Cybersecurity, Cybercrimes, and Investigations

CompTIA Luncheon

Wednesday, December 8, 2021

Bandler Group LLC
Bandler Law Firm PLLC

CompTIA

Good cybersecurity protects from cybercrime

Cybercrime is a threat to every single organization. Attacks can disable operations and cause serious harms that are costly, time consuming, and stressful. Organizations should protect against cybercrime threats including:

- ***Data breaches***
- ***Ransomware***
- ***Theft of funds***

Cybersecurity is a legal duty

Laws impose duties upon organizations related to cybersecurity. Organizations need to:

- *Be diligent and reasonable* (not negligent or deficient)
- *Protect the personal and private information* they hold
- *Comply with laws* and regulations that impose specific cybersecurity requirements
- Monitor for, identify, investigate, and accurately *report data breaches* to government and affected parties.

Incident response plans are important

Incident response planning is an important part of a cybersecurity program. Organizations that properly plan for incidents are:

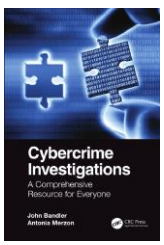
- Aware of the potential harms and their own legal duties
- Better able to prevent incidents from happening in the first place
- Ready to respond effectively to mitigate cybercrime damage.

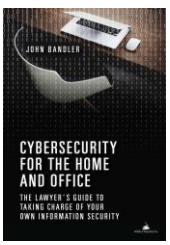
Cybercrime investigation needs to be improved

Cybercrime investigation is uniquely done by both law enforcement and private sector victims of cybercrime. But only law enforcement has the ability to bring cybercriminals to justice, and deter cybercrime attacks. There is room for improvement.

About John Bandler

John Bandler has unique expertise that spans law, technology, business, cybersecurity, investigation of cybercrime, writing, training, and speaking. He is licensed to practice law in NY, CT, and DC, and holds many certifications in cybersecurity, technology, and more. He has been serving the private sector since 2015 and is the author of two books and many articles. He teaches at the law school, graduate, and undergraduate levels, and is a frequent speaker. Previously he served the public as a prosecutor (where he investigated and prosecuted cybercrime among other offenses), state trooper, and military officer.
Visit John's website or find him on LinkedIn to learn more.





John Bandler
Bandler Law Firm PLLC & Bandler Group LLC
48 Wall Street, 11th Floor
New York, NY 10005
JohnBandler@BandlerGroup.com
(929) 265-2775
johnbandler.com

COMPTIA'S FALL ROUNDTABLE

Cybersecurity, Cybercrimes, and Investigations Luncheon

Wednesday, December 8, 2021, 11:30am to 2:00pm

Invitation only, at one of the most celebrated event venues in New York State

Description

CompTIA roundtables are engaging session designed to bring senior level tech executives together to share insight on a variety of topics. We learn about how fellow executives are managing IT, data, law, regulation, cybersecurity, cybercrime and privacy.

This session is led by John Bandler, principal and founder of Bandler Law Firm PLLC. Cybercrime continues to skyrocket but we are not combatting it effectively yet, and legal duties are growing for private organizations. This interactive discussion looks at cybercrime, cybersecurity, and the interplay of economy, business, technology, and law, in the context of preparing for and conducting cybercrime investigations. Cybercrime investigation is uniquely a both private and public sector endeavor, done by people of all backgrounds and skills.

Agenda

Time	Activity	Host
11:30 – 12:00 PM	Arrival, registration, introductions, drinks and appetizers	Teresa Varela, Joe Padin
12:00 – 1:50 PM	Moderated luncheon discussion	John Bandler
1:50 – 2:00 PM	Closing comments	Teresa Varela, Joe Padin

Topics

- Introductions and setting the stage
- Why does cybercrime flourish?
  - Practical effects upon your business
- What are the legal duties for cybersecurity, and why are they increasing?
  - Practical effects
- How do legal duties extend to cybercrime investigation and reporting?
  - Practical effects
- Is "reasonable cybersecurity" and "reasonable cybercrime investigation" an adequate legal and practical standard?
- Summing up government duties and private sector duties to protect against and investigate cybercrime. Is there any other way?

Takeaways

1. Know what legal standards, laws, and regulations apply to your organization regarding cybersecurity measures and cybercrime reporting.
2. Comply with these legal requirements, demonstrate compliance, and protect from cybercrime.
3. Review internal rules (policies, etc.) to ensure they align with external rules.
4. Review action (practice) to ensure it aligns with internal policy and law.
5. Prepare and plan for cybercrime response, then prioritize to prevent the need.