# Cyber Coverage Aftermath: Uber and Drizly Cases

When it comes to cybersecurity, C-suites have long wrestled with the appropriate oversight and incident response. The days of those decisions being shielded by organizational responsibility may be ending. Regulators and prosecutors are increasingly turning their attention toward company executives when cybersecurity is believed to have been mishandled.

On Oct. 5, 2022, a California federal jury found the former chief security officer of Uber Technologies, Inc. guilty of criminal obstruction and misprision for failing to report a 2016 cyber intrusion affecting 57 million Uber users and 600,000 driver license numbers. The case is believed to be the first time a company executive has faced criminal prosecution for failing to disclose a data breach to federal authorities.

The government said the former chief security officer spearheaded a cover-up, including hiding the breach from Uber management and the Federal Trade Commission (FTC), which was investigating Uber's cybersecurity practices at the time. In a news release following the verdict, U.S. Attorney Stephanie Hinds said, "We will not tolerate concealment of important information from the public by corporate executives more interested in protecting their reputation and that of their employers than in protecting users. Where such conduct violates the federal law, it will be prosecuted."[1]

Less than three weeks later, on Oct. 24, 2022, the FTC announced an action against Drizly, the online alcohol marketplace, and its CEO stemming from alleged security failures that led to a data breach exposing the personal information of about 2.5 million consumers.[2] Drizly and its CEO allegedly were alerted to problems with the company's data security procedures before the breach but failed to adequately address them – all the while claiming appropriate security measures were in place. The FTC's proposed order contains a litany of security-related obligations for Drizly spanning 20 years and saddles the CEO with personal obligations that will follow him for a decade, including to other companies.[3] In a news release accompanying the proposed order, the Director of the FTC's Bureau of Consumer Protection Samuel Levine said, "Our proposed order against Drizly not only restricts what the company can retain and collect going forward but also ensures the CEO faces consequences for the company's carelessness. CEOs who take shortcuts on security should take note."[4]

A logical question for directors and officers is whether their Cyber Liability and/or Directors and Officers (D&O) policy will extend coverage for these types of claims. Cyber insurance typically will not cover the *personal* liability of directors and officers following a cyber incident. This type of coverage usually is provided in D&O insurance. However, to better protect a business against the financial consequences of cyber incidents, McGriff recommends investing - at a minimum - in both Cyber Liability and D&O insurance.

Cyber insurance policies provide coverage for claim(s) made against Insured(s), any past, present, and future directors and officers, and other key personnel for actual or alleged privacy or network security incidents committed within the scope of their duties on behalf of the Insured organization. Make sure to review the policy's terms, conditions and definitions because policy forms may further limit how coverage might respond, including:

- **Unfair Trade Practices Exclusion** – Most policy forms, but not all, will have an exclusion with a carve-back for regulatory claims related to data or security breaches. Some policies, however, will add an additional caveat that the carve-back only applies if the *control group* or equivalent was not involved.

- **Definition of Control Group** – Policy definitions are generally broad enough to include a chief information security officer (CISO), chief security officer (CSO), or similar function.

- **Criminal & Intentional Acts Exclusion** – This excludes acts that are committed intentionally and knowingly in violation of the law. Like the Unfair Trade Practices exclusion, there is typically a carve-back that coverage is only excluded if the *control group* participated or colluded in the act.

*(continued)*

Some policies will take it a step further and impute the exclusion to the company as a whole, if the act was committed by someone in the *control group*. Coverage only applies for defense costs, and only up to final adjudication, at which point the carrier could seek repayment of the defense costs if the executive is found guilty.

The recent actions by the Justice Department and FTC underscore the need for company executives and their boards keeping a close eye on cybersecurity. Key considerations include:

- Make sure that cybersecurity best practices are being implemented (e.g., multi-factor authentication, system patching, robust offline backups, encryption, and tabletop exercises, among others) because they increasingly are being viewed as the floor, not the ceiling, for cybersecurity reasonableness.
- Designate qualified individuals for data privacy/cybersecurity program management roles.
- Ensure appropriate executive and board oversight of cyber risk.
- Develop written security and response plans that are practical, implementable, reflect the organization's operational footprint, and include the prompt assessment of notification obligations (under statute and contract).
- Conduct frequent and consistent training for all employees.
- Develop a bespoke process for collecting, using, protecting, and managing data throughout its lifecycle.
- Limit access to personal and other sensitive data only to personnel who need it.
- Ensure the accuracy of statements and claims made regarding cybersecurity, e.g., customer contracts, company website, etc.

For public companies, the stakes are about to get higher. The Securities & Exchange Commission is considering proposed rules for public companies that would, among other things, require periodic disclosure of a company's policies and procedures to identify and manage cybersecurity risks; management's role and expertise in implementing cybersecurity policies, procedures, and strategies; and the board's oversight role and cybersecurity expertise.[5]

[1] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[2, 4] https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million
[3] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf
[5] https://www.sec.gov/news/press-release/2022-39

**If you have questions about this advisory, please contact:**

**Daniel Smith**
*Marketing Account Executive*
McGriff Executive Risk Advisors
Daniel.Smith@McGriff.com
(678) 303-7256

**Scott Ferber**
*Partner*
McDermott Will & Emery LLP
The McDermott Building, 500 North Capitol Street, NW
Washington, DC 20001-1531
sferber@mwe.com
(202) 756-8988

**Natalie Santiago, JD**
*Sr. Vice President, Claims Manager*
McGriff Executive Risk Advisors
NSantiago@McGriff.com
(713) 402-1410

**Suzanne Gladle, ARM**
*Sr. Vice President, Cyber Insurance Practice Leader*
McGriff Executive Risk Advisors
SGladle@McGriff.com
(315) 750-6010