dkt. No. 250 (N.D. Cal. Jan. 11, 2023)

[2] *See* https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.

[3] Dkt. 102, Case 1:21-cv-00138-RP, filed Feb. 7, 2023.

[4] *In re Caremark Int'l Inc. Derivative Litig.,* 698 A.2d 959, 967-68 (Del. Ch. 1996).

[5] *Construction Industry Laborers Pension Fund v. Bingle,* Case No. 2021-0940, 2022 WL 4102492 at *3-4 (Del. Chan., Sept. 6, 2022) (unpublished).

[6] https://www.law360.com/articles/1562965/solarwinds-shareholders-challenge-toss-of-data-hack-suit.

[7] https://www.law360.com/articles/1467870/chancery-oks-record-237-5m-boeing-737-max-damage-deal.

[8] *See* https://www.redgravellp.com/consumer-privacy-laws-taking-effect-2023.

[9] §7051(a)(7) of the regs. Cal. Code Regs., title 1, §7051(a)(7).

[10] *See* https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=3235-AM89 and https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=3235-AN08.

[11] *See* https://www.iso.org/benefits-of-standards.html.

[12] For more information about the revised ISO 27001, see "Updated ISO Standards Require Enhanced Information Governance."

[13] *See* https://www-pymnts-com.cdn.ampproject.org/c/s/www.pymnts.com/cybersecurity/2022/zurich-insurance-ceo-cyberattacks-will-be-uninsurable/amp/.

Upcoming Board *of* Governors' Meetings

Upcoming meetings of the Board of Governors of the Seventh Circuit Bar Association will be held on:

Friday, September 8
4 P.M. Central