Beyond a Culture of Fear

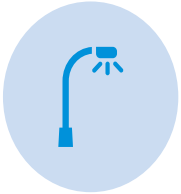
The Benefits of Legal and CISOs Uniting in a Post Uber and Twitter World

Ron Raether and Andrea Hoy, CISSP, CISM, CDPSE, MBA

History of Issues

Perceptions of CISOs within an Organization

Tasked with ensuring nothing “bad” happens.



Keep the lights on and the systems working.

Business enabler or cost (*i.e.*, reactive to needs) rather than a business asset.

Required to *check-the-box* for compliance regulations.

Roadblock to productivity and flexibility.

The Blame Game

CISO's Treatment During Yahoo 2013 and 2014 Data Breaches:

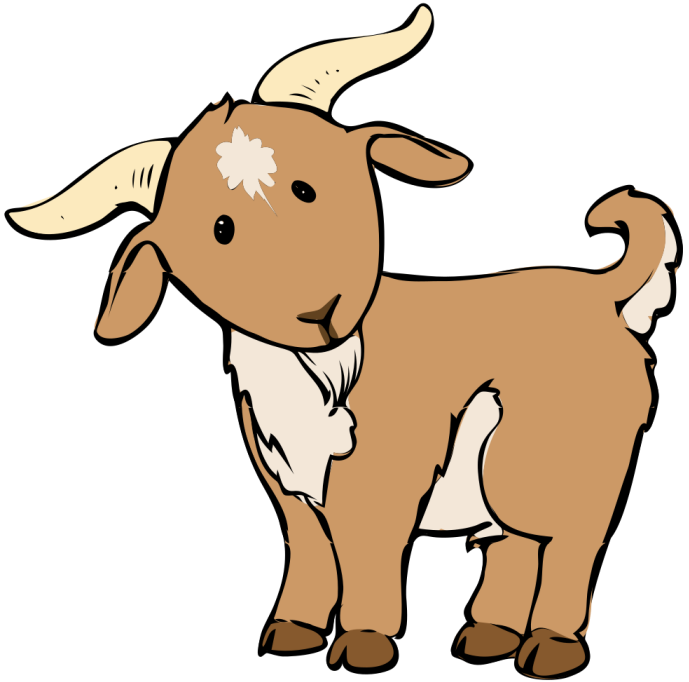
- CISO not invited into the inner circle.
- No opportunity to inform top-level leadership of security issues.
- No financial support to the CISO.

CISO's Treatment During Equifax Data Breach:

- Show of accountability to the public, customers, and clients.
- After announcing the 2017 data breach, CISO and CIO were pushed out of the company.

Chief Information “Scapegoat” Officer

- **Why are CISOs worried?**
- **Why would organizations need a scapegoat?**
  - Nobody is 100% secure. So why are we looking for someone to blame?
- **Why do CISOs feel they are typically the scapegoat following a data breach?**
  - Blaming the CISO for things outside of their control (*e.g.*, reduced budget, lack of seat at the executive table).



The Current Environment

Considering Uber and Twitter

Uber 2016 Data Breach – Timeline

Nov. 14, 2016: Threat actor demands a large ransom payment to delete data (records on approximately 57 million Uber users and 600,000 driver license numbers).

Nov. 15, 2016: Sullivan contacts then-CEO Travis Kalanick about a “sensitive” matter. The two discussed how the matter could be treated “as a [bug] bounty situation.”

Dec. 8, 2016: Uber authorizes a $100,000 payment under the bug-bounty program, who later sign non-disclosure agreements regarding the incident. An Uber lawyer was involved in drafting the agreement. The lawyer testified Sullivan changed the agreement to lie that the hackers had not “obtained” data.

September 2017: Sullivan is asked to brief the new CEO (Khosrowshahi) about the 2016 Uber data breach. However, according to court documents, Sullivan's briefing omits key details about the breach.

Nov. 21, 2017: Khosrowshahi discloses the 2016 breach with an apology for not doing so earlier. Sullivan and Craig Clark, a senior lawyer on Sullivan's team, were fired apparently for concealing the breach and paying hackers as bug bounty.

Per the Department of Justice, “The evidence showed that, despite knowing in great detail that Uber had suffered another data breach directly responsive to the FTC’s inquiry, Sullivan continued to work with the Uber lawyers handling or overseeing [the inquiry for the 2014 breach], including the General Counsel of Uber, and never mentioned the incident to them.”

Twitter – The Whistleblower Complaint

Peter “Mudge” Zatko was employed as “Senior Lead,” a member of the senior executive team responsible for Information Security, Privacy, Physical Security, Information Technology, and Twitter Service” from November 16, 2020, until January 19, 2022, which is when CEO Parag Agrawal terminated Mudge.

Mudge filed a whistleblower complaint on July 6, 2022, with Congress, the justice department, the Federal Trade Commission and the Securities and Exchange Commission alleging that Twitter mislead regulators and the public about its safety practices.

Later testifying in front of Congress, Mudge stated:

- ***“I am here today because Twitter leadership is misleading the public, lawmakers, regulators and even its own board of directors,” Mudge said as he began his sworn testimony. “They don’t know what data they have, where it lives and where it came from and so, unsurprisingly, they can’t protect it,” Mudge said. “It doesn’t matter who has keys if there are no locks.”***

A Twitter spokesperson indicated that the allegations are "riddled with inaccuracies" and that Mudge was fired for "ineffective leadership and poor performance."

CISOs' Balancing Act

Uber "Cover Up"

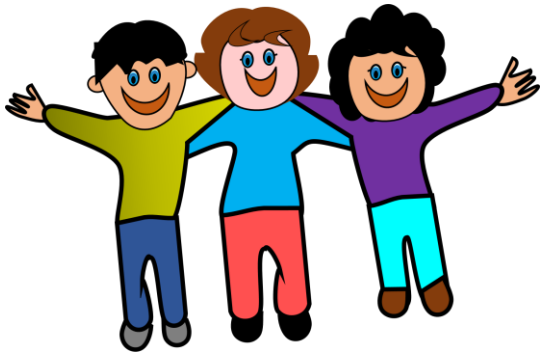
Twitter Whistleblower

Fear Not – We Can Work Together

CISO’s Best Friend

Role of general counsel:

- Effective advocate.
- Objectives naturally align.
- Simplifying obligations and reduce exposure.



Ways general counsel can further support CISO:

- Understand the issues.
- Building the right Culture.
- Establish clear InfoSec processes (e.g. standards).
- Advocate for liability insurance.
- Strong Governance.

The Silo Approach Has Got to Go

- There is no fixed standard when it comes to cybersecurity, making an already difficult job for CISOs even harder.
- Historically, GCs and CISOs led with fear.
  - Regulators and law makers contribute to the culture of fear.
  - It places CISOs on the defensive.
  - To protect themselves, some CISOs created a paper trail, laying out all potential risks and making budget requests that exceed what is needed.
  - GC's may overstate the negative consequences of a breach (e.g, reputational harm and financial damage).

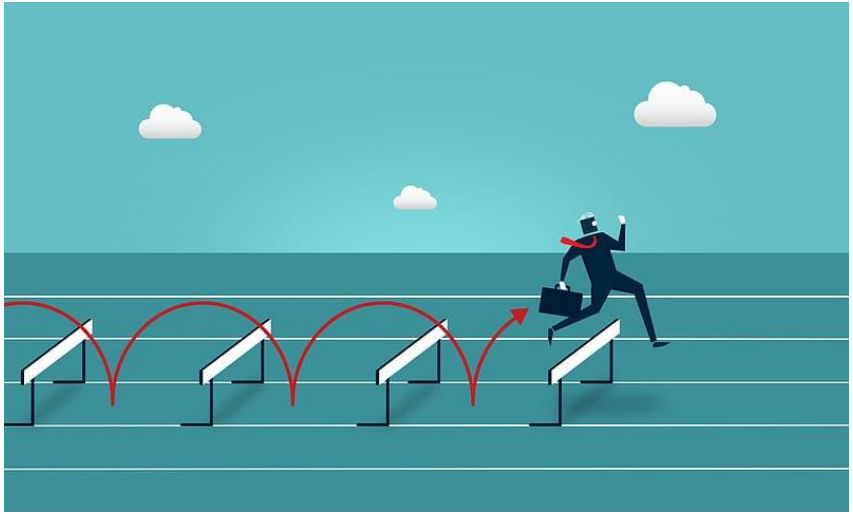
Steps for Dismantling the Silo Approach

- Board Transparency
- Risk-Based Approach
- Defined Roles, Controls and Accountability
- Reach the Right Result
- Do Not Give in To Fear

CISO Onboarding

Give Your CISO What They Need From the Start

- Ability to interview members (*e.g.*, business leaders, CEO, CFO, GC)
- Information on past breaches
- Provide CISO with network and data map
- Develop culture for keeping up with industry (*e.g.*, education, training)
- Provide baseline metrics of incidents detected and stopped
- Procedures for how security briefings will be reported



Then Let’s Focus On

- Board and executive team reporting.
- Security Steering Committee reporting to the Board.
- Budgeting and resource requests.
- Proper documentation and collaboration.
- Legal privilege discussions.
- Create whistleblower (like) procedures within the company.
- Other issues where working as team will advance the long-term business interests and make finding a scapegoat unnecessary.

Note: *The SEC proposed rules in March that would require U.S. public company boardroom's disclosure of corporate directors with cybersecurity expertise*

Final Thoughts

- **Takeaway #1**: Make thoughtful and collective decisions on information security with appropriate controls and risk-based objectives.
- **Takeaway #2**: Respond appropriately when a data incident occurs. Create controls to prevent a situation in which a few employees can conceal a breach.
- **Takeaway #3**: Provide CISO with executive team and board exposure and support.
- **Issues have existed for decades, or more! Now is the time to act. Consider running workshops to**:
  - (1) Develop plans.
  - (2) Implement plans.
  - (3) Test plans.
  - (4) Measure results to act when needed.

Q&A

Andrea Hoy – CEO
A. Hoy & Associates
ahoy.securIT@gmail.com
888.973.6731 x2001

Ronald I. Raether, Jr. – Partner
Troutman Pepper
ron.raether@troutman.com
949.622.2722

A. HOY & ASSOCIATES
28241 Crown Valley Pkwy. #455
Laguna Niguel, CA 92677

troutman pepper