CLARK HILL

You've Been Hacked! Now What?

By: Melissa K. Ventrone & Jeffrey Wells, January 21, 2021

Melissa Ventrone, Esq., CIPP, Clark Hill

Chair, Cybersecurity, Data Protection, and Privacy Practice

- Leads a team of attorneys, forensic investigators, and crisis experts delivering 24/7, end-to-end breach response support
- Managed 3,000+ breaches for clients ranging from small businesses to F500 companies
- Successfully defended some of the toughest privacy litigation matters and class actions
- Delivers training, simulation exercises, and action plans compliant with state, federal, and international laws
- Distinguished 21 years of service in the Marine Corps Reserve

Jeffrey Wells, ASSET360

Director of Cybersecurity Consulting Services

- Certified Ethical Hacker with 25+ years of experience keeping organizations safe and protecting critical data
- Served as "Cyber Czar" for two Maryland governors and founded a White Hat cyber advisory firm
- Aligns commercial, federal, and military cybersecurity initiatives with NIST, NSA, US Cyber Command, and other military and government entities
- Distinguished cyber career in the US military and intelligence community

Imagine someone trying to break into your house. Now imagine it **60,000 times a day**.

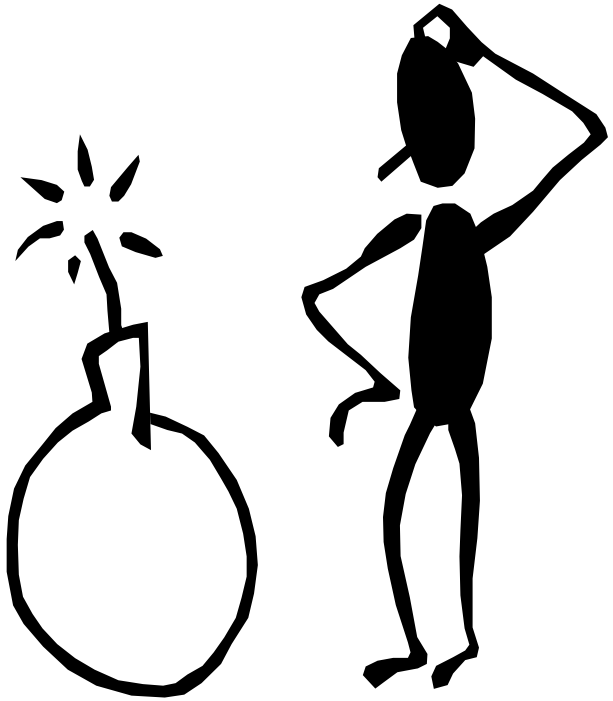
http://www.ibm.com/smarterplanet/ie/en/business_resilience_management/overview/index.html?re=spf

Agenda

- Incident Preparedness
- Legal Requirements
- Cyber Attack
- Lessons Learned

Why Are We Talking About Incident Response?

- Companies want more data, accessibility, and availability, which equals larger risk profiles.
- Attacker tactics keep changing, causing more damage.
- Cyberattacks aren't going anywhere.
- Preparing for an incident reduces the overall damage and costs.



Before We Begin

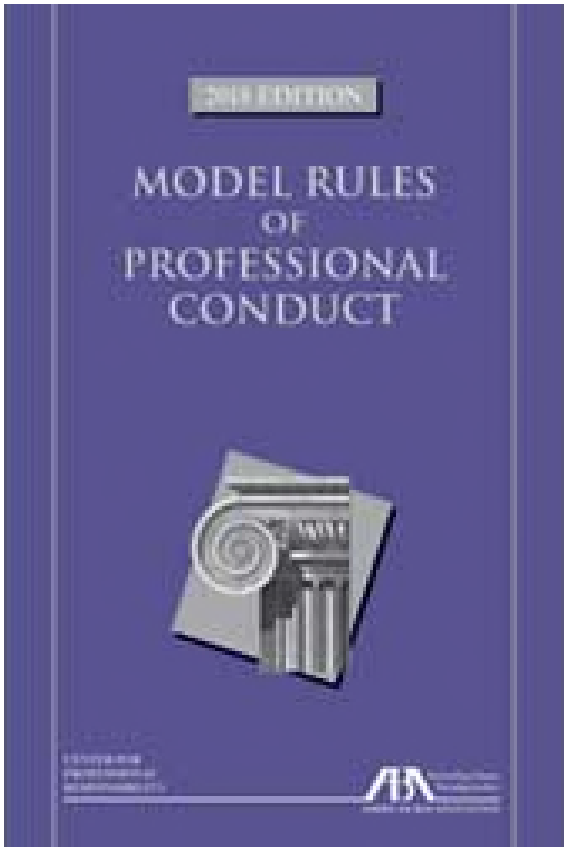
- Data breaches aren't just IT problems.
- Life Cycle of a Data Breach
  - **Incident Identification**: What just happened?
  - **Response Team Engagement**: Are the right people/partners part of the team?
  - **Containment**: Have you stopped the "bleeding"?
  - **Remediation**: Have you taken steps to prevent this type of event from occurring in the future?
  - **Notification** and beyond
- Logistical execution makes the difference between good and bad response.
- PRACTICE!

What's at Stake?

- Reputation Damage
- Customer Safety
- Legal & Compliance Risk
- Business & Supply Chain Interruption
- Data Loss (e.g. customer, employee, trade secrets)
- Costs (e.g. legal, forensics, ransom payment)

Ethical Obligations

Duty to Safeguard – Key Ethics Rules



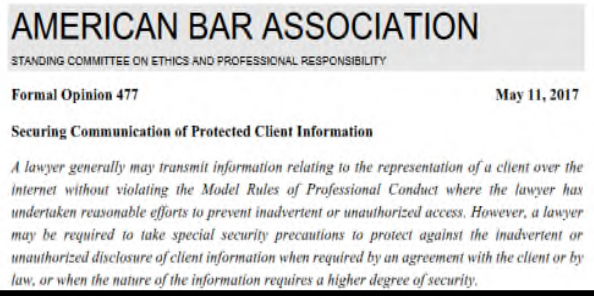
Rule 1.1 Competence

Rule 1.4 Communication

Rule 1.6 Confidentiality

Rules 5.1, 5.2, 5.3 Supervision

Duty to Safeguard – Ethical Rules



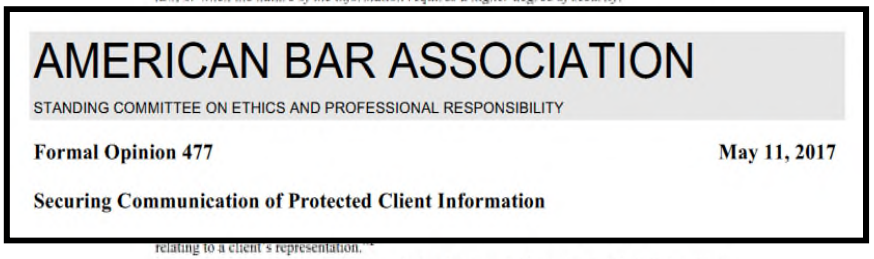
AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477 **May 11, 2017**

Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477 **May 11, 2017**

Securing Communication of Protected Client Information

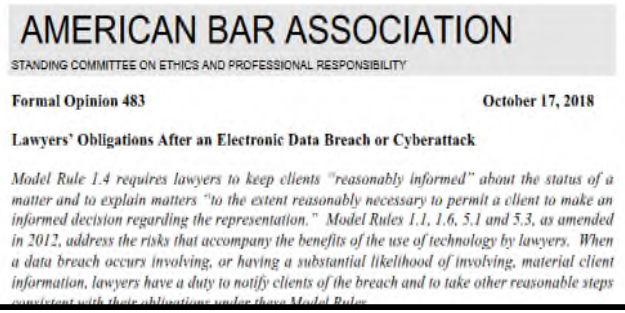
relating to a client's representation.[2]

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.[2]

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.[3]

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c)

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).
2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting authcheckdam.pdf.
3. *See* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].



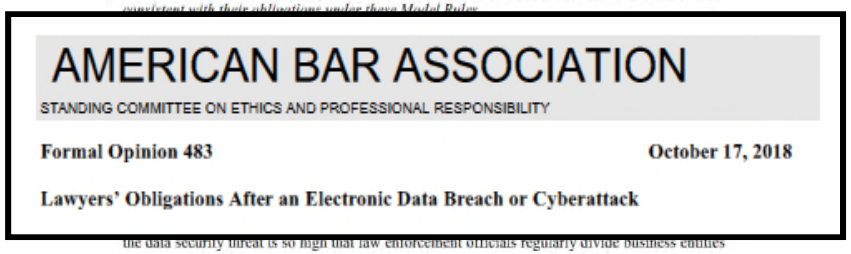
AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

1 This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.
2 *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com (explaining that "[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence."); *See also Criminal-Seeking-Hacker' Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).
3 Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.
4 Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
5 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").


Cyber Attack Simulation

The Scenario

- Lux Retailer ("Lux") is an American technology manufacturer headquartered in warm, sunny Austin, Texas with over 45,000 employees and operating centers in Michigan, Illinois, California and Texas.

- Known for innovation and cutting edge technology, Lux combines advanced integrated software, ease of use, and convenience for its customers. Key R&D initiatives are focused on additional ways that its software can use data to increase profitability. Lux offers on-premise software and Software as a Service (SaaS).

- It is your first week on the job, and you are responsible for overseeing IT operations in the newly opened facility located outside of Austin, Texas.

Cyber Attack

- An employee receives an email message from a purported "security researcher" who claims to have identified and exploited a vulnerability in Lux's system and taken data.

- For a $1M "consulting fee," the researcher will tell Lux the vulnerability and delete the data.

Choose Your Response

What do you do?

A	B	C	D
Nothing – everyone knows these types of emails are fake.	Call the help desk and report the email.	Call your cyber insurance carrier immediately.	Call the FBI or local law enforcement.

15

Initial Investigation

- The employee forwards the email to the help desk.

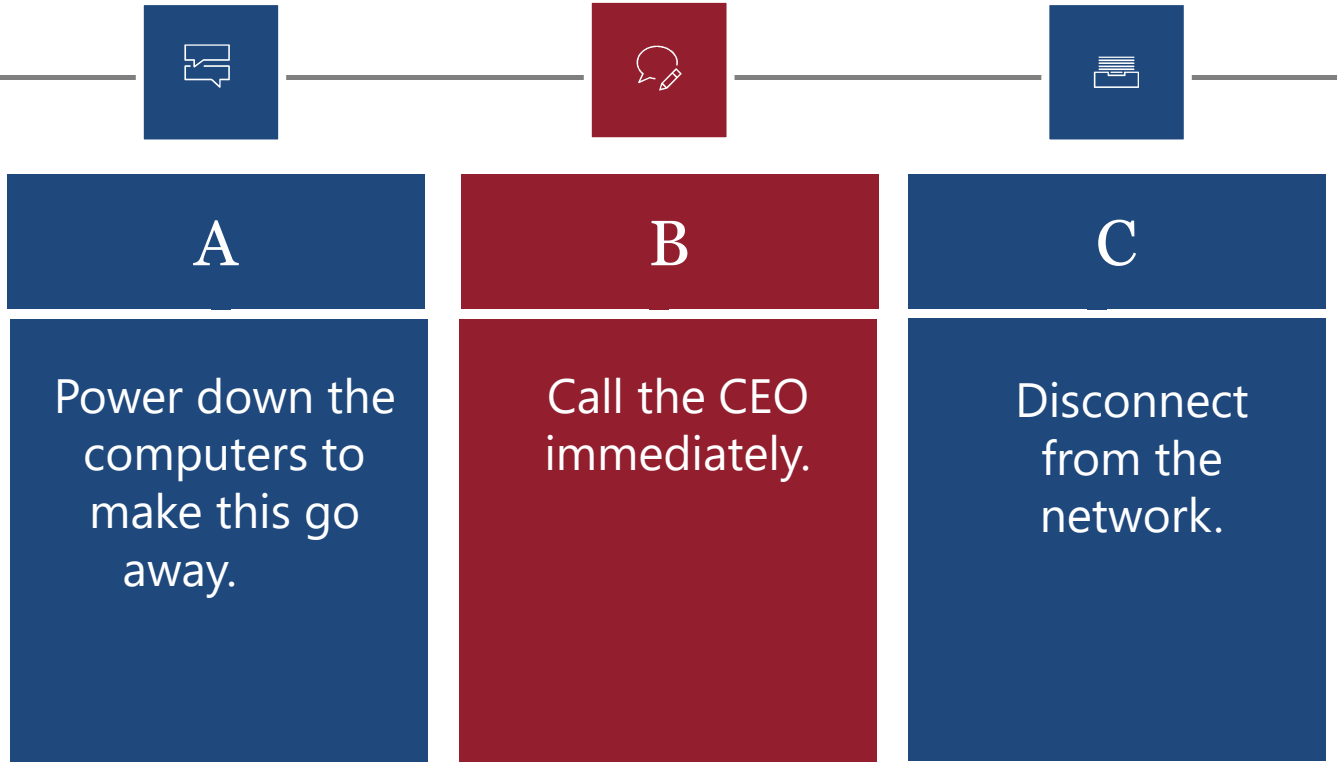
- The help desk reviews the email and informs the employee that it is spam and to delete the email.

More Problems

- The help desk starts receiving complaints from users that they can't access files.
- Complaints are escalated and IT identifies a pop-up note on a device stating that all files have been encrypted and the only way to recover files is to pay $10M within 72 hours.
- The note says Lux data will be published if the demand is not paid within 72 hours.

Choose Your Response

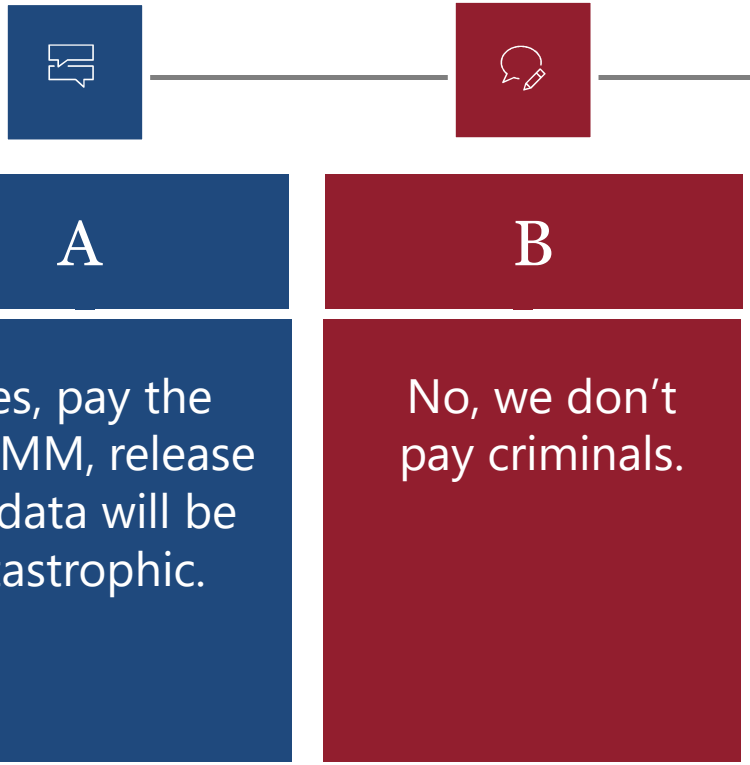
Upon seeing the ransom demand, what is your immediate response?



18

Choose Your Response #2

Demand is $10 million, do you pay it or not?



19

To Pay Or Not To Pay

- The company has good backups
  - But what if it will take 2 weeks to restore systems from backup?
  - What if the attacker deleted your backups?

- Story time:
  - What if you forget the password to the backups?
  - What if your backups are from 7 months ago?

Ransomware

- IT reports that it appears all systems are encrypted.
- Not only are company emails and files impacted, but operations have been halted. Email is down as well.

What are Next Steps?

- Trigger your incident response plan/team
- Contact external legal counsel specializing in incident response
- Contact your insurance carrier
- Legal counsel contacts external computer forensic experts
- Legal counsel engage an external crisis communication team

Things Not To Do

- Immediately send a communication to your employees about the ransomware attack
- Immediately start contacting your clients
- Delete the encrypted information off of the devices
- Try and solve this internally
- Release a press statement about the ransomware attack
- Panic

Incident Update – 24 hours

- Outside breach response counsel is engaged, computer forensics and crisis communication firms engaged under attorney-client privilege.
- Negotiations opened with threat actor, ransom reduced to $5 million.
- Forensic investigation – have collected about 50% of forensic artifacts for investigation, can't tell if data was taken.
- Systems still not operational, email still down.

Communication

- Internal communications – who needs to know what?
  - Board of directors
  - Management
  - Employees
- External communications?
  - Customers
  - Business partners (contractual requirements)
  - Vendors
  - Media – reactive statement
  - Regulators

Choose Your Response

Ransom has been reduced to $5 million, do you:

A	B
Pay the $5M, this is a 50% discount, to protect your data	Not pay – Lux doesn't engage with criminals.

26

You Choose Not To Pay The Ransom

- As the team is attempting to restore data from backups, the attacker starts releasing your data.
- A file containing prototypes and trade secrets for your company is posted online. Attacker says they have more data.

You Chose To Pay The Ransom

- Pay for decryption key:
  - Create forensic copy of affected devices.
  - Test decryption key to confirm no malicious processes.
  - Test decryption key on data, then execute.
  - Review device to make sure no secondary infection is present.
  - Restore to clean devices.
- Threat actor states that all Lux data has been deleted.

Forensic Investigation

- Forensics discovered that an update for a security tool provided by a third-party that contained a backdoor that allowed attackers to gain access to the network
- The attacker gained access to the environment and deployed other tools throughout the environment to gain admin privileges
- Used the admin privileges to move laterally, take data and deploy ransomware

Notification Requirements

- Contractual notice
- Statutory notice
- Regulatory notice
- Business reasons

The Fallout

- After working around the clock for 3 weeks, the response team has successfully restored data from backups.
- Business Loss
- Reputational Harm
- Potential Litigation

What We've Learned

Lessons Learned

- Preparation is key
  - Create incident response plan – include management in plan, not IT only
  - Identify external resources and pre-negotiate contracts
  - Think about logistics

- Training is important
  - Test the plan – test different portions, update it
  - Ensure everyone understands their roles

Avoid Common Response Pitfalls

- Don't panic (no really, don't panic)
- Have physical copy of plan
- Follow your plan
- Bring in the right team
  - Notify your carrier
  - Consult with experienced privacy counsel
  - Qualified computer forensic firm
- Be mindful of communications

Thank you!

Questions? Contact:

Melissa Ventrone
mventrone@clarkhill.com

Jeffrey Wells
jwells@clarkhill.com

24/7 Breach Response Hotline:
breachresponse@clarkhill.com
877.912.9470

Assembling the Team

- Key members of the Incident Response Team are alerted including:
  - Legal Counsel
  - Information Security
  - Communications
  - HR
  - Risk
  - Finance
  - Operations

Your Service Provider

- The business-critical applications are hosted by an outside service provider. Your access to the system is limited to entering data, assigning/terminating accounts, resetting passwords, running reports.
- The service provider is responsible for the security, integrity, and availability of data and applications. The contract simply says provider is required to have adequate back-ups.
- You call the relationship manager and help desk and leave urgent messages. Hours later, the relationship manager, calls and tells you their entire system has been hit by a ransomware attack. They are working to restore the systems and will be in touch shortly.

Ransomware On the Vendor's System

- In house counsel reviews the vendor contract and advises that:
  - The SLAs do not anticipate this type of event.
  - The contract does not contain sufficient audit requirements.
  - There is no termination/requirement to assist with migration.

Legal Compliance & Data Protection Regulations

- Location and industry drives compliance requirements
- Many laws include security requirements, non-compliance can result in fines and penalties
- Contractual requirements
- Develop, implement, and audit a compliance program

Law Enforcement Arrives

- The FBI shows up at your facility.
- They ask to image your servers and request that the company not notify any of its customers or employees of this event.
- The FBI wants the hackers to continue operating so they can gather evidence in order to attempt to arrest the individual(s).

Choose Your Response

Which external partners need to be engaged?

A	B	C	D
Cyber Insurance Carrier	Outside Privacy Counsel	Forensic Investigators	All Choices

41

Choose Your Response

What do you do?

A	B	C	D
Tell the reporter everything – the story will come out anyways.	Say nothing. Who cares about the news - our clients are loyal.	Engage crisis communications to release a holding statement.	Resign.

42

Brian Krebs is Calling

- You receive a phone call from Brian Krebs, a well-known cybersecurity reporter who has announced high profile data breaches and has a substantial social media following.
- Mr. Krebs references a security incident at your facility and asks for a statement before posting to his blog.

Data Breach

What is a Data Breach? Is it:

A	B	C	D
The unauthorized access to personally identifiable information or protected health information?	The unauthorized acquisition of personally identifiable information or protected health information?	The unauthorized access or acquisition of personally identifiable information or protected health information that causes a risk of harm to the individual?	Who cares? I'm only here for the free lunch.

Data Breach Exercise Rules of the Road

- Facilitators will present a scenario based upon their response experience.
- Participants will provide input on proposed actions.
- There is no wrong answer.
- Facilitators will share pros/cons for each choice.

Data Breach Exercise Goals

- Understand how to navigate a security incident
- Identify the right partners to assist with the response
- Identify critical decisions during a response
- Recognize and avoid common pitfalls that complicate the response and exacerbate harmful effects

Supply Chain Considerations

- What is supply chain cyber risk?
  - Cyber risk to your organization from your supply chain such as reliance on vendors and new technology
- Addressing supply chain risk:
  - Require due diligence reviews by vendors
  - Address / shift risk in contracts
  - Include audit requirements
- What if you are the supply chain?

Your Mission

Your objectives in this exercise are to:

A	B	C	D
Minimize the impact from a cybersecurity attack.	Keep costs to a minimum (budgets are tight due to the pandemic).	Maintain the company's brand reputation.	Ensure consumer safety.

48