



BUTLER | SNOW

---

# Cybersecurity Case Study

H. Barber Boone

Blythe K. Lollar

LAW ELEVATED

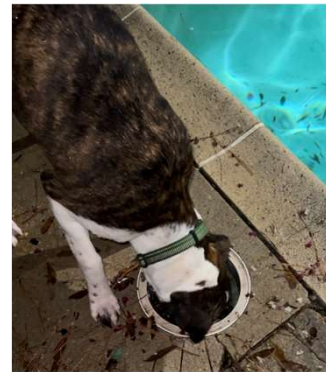
BUTLER | SNOW

**H. Barber Boone**



THE UNIVERSITY of  
**MISSISSIPPI**  
SCHOOL OF LAW

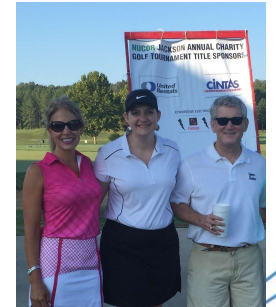
**accenture**



# Blythe K. Lollar



THE UNIVERSITY of  
**MISSISSIPPI**  
SCHOOL OF LAW





# Cybersecurity Can't Be Ignored

What Can I do to Prepare for WHEN (Not IF) This Happens To My Company?

Federal judiciary 'vulnerable' to cyberattacks,  
U.S. lawmakers told

Reuters May 12, 2022

The Internet Archive is under attack, with a breach  
revealing info for 31 million accounts

The Verge Oct. 9, 2024

Alaska court system forced offline  
by cyberattack

The Hill May 3, 2021

Data Breach Impacts 800,000 Insurance  
Customers

Forbes Nov. 2, 2024

U.S. Justice Department probing cyber  
breach of federal court records system

Reuters July 29, 2022

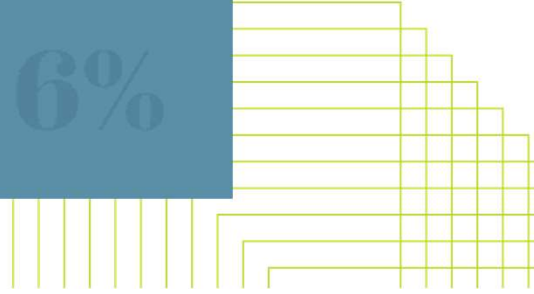
**23andMe Settles \$30M Class-Action Lawsuit**

Personal data of nearly half of the popular genetic testing company's customers --  
6.9 million people -- was exposed in the data breach.

CNET Nov. 8, 2024

CFPB says employee breached data of 250,000  
consumers in 'major incident'

Politico April 19, 2023



# Incident Response Phases

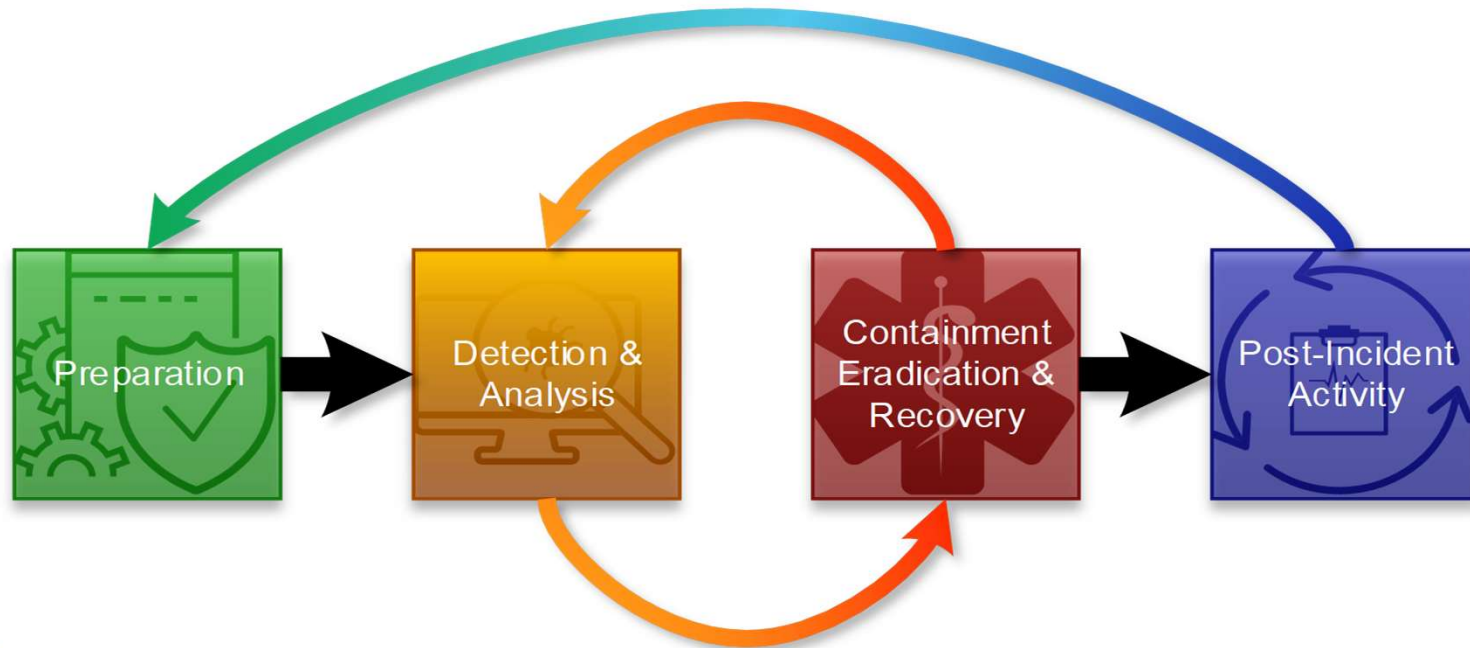
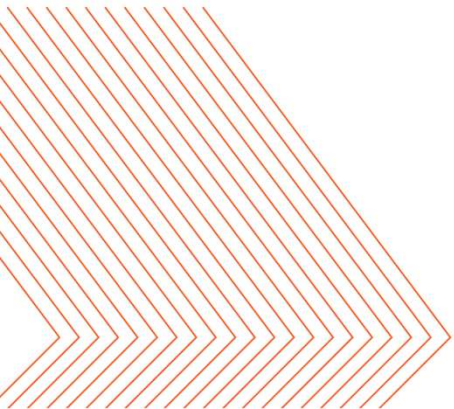


Figure 1: Incident Response Phases – NIST SP 800-61 Rev. 2

# Company Background

- You are a General Counsel of a company that manufactures locker bones, internal shelves for grade school lockers.
- You sell most of your products directly to consumers through your website, but you also have partnerships with other companies which sell your product to their customers. You ship directly to those customers.
- Your company has several facilities across the country.
- July and August are your busiest months as school starts around the country.



# Business as Usual

- **Tuesday, June 25 – Leadership Meeting**

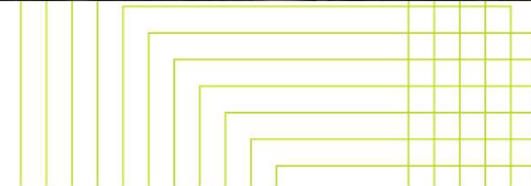
- CTO mentions that one of the servers has gone down and is inaccessible. Their team is looking into it, but it probably is time for that server to be replaced anyway. He will work on getting a quote for a new server.





# Storm is Brewing

- **Thursday, June 27 – Technical Call**
  - You get on a call with the CTO and other members of the technical team. Some members of the Procurement Group have been locked out of their accounts.
  - There was a full system outage for 2 hours the night before, but the technical team was able to reboot the system.
  - They still haven't gained access to the server mentioned earlier in the week.
  - A second server would not startup after the reboot.
  - All systems are operating because of the redundancies.



# Storm is Brewing

- **Thursday, June 27 – After the Technical Call**
  - You walk into the COO's office as he is getting off the phone with the CTO.
  - They are having some difficulty with the servers and want to bring in some additional help during this busy time.
  - IT is understaffed and this additional help would let the IT team work on keeping the order system running and the other team would focus on fixing the down servers.



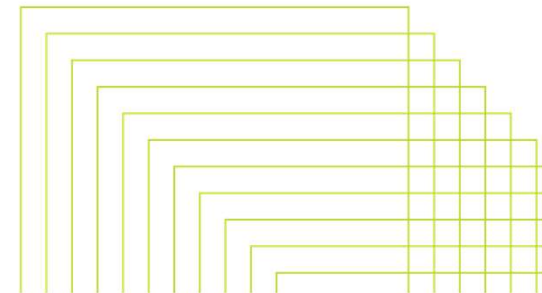
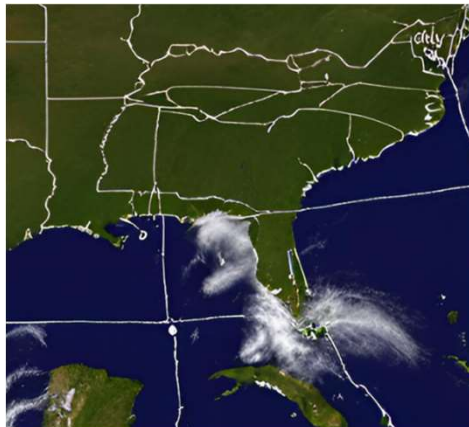
# Lightning Strikes

- **Friday, June 28 – 3:00 P.M. – Emergency Leadership Meeting**
  - CTO says he received a ransom e-mail.
  - The e-mail says that he was a hacker and that he has accessed and downloaded all of the company's files.
  - If the company does not pay them \$10 million within days, he will release the information on the dark web.
  - CTO is looking into whether the hacker's claims are correct.
  - Team agrees to meet on Saturday at 9:00 A.M.



# Summer Storm or Hurricane?

- **Saturday, June 30 – 9:00 A.M.**
  - CTO says the hacker has provided them with screenshots of file directories that seem to match up (~90%).
    - Some of the file sizes don't match up.
    - Some of the modified dates don't match up.
  - But he doesn't know whether the hacker actually has the documents or if he just has the directory listing.
  - The team wants to use the weekend to determine what the hacker actually has, ... if anything.



# Summer Storm or Hurricane?

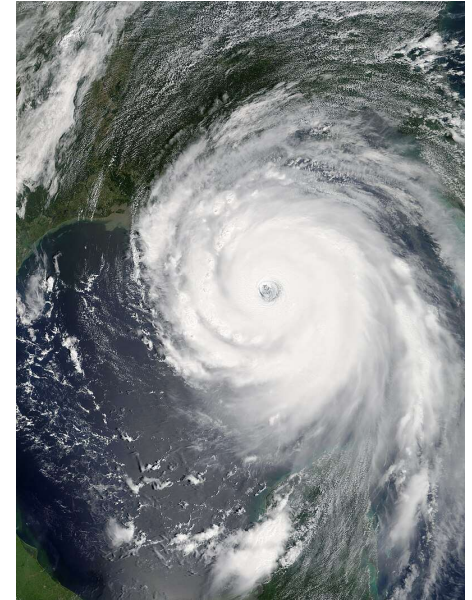
- Saturday, June 30 – 9:15 A.M.
  - You, as a knowledgeable General Counsel, stand up and say, “We don’t have time.”
  - You start ringing the alarm bells.
    - You call outside counsel who immediately contacts data breach incident response company.
    - You begin contemplating who you need to inform of the data breach.
      - Cyber Insurance Carrier – Always call them first!
      - Board of Directors – Is it too soon?
      - Management Beyond Leadership Teams – What would you say?
      - Employees? – What would you say?
      - Business Partners and Customers– Probably too soon; you don’t know anything yet.
  - Lingering thoughts
    - What are your reporting obligations to governmental and regulatory authorities?
    - What is your litigation risk?





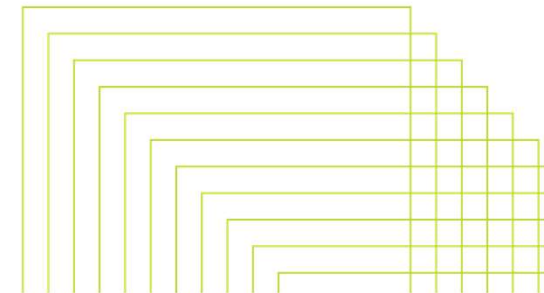
# Beginning to Look Like a Hurricane

- Saturday, June 29 – 3:00 P.M.
  - Data Breach Forensic Analyst
    - Has been given access to company's systems and is investigating.
  - CTO
    - Received another e-mail from hacker. He wants to be paid.
    - Threatens to release the data.
    - Gives additional "Proof of Life" to show he has exfiltrated documents.
  - IT Department
    - Trying to get systems back up and running. Assisting Data Breach Forensic Analyst in gaining access and investigation.
  - Data Breach Counsel
    - Urgently requests to know what kind of data company stores and where it is located.
    - Working with leadership to identify potential statutory and/or regulatory compliance obligations.



# Definitely a Hurricane – What Category?

- **Sunday, June 30 – 3:00 P.M.**
  - Data Breach Forensic Analyst
    - Ensured Threat Actor (new term) no longer has access to company's systems.
    - Threat Actor had access to Server 1.
    - Still investigating other servers.
    - Developing a timeline of what happened.
  - CTO
    - Needs to respond to Threat Actor. What should we say?
  - Data Breach Counsel
    - Needs to know what kind of information company stores so it can determine whether notifications need to be made and in which states.
    - What about business partners? What terms are in the contracts about notification?




# Hurricane At Least A Category 2

- Monday, July 1 – 10:00 A.M.
  - Data Breach Forensic Analyst
    - Threat Actor had access to Servers 1 and 2.
    - Still investigation other servers.
    - Almost complete with timeline of what happened.
  - CTO
    - With assistance of Data Breach Forensic Analyst, determines that Threat Actor is part of an OFAC sanctioned group. Even if company wanted to pay ransom, they can't.
    - So, they try to stall the Threat Actor.
    - Threat Actor lashes out and calls member of senior leadership directly.
  - Data Breach Counsel
    - What kind of data is contained in Servers 1 and 2?
      - IT is working on it.
  - General Counsel
    - Need to inform business partners.



# Hurricane – Category 5

- **Monday, July 1 – 3:00 P.M.**
  - Data Breach Forensic Analyst
    - Timeline Complete
      - On May 20, a shipping clerk in the Des Moines, Iowa warehouse clicked on a malicious Facebook link from the company's computer.
      - This gave the threat actor initial access to the system.
      - Over the next few days and weeks, the threat actor was able to make lateral movement into company's system, until it got an admin password.
      - The Threat Actor then began creating its own credentials and gave itself access to numerous systems, including Servers 1, 2, 6, and 7.
      - There are signs of exfiltration since Wednesday, June 5.
      - There were notifications of improper access, but improperly trained IT employees did not recognize threats and did not identify data breach.
- 

## MAY 2024

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

## JUNE 2024

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

## JULY 2024

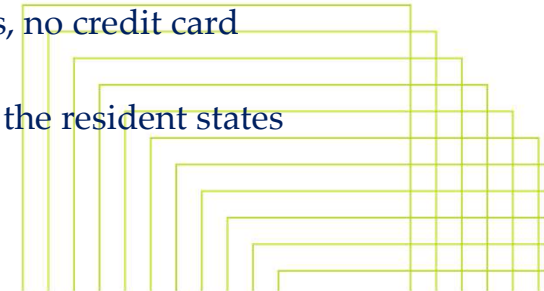
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			





# Hurricane – Category 5 Cont.

- Monday, July 1 – 3:00 P.M.
- CEO
  - Informs Board of Directors
    - Board of Directors demand daily meetings with CEO, CTO, COO and General Counsel for update on status.
  - Informs Business Partners
    - Each business partner demands meeting with CEO, CTO, COO and General Counsel.
    - Demands daily updates (to be drafted by General Counsel).
- CTO
  - Threat actor is frustrated with lack of movement and threatens to begin loading data on the dark web.
  - IT team is investigating the affected databases to see what customer data was impacted.
- Data Breach Counsel
  - IT team has identified that Server 1 contains customer names and addresses, no credit card information.
  - Counsel team investigating what notifications are necessary, by identifying the resident states of the affected customers.



# Hurricane – Category 5 Cont.



- Tuesday, July 2 – 9:00 A.M.
  - Data Breach Forensic Analyst
    - Completes its investigation to identify threat actor’s actions.
      - Servers 1, 2, 6, and 7 were accessed by threat actors and exfiltrated.
    - Drafts recommendations for additional security measures.
  - CEO
    - Daily meeting with Board of Directors, Business Partners and data breach response team.
  - CTO
    - Threat Actor is frustrated with lack of movement and uploads data to the Dark Web.
      - Data Breach Forensic Analyst downloads data and confirms exfiltration Threat Actor claimed.
    - IT team determines that Servers 2 and 6 contain no customer information.
    - IT team determines that Server 7 is a back up server that contains files from software implementation in the previous year.
      - But, identifies a file that contains every customer, address, credit card number and purchase history since the company’s beginning.

# Hurricane – Category 5 Cont.

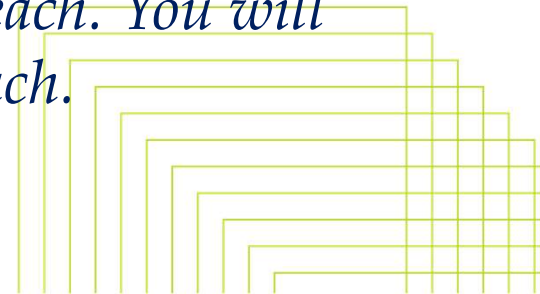
- Tuesday, July 2 – 9:00 A.M.
- Data Breach Counsel
  - Notifications to all customers whose data was on Server 1 and who was listed in the file found on Server 7 are necessary. This includes notifications in 42 states and requires notification of the Attorney General in 30 states.
  - Public statements are necessary.
  - Recommends to inform Board of Directors and Business Partners of the notifications necessary.
- Data Breach Notification Vendor
  - Provides draft notifications to General Counsel and Data Breach Counsel for review.
    - Offers 1 year of credit monitoring.



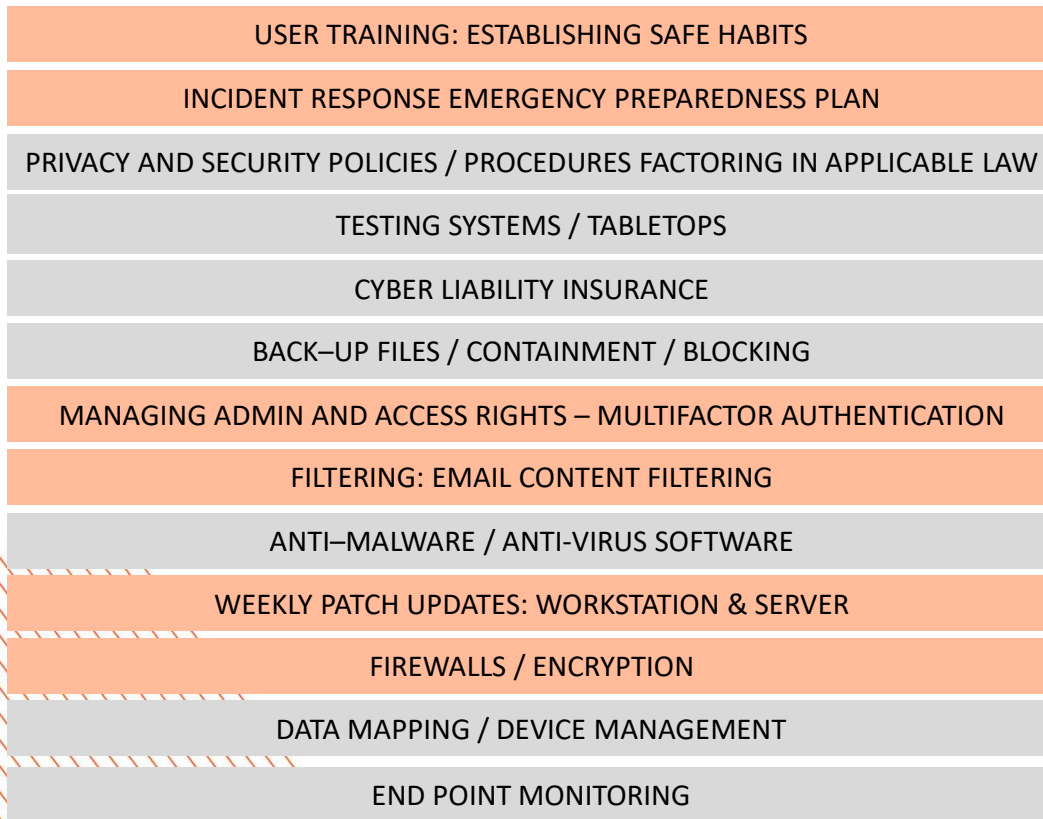
# Wisdom Earned the Hard Way

- Data Governance
  - If you know what type of data you keep and where you keep it, you will be steps ahead in the middle of the storm.
- Data Hygiene
  - Are you deleting the data you don't need?
  - Keeping data "just in case" is not a proper business purpose.
    - It can cost you in the event of a breach.
- Understand Your Legal Compliance Obligations
  - Don't wait until you've been impacted by an incident to determine whether you are subject to rapid reporting requirements, statutory notification obligations, or strenuous compliance programs such as the GDPR, PCI, etc.

*You will not be judged on whether you have a data breach. You will be judged by how you react to the data breach.*



# Managing Risk Through a Layered Approach







**H. Barber Boone**  
**Ridgeland Office**  
**(601) 985-4479**  
**[Barber.Boone@butlersnow.com](mailto:Barber.Boone@butlersnow.com)**



**Blythe K. Lollar**  
**Ridgeland Office**  
**(601) 985-4122**  
**[Blythe.Lollar@butlersnow.com](mailto:Blythe.Lollar@butlersnow.com)**

