

November 9, 2023

The Unlikely Pair: Importance of Building Strong Relationships Between InfoSec and Legal

Rachel Ehlers
Baker McKenzie

Emily Voorheis
Marriott Group

Jason Goodman
Marriott International

Speakers



Rachel Ehlers

Partner, Data Privacy and
Cybersecurity
Baker McKenzie, LLP



Jason Goodman

Sr. Director, Security Ops and
Incident Response
Marriott International, Inc.



Emily Voorheis

VP and Corporate Counsel,
Cybersecurity
Marriott International, Inc.

01 Current Regulatory and Threat Landscape

02 Security Officers Under Fire

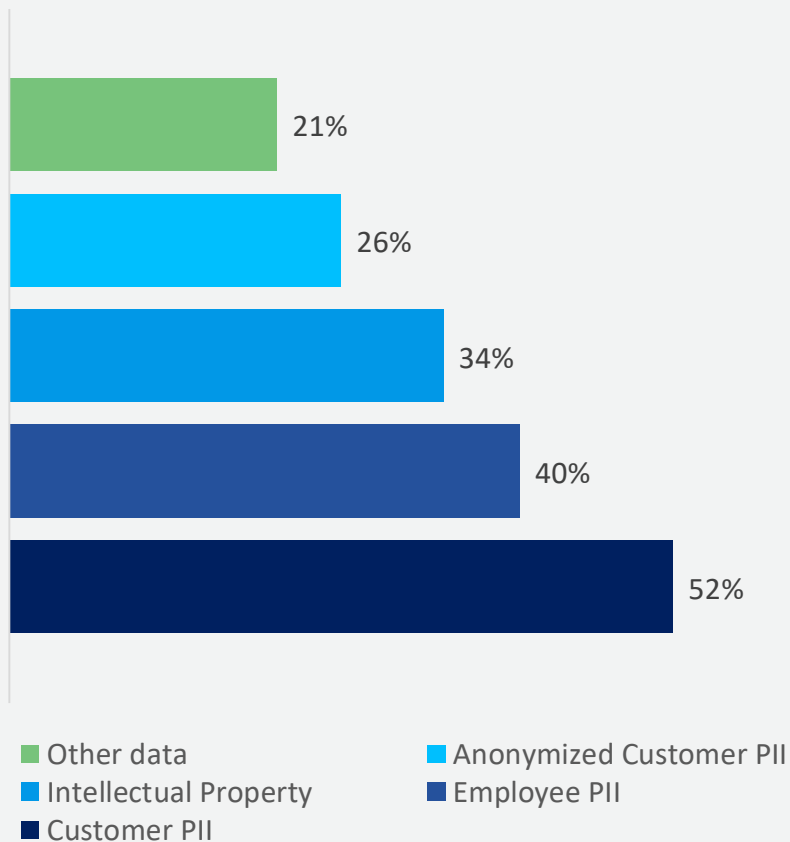
03 Key Ways to Partner

04 Practical Tips to Strengthen Relationships Between the Functions

Current Regulatory and Threat Landscape

Threat Landscape

Types of data involved in breach



\$9.48 M

*Average total cost
of a US data breach*

57%

*of data breaches result in
organization increasing the
cost of products or services*


84%

*of private sector organizations hit by
ransomware reported that the attack
caused them to lose revenue*



October 5, 2023

Clorox ransomware attack which caused product shortages linked to earnings loss

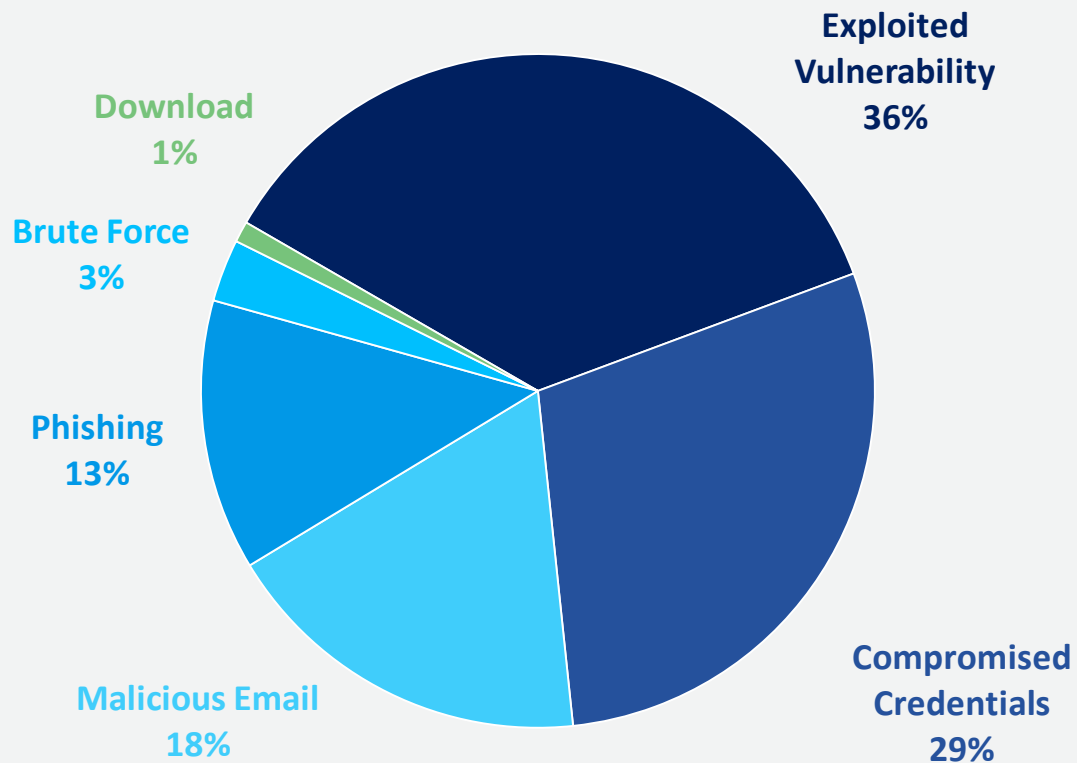
 [Amritpal Kaur Sandhu-Longoria](#)
USA TODAY

The Clorox Company announced that an August cyber attack that caused product shortages, will impact first quarter earnings for 2024, and they expect sales to drop 23% to 28%.



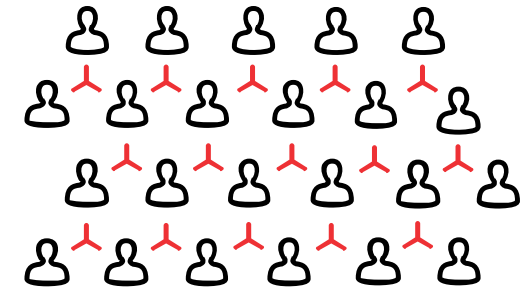
Threat Landscape

Initial attack vector



74%

*of all breaches involve
a human element*

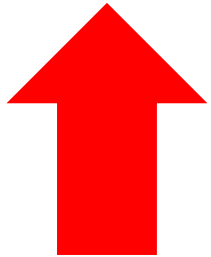


According to a 2022 Unit 42 survey:

- In 50% of cases, organizations lacked **multifactor authentication** on key systems
- In 44% of cases, organizations didn't have **endpoint detection and response (EDR) or extended detection and response (XDR)** security
- In 28% of cases, **poor patch management** contributed to attack success
- In 11% of cases, organizations **failed to review/action security alerts**
- In 7% of cases, **weak password security** practices contributed to attack success
- In 7% of cases, **system misconfiguration** was a contributing factor

Threat Landscape

Rising "double extortion" attacks



30%

In 30% of ransomware attacks involving data encryption, data was also stolen

277 days

average time to identify and contain breach

Data Recovery Is Common

97%

of organizations that had data encrypted got data back

70%

Used backups to restore data

46%

Paid ransom and had data returned

2%

Used other means to recover data

21% of organizations used multiple recovery methods

S	M	T	W	T	F	S
		X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X		

New SEC Cybersecurity Rule

- Initial determination on materiality of a cybersecurity event "without unreasonable delay"
- If incident is material, must be reported using Form 8-K within four days of the materiality determination
- Annual reporting of cyber assessment, identification and management process and Board and management oversight of cyber risks
- First reporting in December 2023 for most registrants



Critical Infrastructure Risk Management Cybersecurity Improvement Act (CIRCIIA)

- Precise scope TBD as part of current rulemaking
- Applies to entities in one of 16 critical infrastructure sectors
- Must report cyber incidents within 72 hours of companies' reasonable belief that incident has occurred
- Must report ransom payments within 24 hours after a payment is made



FTC Enforcement

- Expanded cyber mandate
- **Chegg**: EdTech company accused of lax security practices, exposing sensitive customer and employee data
- **Drizly**: Repeated failures to secure consumer data from hackers
- **GoodRx**: Fine of \$1.5M under Health Breach Notice Rule; failed to report unauthorized disclosure of health data with advertising companies



Security Officers Under Fire

Case Study: US v. Sullivan

- Joseph Sullivan appointed Uber's Chief Security Officer in April 2015
- At same time, Uber was being investigated by FTC for 2014 cyber incident
- Sullivan was deposed in November 2016 around investigation
- Soon after, Sullivan learned of a new cyber incident which exposed PII of millions of drivers and customers; Sullivan told team to conceal 2016 incident
- Sullivan approved payment to threat actors of \$100K under Uber's bug bounty program; threat actors signed NDA and agreed to destroy compromised data
- Sullivan did not disclose 2016 incident to FTC or other authorities
- In 2017, Uber's new management notified FTC and public about 2016 incident



Case Study: US v. Sullivan

Charges

- Obstruction of justice (U.S.C. § 1505)
- Misprision of a felony (18 U.S.C. § 4)
- Wire fraud counts dismissed before trial

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 15, 2016 to Nov. 21, 2017 in the county of San Francisco and elsewhere in the Northern District of California, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1505	Count One: Obstruction of Justice Max. Penalties: 5 years in prison; \$250,000 fine; 3 years of supervised release; \$100 special assessment; restitution; forfeiture
18 U.S.C. § 4	Count Two: Misprision of a Felony Max. Penalties: 3 years in prison; \$250,000 fine; 1 year of supervised release; \$100 special assessment; restitution; forfeiture

Obstruction of justice

- Obstruction of justice requires three elements:
 1. The existence of an agency proceeding;
 2. The defendant was aware of the proceeding; and
 3. The defendant intentionally endeavored corruptly to influence, obstruct, or impede the pending proceeding
- Sullivan argued that the prosecution also needed to show that there was a nexus between the proceedings and the conduct of the defendant, but the court rejected this additional element
- Sullivan also argued that, where the prosecution relies on the defendant's failure to disclose (rather than on affirmative acts of obstruction), a "duty to disclose" must also be established; but the court also declined to read this requirement into the test for obstruction

Case Study: US v. Sullivan

Verdict and sentencing

- In Oct 2022, jury returned a guilty verdict on both the obstruction and misprision counts
- Verdict was affirmed by judge on motion for acquittal
- In May 2023, Sullivan was sentenced to 3 years' probation plus 200 hours of community service; prosecutors had sought a custodial sentence
- Sullivan appealed conviction in Oct 2023

The New York Times

Oct. 5, 2022

Former Uber Security Chief Found Guilty of Hiding Hack From Authorities

A jury found Joe Sullivan, who led security at the ride-hailing company, guilty on two different counts. The case could change how security professionals handle data breaches.

Case Study: SolarWinds

Background

- In Dec 2020, SolarWinds, which provides IT management solutions, disclosed that it had detected that Russian intelligence actors has injected malicious code into its Orion software, which is used by approximately 33,000 customers
- Among those affected were multiple US federal agencies (including the Treasury Department, CDC, DoJ. FAA), NATO, the U.K. government, the European Parliament, Microsoft
- According to a White House briefing, this compromise allowed Russian intelligence "to spy on or potentially disrupt more than 16,000 computer systems worldwide"



SEC Response: Wells Notice

- In June 2023, SolarWinds disclosed via Form 8-K that certain executives, including its CFO and CISO had been issued Wells Notices by the SEC
- Wells Notices are used by the SEC's enforcement division to inform recipients that it is prepared to recommend charges and provides recipients with the opportunity to explain to the SEC why they should not be charged



Case Study: SolarWinds

SEC Response: District Court Action

- ➔ On October 30 the SEC filed a SDNY complaint, naming both SolarWinds and Timothy Brown, its CISO, as defendants
- ➔ The complaint alleges that SolarWinds and Brown made materially false and misleading statements in its SEC filings and other public-facing statements that SolarWinds employed strong cybersecurity practices, when in fact it (1) failed to maintain a secure development lifecycle for software it developed, (2) didn't enforce the use of strong passwords on all systems, and (3) didn't remedy long-running access control problems

THE WALL STREET JOURNAL.

Oct. 30, 2023

Cyber Chiefs Worry About Personal Liability as SEC Sues SolarWinds, Executive

Tim Brown, the company's top security executive, is named in SEC suit

As the Securities and Exchange Commission gets more aggressive in enforcing cybersecurity regulations, corporate cyber chiefs want to insulate themselves from potential liability. The SEC on Monday sued technology company SolarWinds and its head of security, alleging they defrauded shareholders by misleading them about cyber vulnerabilities and the scope of a 2020 cyberattack.

SEC Response: District Court Action

Case 1:23-cv-09518 Document 1 Filed 10/30/23 Page 8 of 68

14. During 2020, Brown learned about increasing cybersecurity attacks against, and vulnerabilities involving, Orion and other SolarWinds' products. This included cybersecurity attacks against two customers who were using the Orion product, U.S. Government Agency A in May 2020 and Cybersecurity Firm B in October 2020.

15. Shortly after the October 2020 attack against Cybersecurity Firm B, SolarWinds employees including Brown recognized similarities between that attack and the attack on U.S. Government Agency A. But when personnel at Cybersecurity Firm B asked SolarWinds employees if they had previously seen similar activity, InfoSec Employee F falsely told Cybersecurity Firm B that they had not. He then messaged a colleague, “[W]ell I just lied.”

Key Partnership Areas

Key Partnership Areas

Governance



Incident Response

Pre-Attack Readiness: Action Items

Trainings and Tabletops

Incident Response Plan

Avoidance

- Back-up systems and segregation
- Operational recovery plan
- Back-up communications systems
- Business continuity plan

Engagement with service providers:

- Forensic
- eDiscovery
- PR/Crisis Management
- External legal counsel

Insurance

Post-Attack Response: Action Items

Containment and info gathering

Systems recovery

Engagement with threat actor

Reporting to authorities and regulators

Dealing with vendors

Breach notification obligations and credit reporting

Corporate/employee investigations

Remediation

Litigation and regulatory response

Key Partnership Areas

Insider Threats

Design and implement program
Identify and map key risks
Threat modeling



Threat containment
Crisis management
Investigation

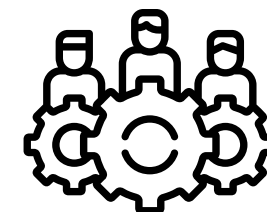
**Prevention and
preparation**

**Detection and
assessment**

**Management and
Mitigation**



Proactive and ongoing
Malicious code review
Engagement with HR



Key Partnership Areas

Data Loss Prevention

**Classify and
prioritize key data**

**Identify system
vulnerabilities
proactively**

**Understand risk
scenarios**

**Distinguish risk
between internal
and shared data**

**Access controls /
identity
management**

**System monitoring
and logs**

**Monitor data
movement**

Employee training

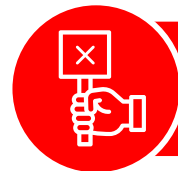
Bug Bounty Programs

Offer rewards to individuals (typically outside the organization) in exchange for discovering and reporting security exploits and vulnerabilities



Dos

- Use bug bounty programs to detect new vulnerabilities and secure your systems
- Establish a bug bounty policy that clearly sets out how the program operates
- Engage with program participants



Don'ts

- Use bug bounty programs to fund ransomware payment or to engage with threat actors
- Mislead bug bounty participants or authorities
- Isolate your bug bounty program from other larger information security program

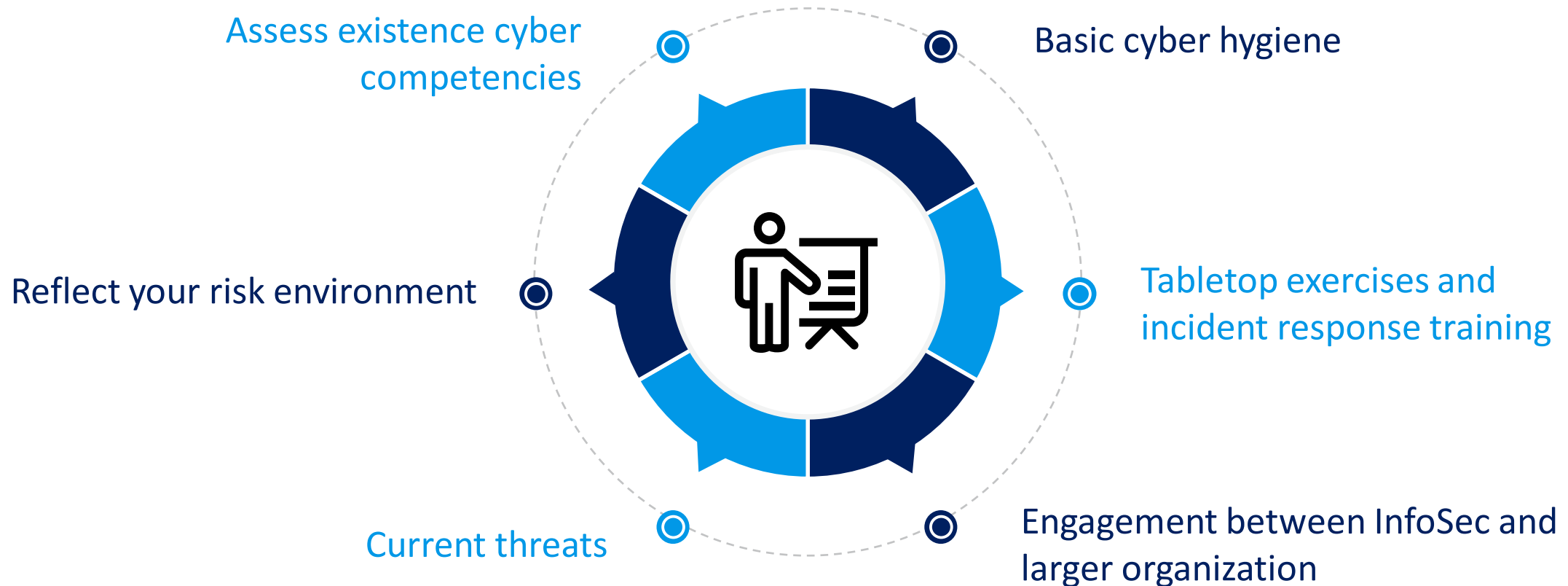
Key Partnership Areas

Communications



Key Partnership Areas

Training



Practical Tips to Strengthen Relationships Between Security and Legal Functions



Establish relationships between Legal and InfoSec; and be able to articulate how such relationships can help:

- Provides an ally at the senior executive level (GC)
- Brings in outside counsel for broad experience and perspective on certain issues
- Provides a legal perspective on the impact side of the risk equation (impact of non-compliance, impact of slow response, etc...)
- Is a sounding board when contemplating new situations/scenarios
- Helps with regulatory requests
- Helps with contract interpretation when dealing with third parties (franchise, vendors)
- Can be the 'bad cop' when dealing with difficult business partners or third parties
- Follows changing legislation, keeps us informed, and helps us plan to comply
- Provides analysis of notification requirements for privacy/security incidents



Stay connected and expand Legal and InfoSec collaboration beyond the typical areas:

- Triage meetings
- Involvement in non-privacy or cyber matters where there are potential privacy or cyber implications
- Quarterly threat meetings

Practical Tips

- ✓ Prepare for the worst -- evaluate risks and liabilities candidly
- ✓ Understand reporting obligations
- ✓ Adopt written policies; socialize throughout organization
- ✓ Monitor and manage vendor risks
- ✓ Understand how to frame cyber risk as a board issue

Questions