
Our Incident Response Plan
goes something like this...
HELP!
HELP!

1. Which is the most volatile memory?

A. Hard disk
B. CPU cache
C. RAM
D. USB drive

Answer: B

14. Which option best describes an incremental backup?

A. Daily backups are appended to previous backups.
B. Daily backups are maintained in separate files.
C. Daily backups are appended to the full backup.
D. Daily backups are mirrored to the cloud.

Answer: B

15. Which option is most accurate regarding a recovery point objective?

A. The time after which the viability of the enterprise is in question
B. The point at which the most accurate data is available for restoration
C. The point at which the least accurate data is available for restoration
D. The target time full operations should be restored after disaster

Answer: B

16. Which team is made up of members from across the enterprise?

A. Dedicated full-time incident response team
B. Functional incident response team
C. Third-party incident response team
D. Expert incident response team

Answer: B

18. Prior to analysis, data should be copied from a hard disk utilizing which of the following?

A. Write protect tool
B. Block data copy software
C. Bit data copy software
D. Memory dump tool

Answer: C

Equifax Self-Inflicted Wounds

- Following the breach, they directed potential victims to a separate domain, equifaxsecurity2017.com, instead of building pages about the breach on their main, trusted website, www.equifax.com. The new site was riddled with bugs, and you could not rely on the application designed to let you know if you were part of the breach.
- The company's official Twitter account mistakenly tweeted a phishing link four times, instead of the company's actual breach response page.
- They waited at least a month before disclosing the breach, and company executives sold 2 million in stock holdings before the breach was disclosed.

When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.

- An intruder has broken into database(s) that contain personal information on an individual.

- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.

- A department or unit has not properly disposed of records containing personal information on an individual.

- A third party service provider has experienced any of the incidents above, affecting the organization’s data containing personal information.

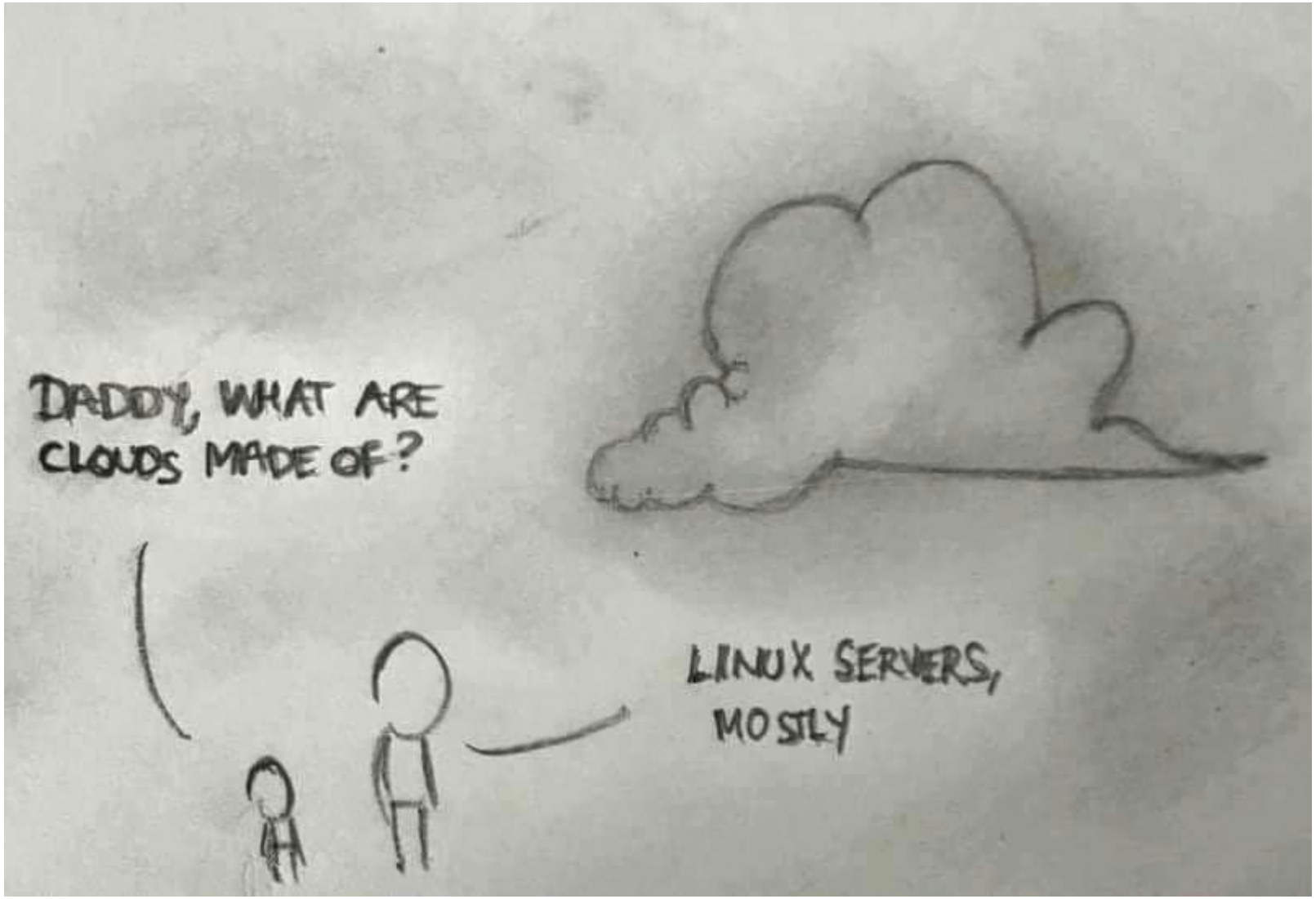
The following incidents may not require individual notification, the organization may conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

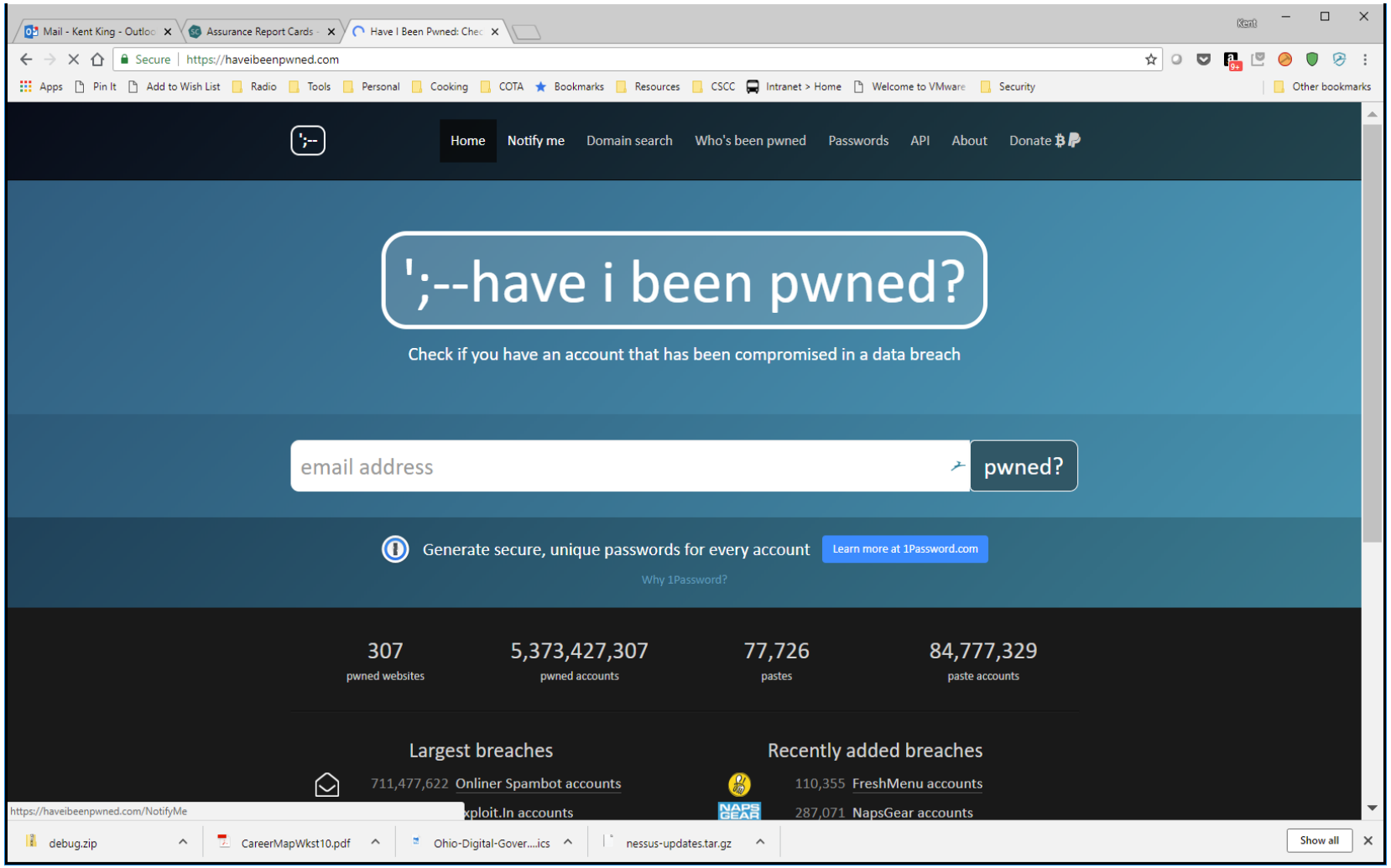
- The organization is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.

- The organization determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.

- An intruder accessed files that contain only individuals' names and addresses.

- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.


DADDY, WHAT ARE CLOUDS MADE OF?
LINUX SERVERS, MOSTLY



IT gets a notice from “Have I Been Pwned” that several non-IT staff IDs and passwords have been posted in a data breach from Fluffy Cloud Data, Inc.

IT Security interviews the employees involved and they state that they did use the Fluffy service, but no sensitive information was placed on the site.

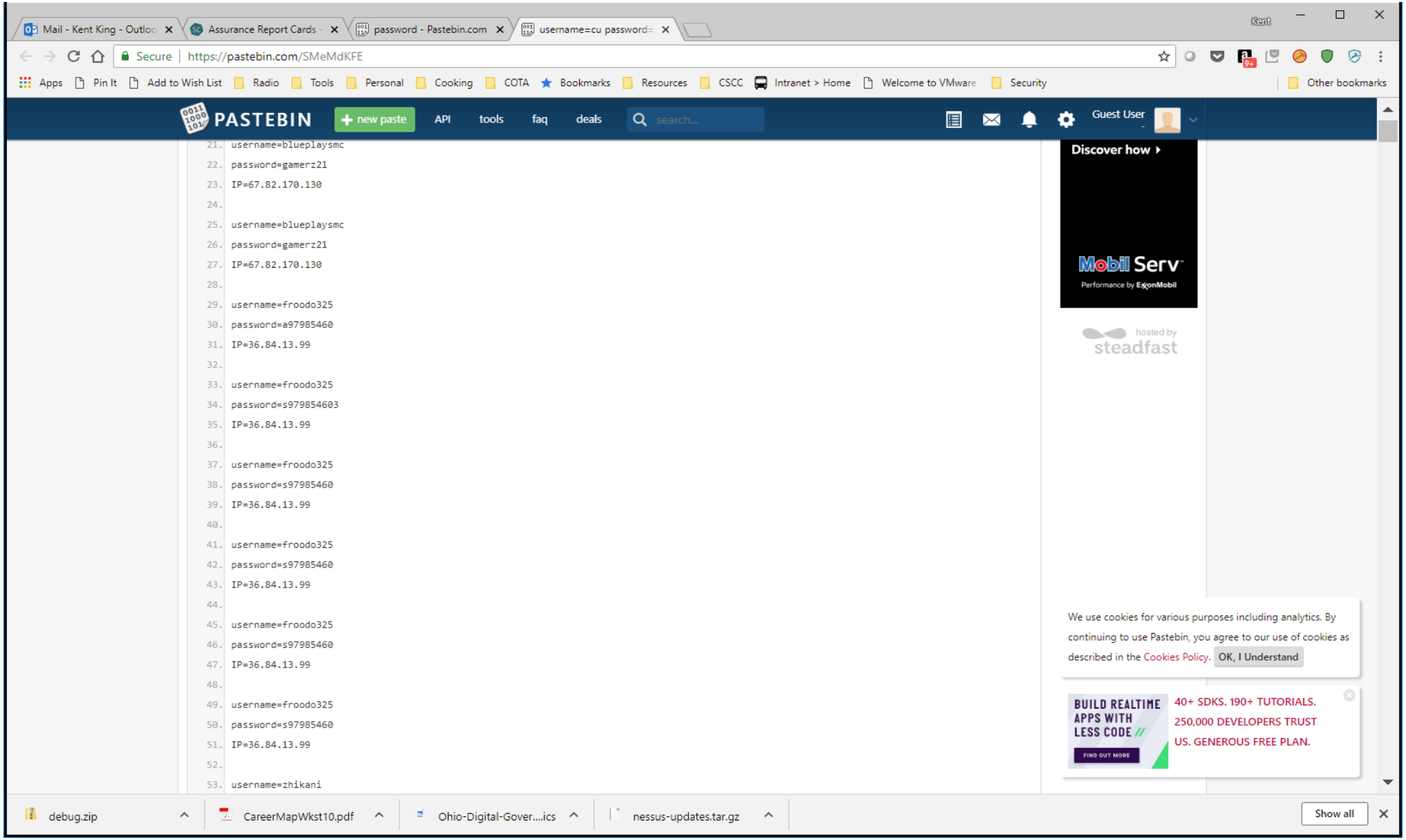
Based on what we know now:

1. How critical is this event?
2. Does anything have to be reported externally (regulators, etc.)
3. How far “up the chain” should this go internally?
4. What next steps will you recommend?

The Next Day

The company PR firm advises they have a reporter’s request for comment on the personal information of customers and employees found on Pastebin.

What do we tell the PR firm to say to the reporter?


Mail - Kent King - Outloc
Assurance Report Cards -
password - Pastebin.com
username=cu password=
Secure | https://pastebin.com/SMeMdKFE
Apps | Pin It | Add to Wish List | Radio | Tools | Personal | Cooking | COTA | Bookmarks | Resources | CSCC | Intranet > Home | Welcome to VMware | Security | Other bookmarks
PASTEBIN
+ new paste
API
tools
faq
deals
search...
Guest User
21. username=blueplaysmc
22. password=gamerz21
23. IP=67.82.170.130
24.
25. username=blueplaysmc
26. password=gamerz21
27. IP=67.82.170.130
28.
29. username=froodo325
30. password=a97985460
31. IP=36.84.13.99
32.
33. username=froodo325
34. password=s979854603
35. IP=36.84.13.99
36.
37. username=froodo325
38. password=s97985460
39. IP=36.84.13.99
40.
41. username=froodo325
42. password=s97985460
43. IP=36.84.13.99
44.
45. username=froodo325
46. password=s97985460
47. IP=36.84.13.99
48.
49. username=froodo325
50. password=s97985460
51. IP=36.84.13.99
52.
53. username=zhikani
Discover how
Mobil Serv
Performance by ExxonMobil
hosted by steadfast
We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy. OK, I Understand
BUILD REALTIME APPS WITH LESS CODE
FIND OUT MORE
40+ SDKS. 190+ TUTORIALS. 250,000 DEVELOPERS TRUST US. GENEROUS FREE PLAN.
debug.zip
CareerMapWkst10.pdf
Ohio-Digital-Gover....ics
nessus-updates.tar.gz
Show all

IT Security re-interviews the employees involved and now they come clean that they had stored numerous customer and employee files on the service because other options “took too long” and “were not accessible” when needed.

Based on what we know now:

1. How critical is this event?
2. Does anything have to be reported externally (regulators, etc.)
3. How far “up the chain” should this go internally?
4. What next steps will you recommend?

The Next Day

Working with IT Security, IT staff attempt to contact Fluffy to learn more about the breach. However, Fluffy was a startup, their VC funding dissolved in the breach and the only IT guy there is packing his box, it's his (and everyone's) last day. Fluffy Cloud Data is now another defunct start-up.

Based on what we know now:

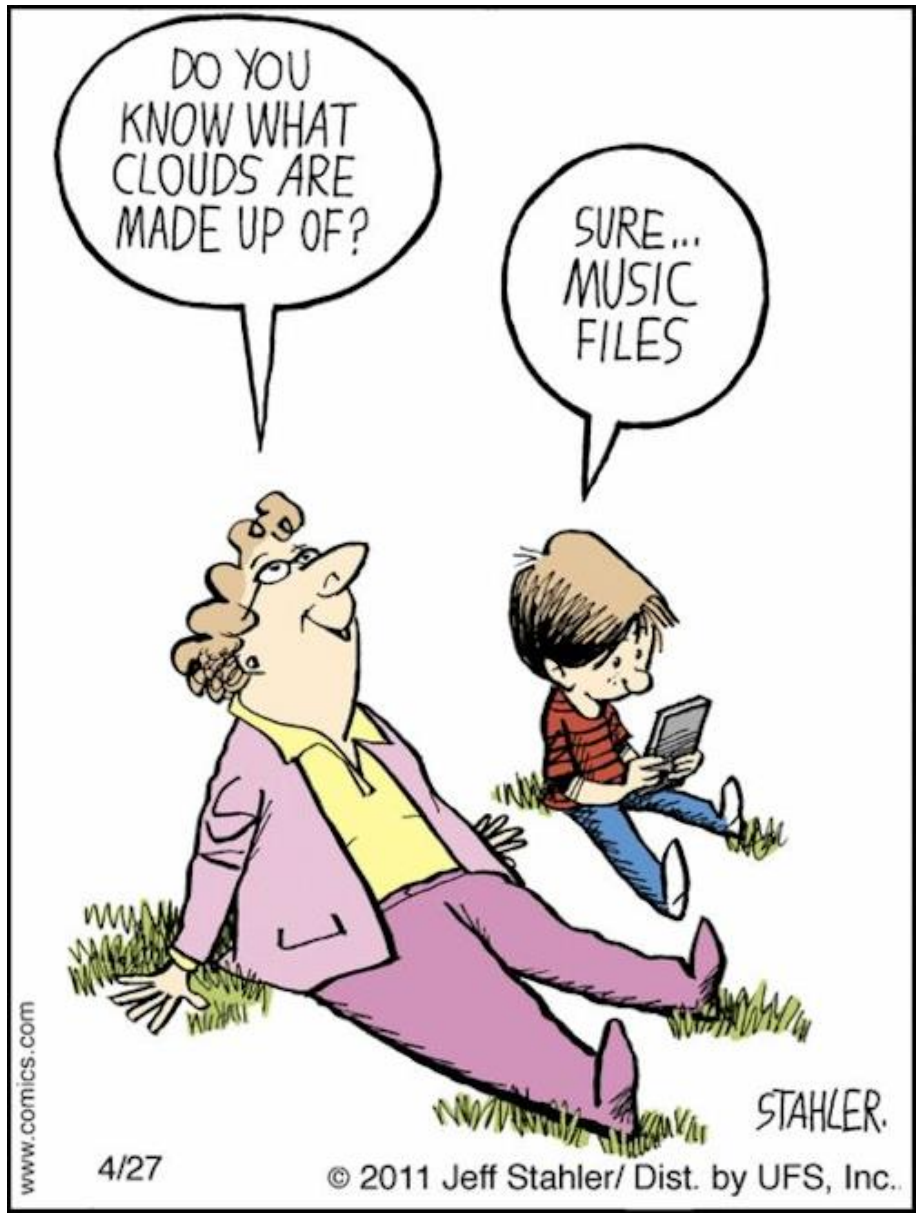
1. How critical is this event?
2. Does anything have to be reported externally (regulators, etc.)
3. How far "up the chain" should this go internally?
4. What next steps will you recommend?

A Week Later

Company is served with a class-action lawsuit involving numerous customers. The state AG has contacted the Legal Department requesting more information on the use of Fluffy Cloud Data, Inc.

Based on what we know now:

1. How critical is this event?
2. Does anything have to be reported externally (regulators, etc.)
3. How far “up the chain” should this go internally?
4. What next steps will you recommend?


DO YOU KNOW WHAT CLOUDS ARE MADE UP OF?
SURE... MUSIC FILES
STAHLER.
www.comics.com
4/27
© 2011 Jeff Stahler/ Dist. by UFS, Inc.

Lessons Learned

1. Preparation is the key to effective response.

2. Standard preventative and detection controls are critical to incident management.

3. Planning, practice, and testing processes must go beyond the checkbox.

4. Disclosure and public relations protocols must also be carefully planned and rehearsed.

5. Know before the worst happens how you will respond to customers and the public.

Lessons Learned

- Escalate a reported incident quickly and efficiently.
- Ensure that the entire response team has an understanding of the attorney client privilege and work products.
- Do not make overstatements or unsupported promises.
- Test all web sites thoroughly.
- Do not register domains too far in advance of public notification (there are caveats).
- Do not hire hackers to cover up your breach.