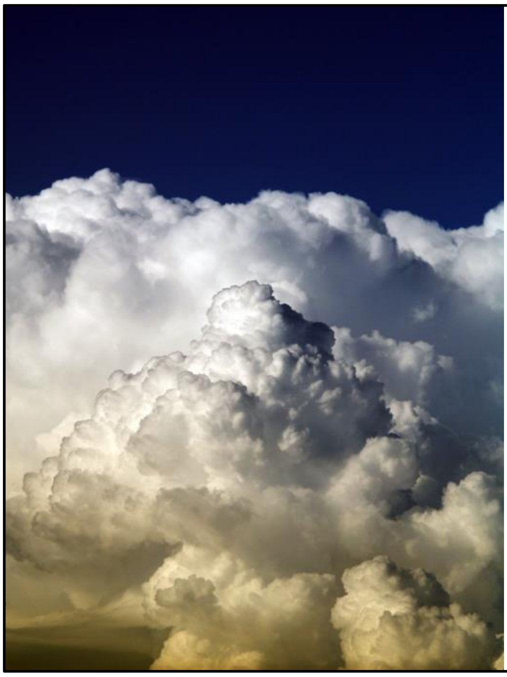
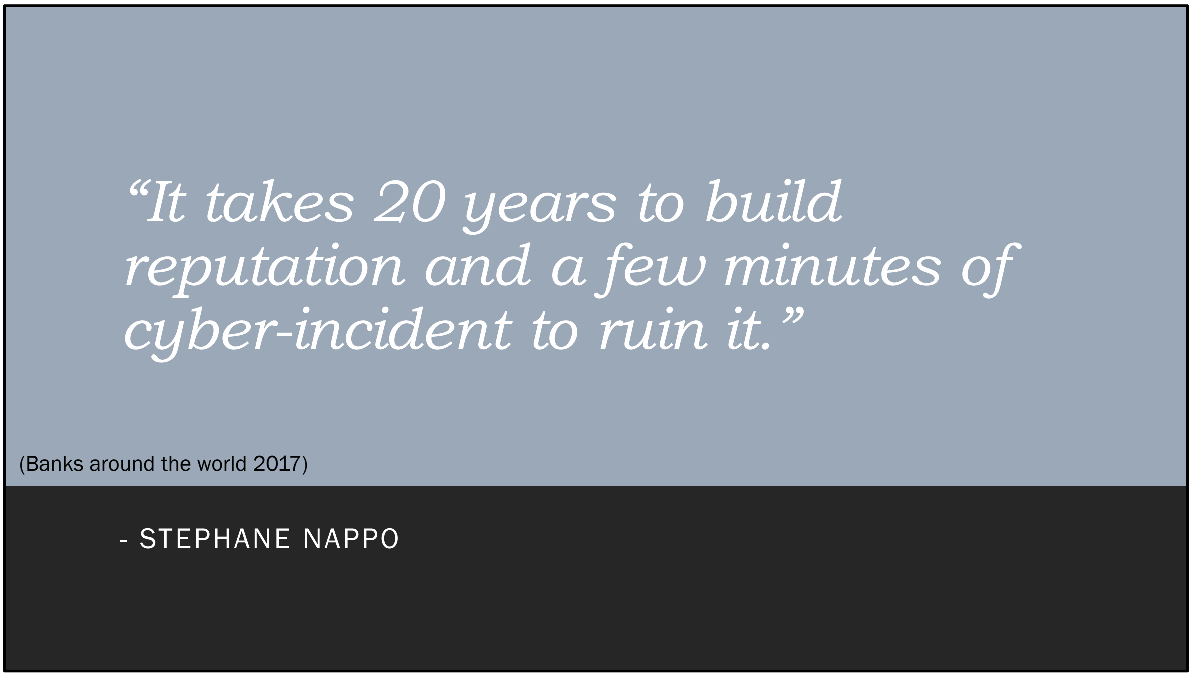


Cloud Storage

BY: ETHAN POWELL



> *"It takes 20 years to build reputation and a few minutes of cyber-incident to ruin it."*

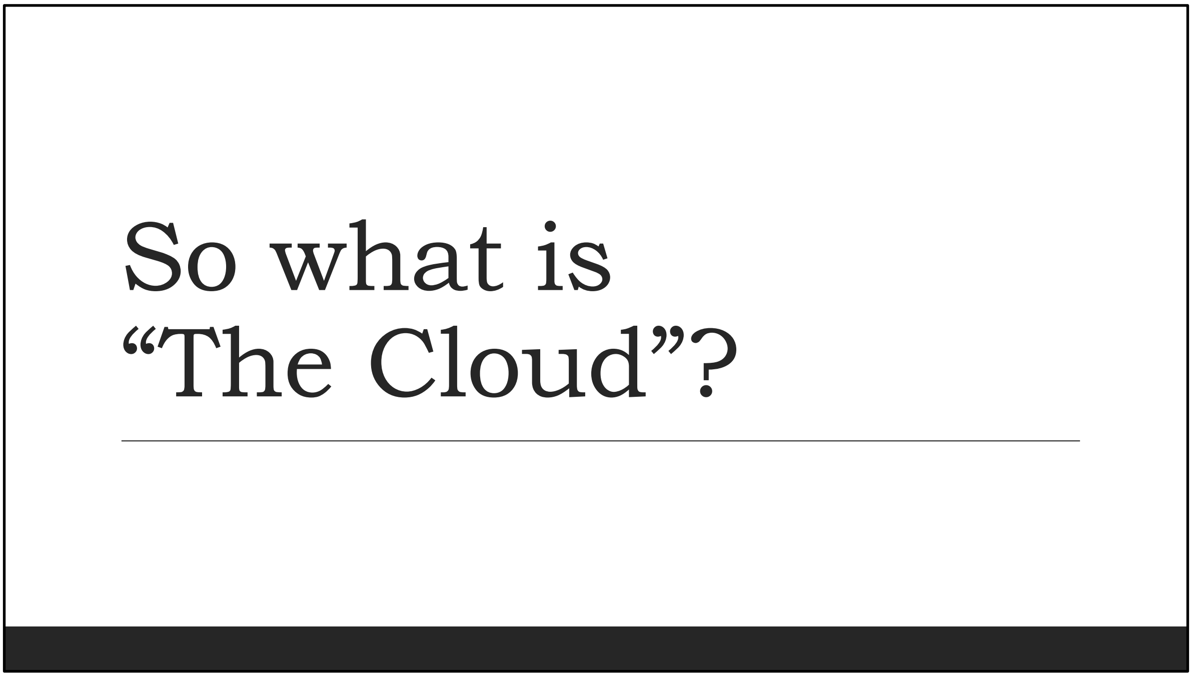
(Banks around the world 2017)

- STEPHANE NAPPO

Stephane Nappo is the Global Head of Information Security for the Société Générale International Banking pole. This banking industry is stationed in France. It ranks 7th in the world by assets according to relbanks.com (Banks around the world 2017).

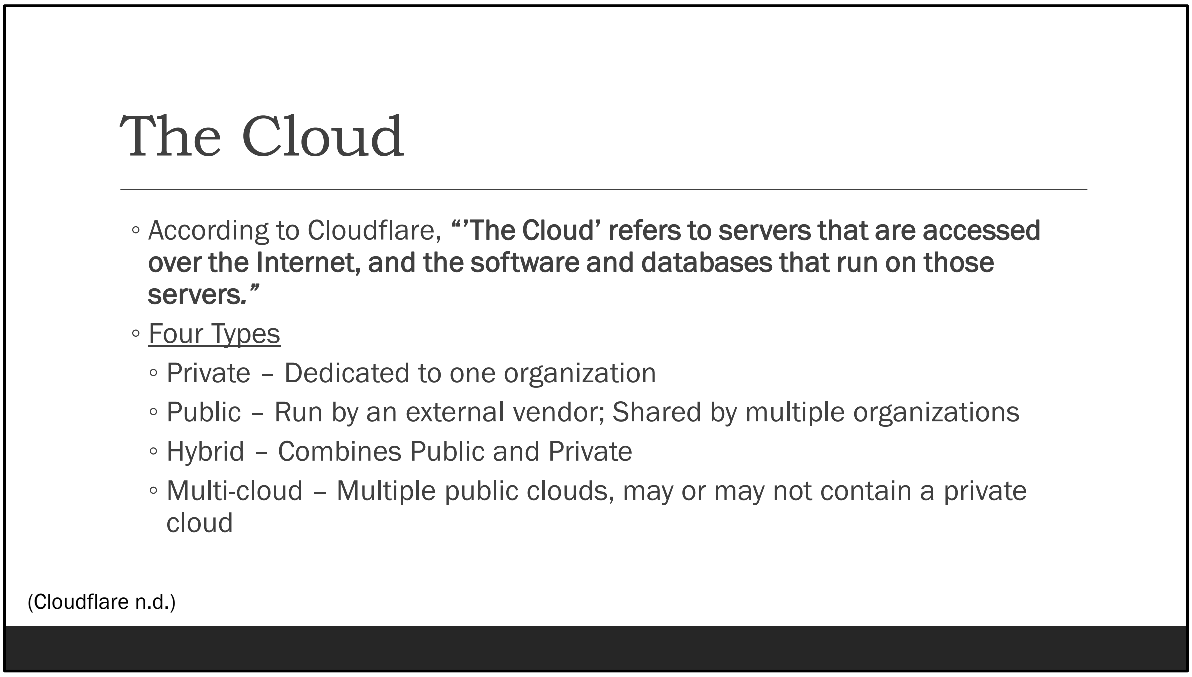
You can begin to see that if a security breach happened, massive repercussions would ensue.

Security is KEY!



So what is “The Cloud”?

We always hear about it, talk about it, but what really does the cloud entail?



The Cloud

- According to Cloudflare, **"'The Cloud' refers to servers that are accessed over the Internet, and the software and databases that run on those servers."**
- Four Types
  - Private – Dedicated to one organization
  - Public – Run by an external vendor; Shared by multiple organizations
  - Hybrid – Combines Public and Private
  - Multi-cloud – Multiple public clouds, may or may not contain a private cloud

(Cloudflare n.d.)

The cloud is essentially a big warehouse that is filled Servers that hold data or run software. This then allows for people to access this data from anywhere in the world as long as they have an internet connection. Seems pretty useful right?

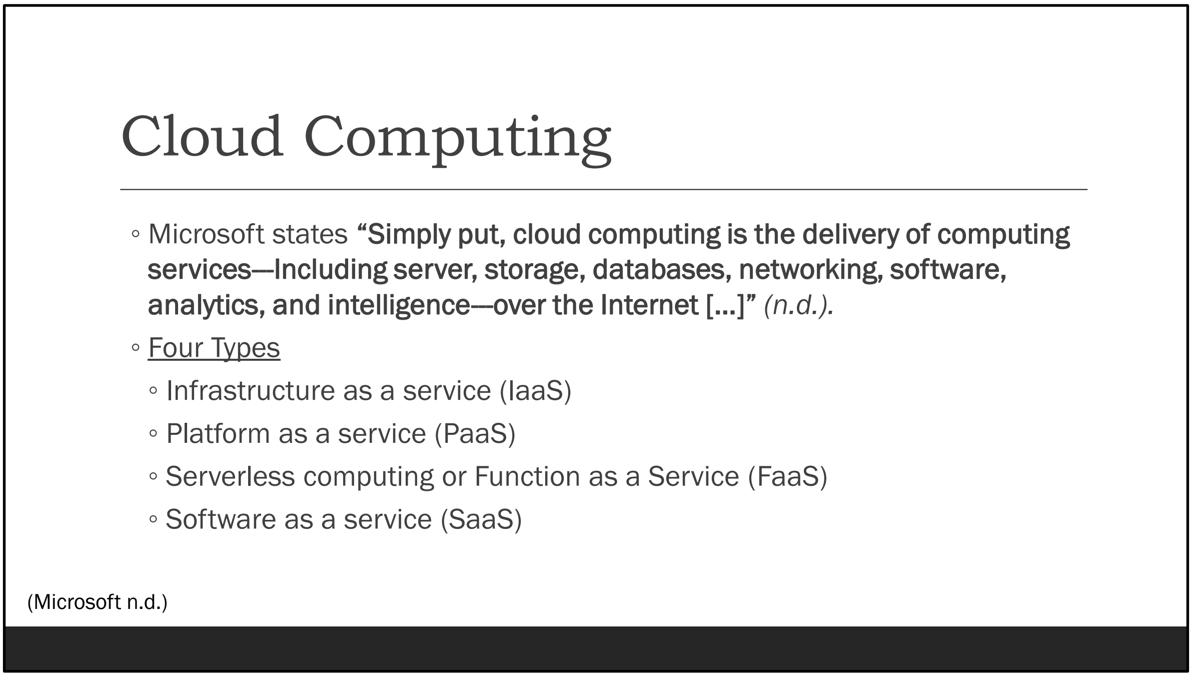
There is not just one type of cloud, they are divided into 4 groups.

Private – This is your home cloud. Usually this cloud refers to a network enabled hard-drive that is in your home that allows for file upload and transfer. Useful for storing files and pictures that you want access to anywhere in the house or for backups of a PC in your home. This also refers to personal company clouds. Private server farms that are owned and operated by the company for roughly the same reasons, File transfer, backups etc.

Public clouds – This is where Google Drive, Amazon Drive, and Dropbox come in. These clouds are owned and operated by companies who rent or provide access to third party individuals. These clouds not only are useful for storing information to be access at home, but also anywhere in the world. These large companies have access to a global network that allows for the cloud to be accessed from anyone with an internet connection, providing useful tools for data transfer and file storage to students and companies alike.

- Hybrid
    - Combines public and private
    - Usually made for companies and small businesses
    - If data overflows on private, can be moved to public

- Multi-cloud
    - Makes use of multiple public and/or private clouds
    - Can be useful for very large data centers and data collection
    - Can have organized clouds based on purpose
    - Usually maintained from multiple third parties



Cloud Computing

- Microsoft states **"Simply put, cloud computing is the delivery of computing services—Including server, storage, databases, networking, software, analytics, and intelligence—over the Internet [...]"** *(n.d.).*
- Four Types
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Serverless computing or Function as a Service (FaaS)
  - Software as a service (SaaS)

(Microsoft n.d.)

- Cloud computing is the transfer of data over the internet simply put

- Infrastructure as a service (IaaS)
  - Rent IT infrastructure like a subscription style
  - Pay monthy/yearly/weekly/etc.
  - Easily scaleable / Pay for what you need
  - Very modular
  - Pay for the are and infrastructure but have to do all the legwork
  - Like buying a plot of land to build the house

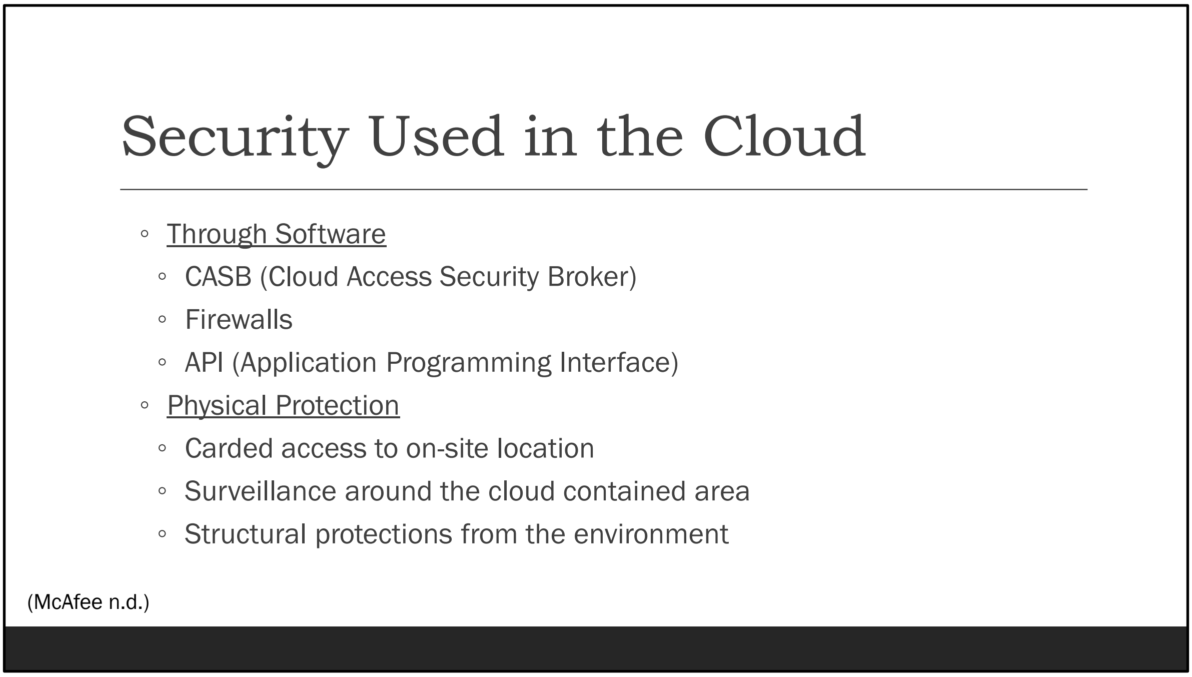
- Platform as a service (PaaS)
  - Rented from third party or manage yourself
  - Includes all from IaaS but includes more development tools and personalization
  - Mange what you are making, the third party takes care of the semantics
  - Mostly for analytics and virtual operating systems
  - Not used for hosting the application, mostly for creating
  - Like buying tools and land to build a house

- Serverless computing or Function as a Service (FaaS)
    - No need to manage infrastructure
    - As software scales, third party scales to accommodate
    - Servers still run the code, but what is involved with management is invisible to the developer
    - Machines aren't dedicated to one service
    - Imagine renting parts of a house as needed

- Software as a service (SaaS)
    - Cloud based apps on the internet
    - Email, office tools, calendars, etc…
    - Rent from third party or manage yourself
    - Quickest to get up and running
    - Third party does everything
    - Like renting a house

Analogy courtesy of Cloudflare 2017

How is it secured?



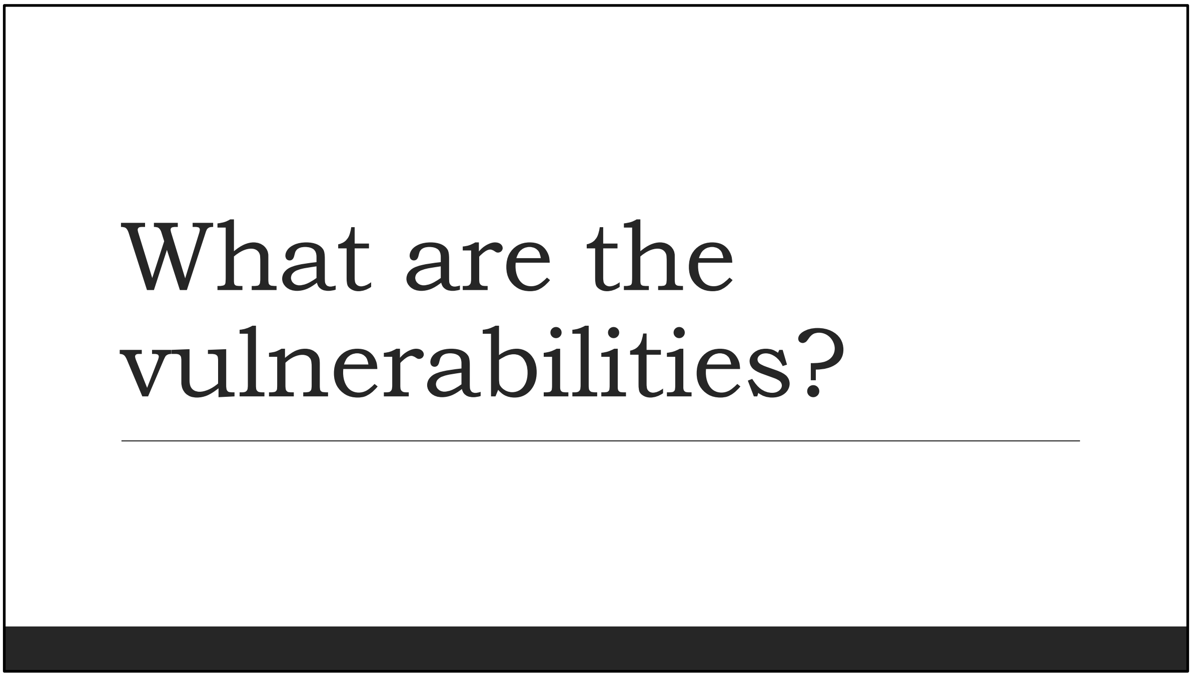
Security Used in the Cloud

- Through Software
  - CASB (Cloud Access Security Broker)
  - Firewalls
  - API (Application Programming Interface)
- Physical Protection
  - Carded access to on-site location
  - Surveillance around the cloud contained area
  - Structural protections from the environment

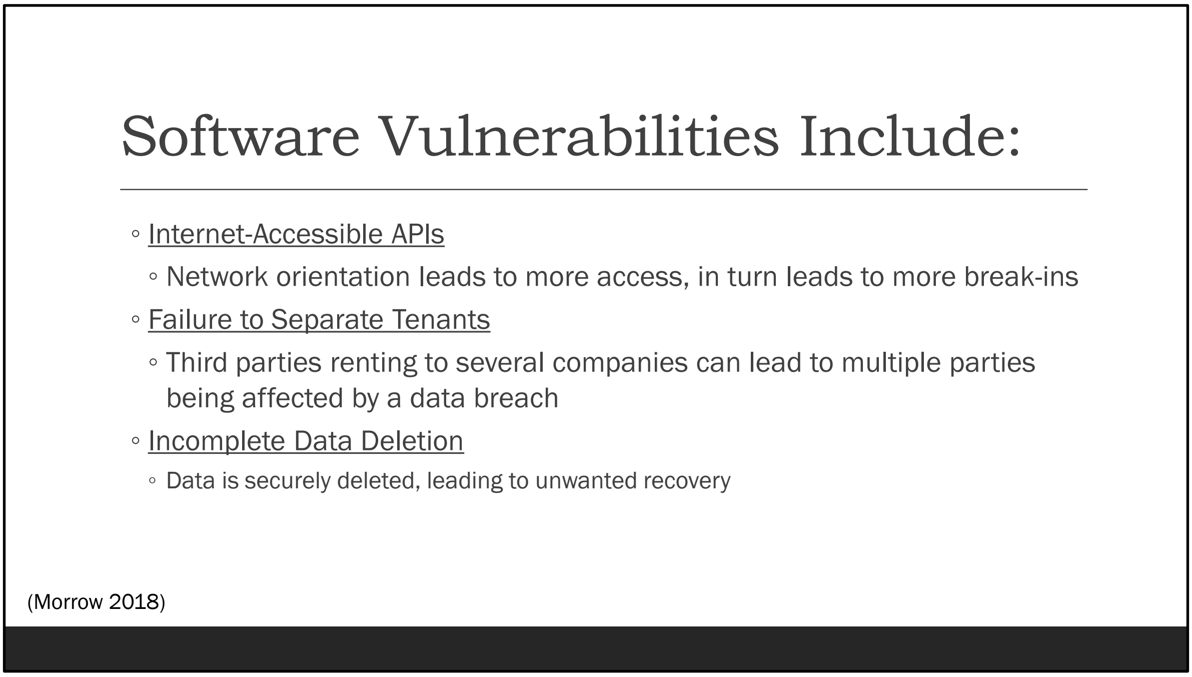
(McAfee n.d.)

- CASB (Cloud Access Security Broker)
  - Cloud-hosted/On-premise
  - Policy enforcement
  - Think of a firewall, but also controls how data is accessed and managed
  - Similar to what companies use on company property such as laptops and phones
  - Can automatically learn what vulnerabilities could occur based on application usage
- Firewalls
  - Monitor control of connections to the cloud
  - Can be adjusted to only allow authorized individuals from a remote location
  - Very similar to firewalls on personal machines
- API
  - Monitors connections to the cloud
  - Can determine location, type of access, what OS the accessor is running, IP Address, etc…
  - Huge surveillance
  - Doesn’t prevent, only monitors
  - Used for data collections and in the improvement of other security styles

- Allows for interaction between user and cloud



What are the vulnerabilities?

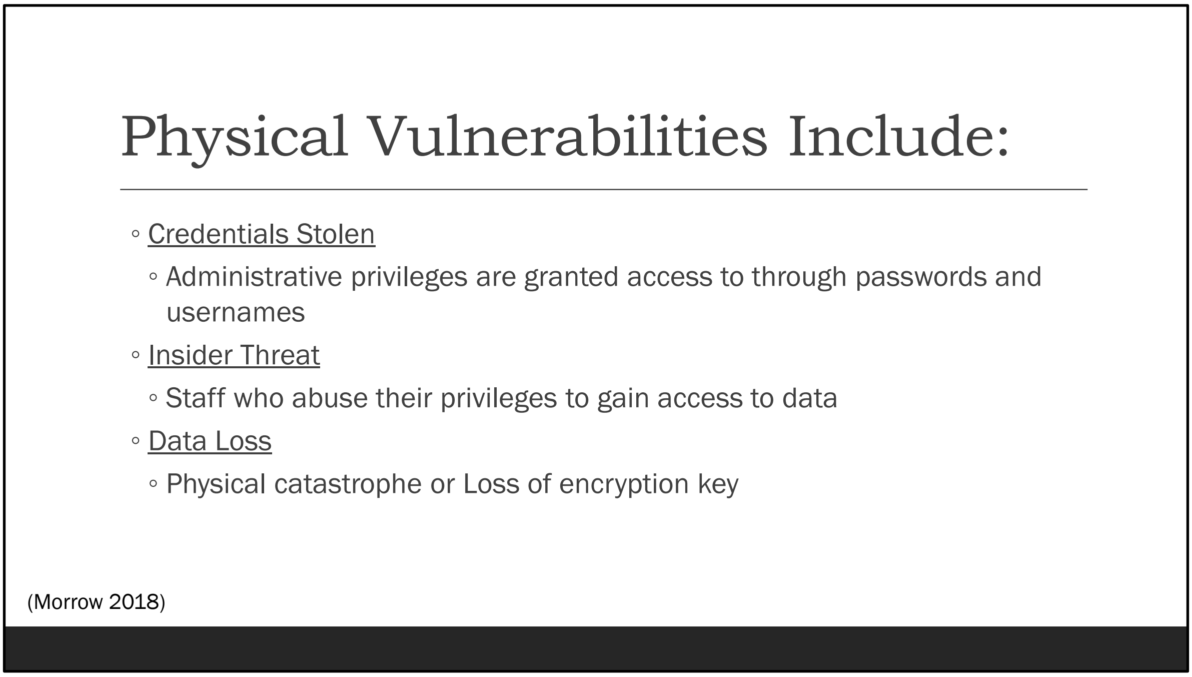


Software Vulnerabilities Include:

- Internet-Accessible APIs
  - Network orientation leads to more access, in turn leads to more break-ins
- Failure to Separate Tenants
  - Third parties renting to several companies can lead to multiple parties being affected by a data breach
- Incomplete Data Deletion
  - Data is securely deleted, leading to unwanted recovery

(Morrow 2018)

- APIs
  - Can become compromised from remote locations
  - More connections than a normal PC makes it harder to track
  - Can lead to unwanted downloads and access of sensitive data
- Separation of Tenants
  - Third parties rent to multiple companies, leading to the same cloud used by several organizations
  - One cloud becomes compromised taking several organizations with it
  - Becomes expensive to dedicate one cloud to each organization
  - No security between clouds, only on access -> bad practice
- Incomplete Deletion
  - Data deletion can’t be verified by the user
  - Deletion left in the hands of the Third party
  - When the company changes hands, residual data could be left
  - Data visible to all who use the cloud, ties into above topic



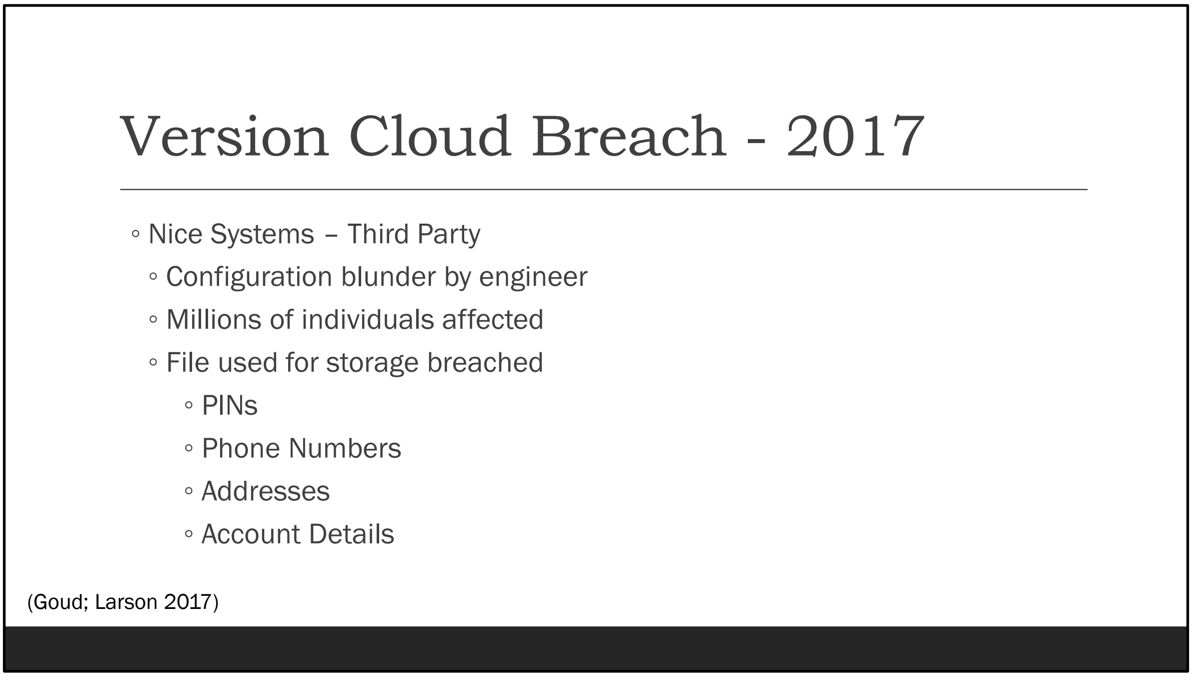
Physical Vulnerabilities Include:

- Credentials Stolen
  - Administrative privileges are granted access to through passwords and usernames
- Insider Threat
  - Staff who abuse their privileges to gain access to data
- Data Loss
  - Physical catastrophe or Loss of encryption key

(Morrow 2018)

- Stolen Credentials
  - Most common type of attack
  - Sticky-note with password written on it
  - Doesn't have to be physically/directly stolen, can be obtained through social engineering
- Insider Threat
  - Abuse of power
  - Very difficult to detect
  - Can be prevented by monitoring employee activities and separation of duties
- Data Loss
  - Back up data to prevent
  - Can be fault of consumer
  - Out of the hands of the provider for majority

How have these been exploited?

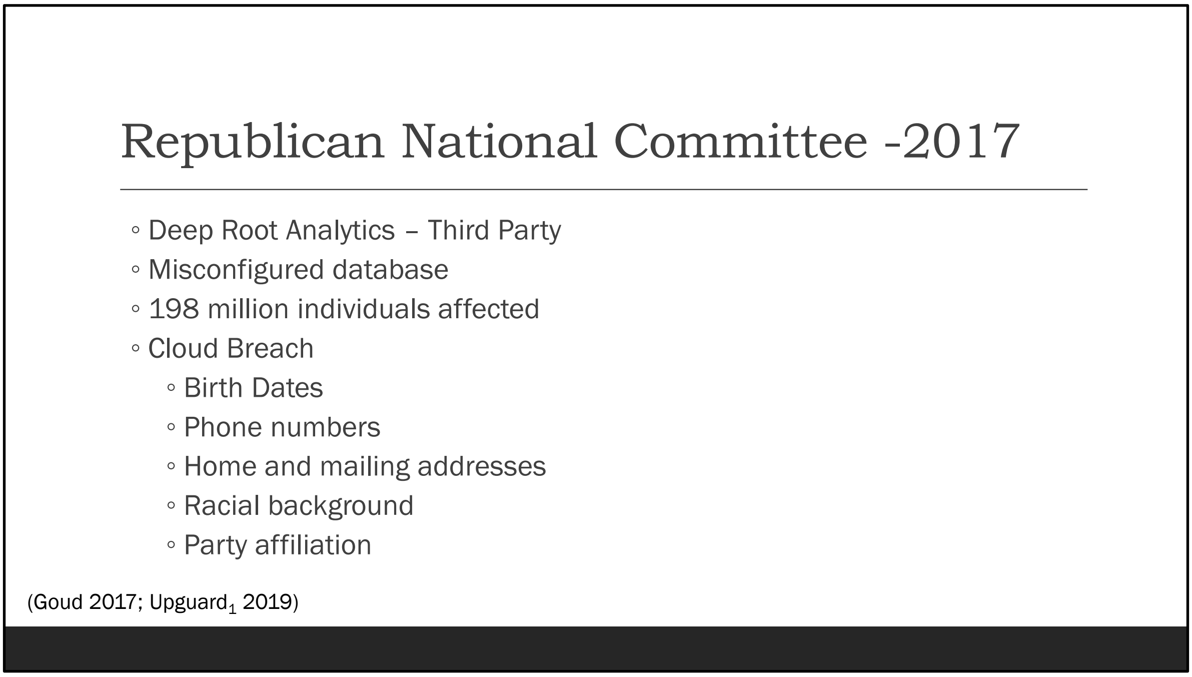


Version Cloud Breach - 2017

- Nice Systems – Third Party
  - Configuration blunder by engineer
  - Millions of individuals affected
  - File used for storage breached
    - PINs
    - Phone Numbers
    - Addresses
    - Account Details

(Goud; Larson 2017)

- Nice Systems
  - Was the third-party provider for Version’s cloud
  - Private cloud
  - Caused by Nice systems, Third party’s fault
  - Configuration error
  - Could have been prevented

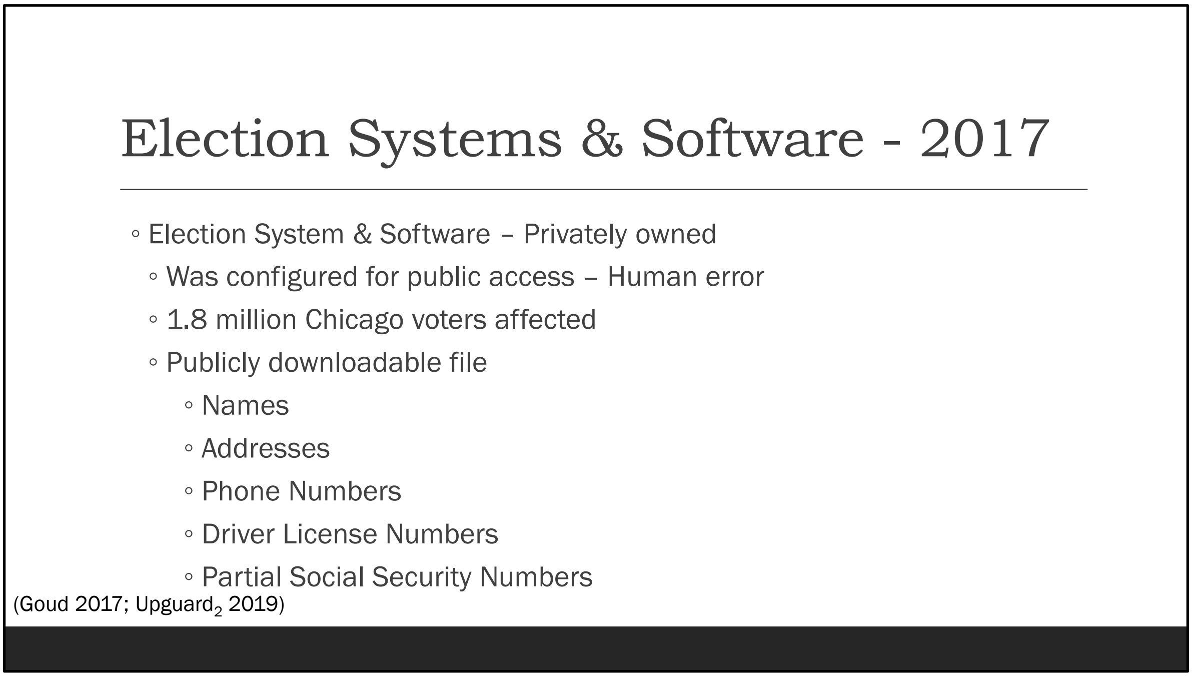


Republican National Committee -2017

- Deep Root Analytics – Third Party
- Misconfigured database
- 198 million individuals affected
- Cloud Breach
  - Birth Dates
  - Phone numbers
  - Home and mailing addresses
  - Racial background
  - Party affiliation

(Goud 2017; Upguard$_1$ 2019)

- Deep Root Analytics
  - Publicly accessible cloud
  - 1.1 terabytes of unsecured information
  - Technical mistake made by third party
  - Configuration error
  - Could have been prevented

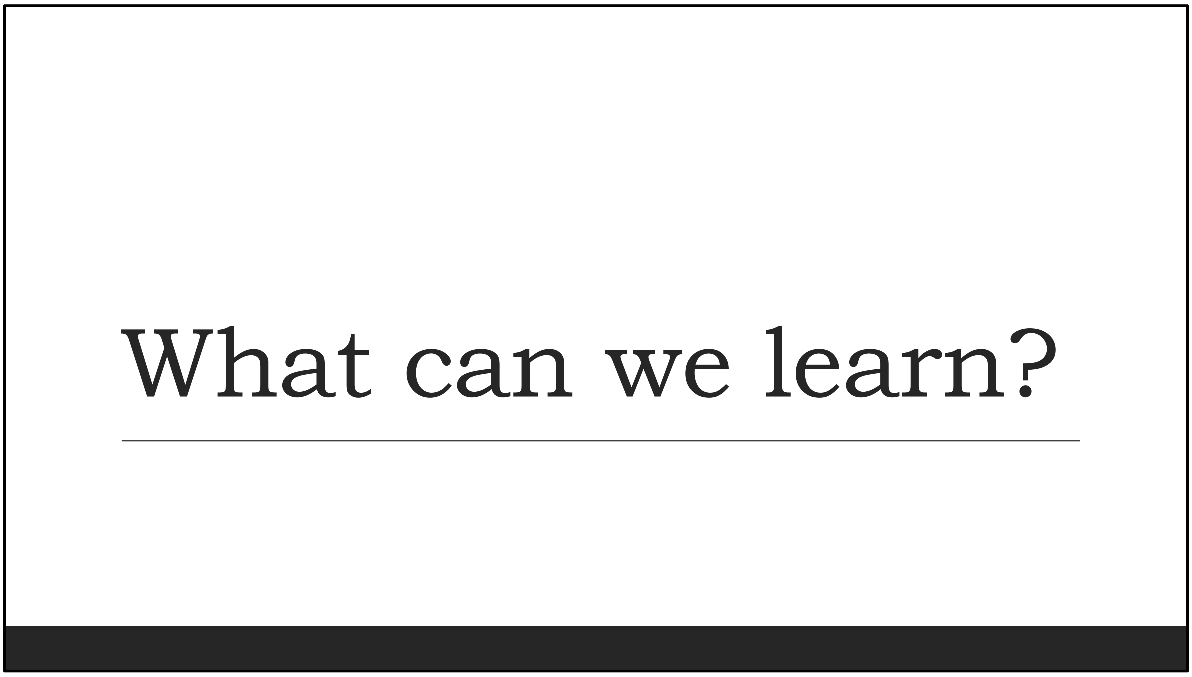


Election Systems & Software - 2017

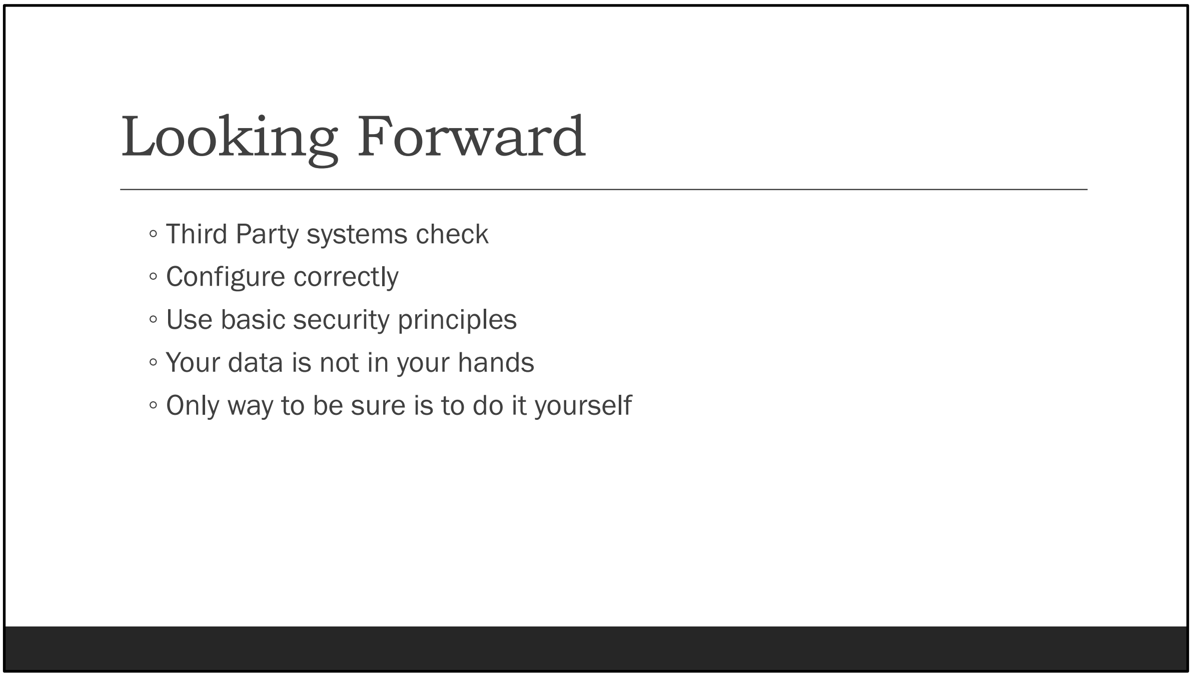
- Election System & Software – Privately owned
  - Was configured for public access – Human error
  - 1.8 million Chicago voters affected
  - Publicly downloadable file
    - Names
    - Addresses
    - Phone Numbers
    - Driver License Numbers
    - Partial Social Security Numbers

(Goud 2017; Upguard$_2$ 2019)

- Election Systems & Software
  - Privately owned cloud
  - Misconfigured from the start
  - Public access allows for any connection
  - 5 GB of data compromised
  - Preventable



What can we learn?

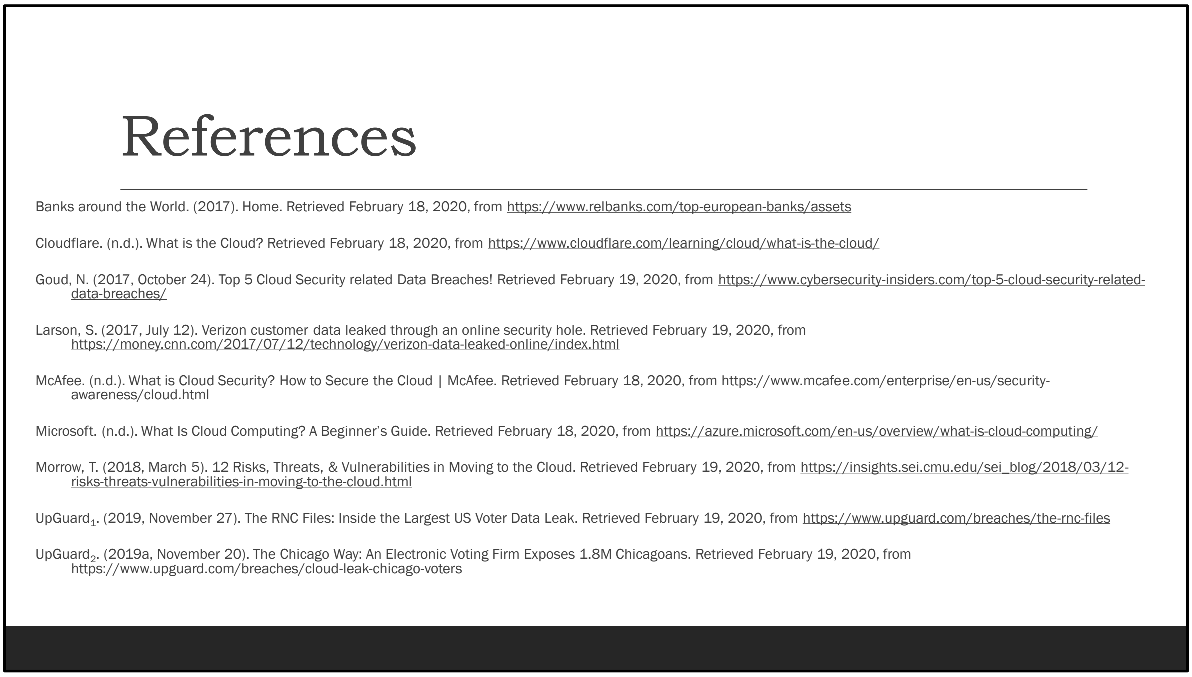


Looking Forward

- Third Party systems check
- Configure correctly
- Use basic security principles
- Your data is not in your hands
- Only way to be sure is to do it yourself

- Third Party
  - Check Reliability of the third party
  - Ask to check their data protection configuration
  - Try putting data on multiple clouds on multiple third parties
- Configuration
  - MAKE SURE YOUR CLOUD IS CONFIGURED CORRECTLY
  - Configuration mistakes can easily lead to data breaches
  - Double and triple check configuration before shipping out
  - Learn common configuration mistakes
- Basic security principles
  - Strong passwords
  - Protect your credentials
  - Encryption
  - Employee monitoring
- Data is not yours
  - Understand that you don’t have control of your data
  - Verification of data security is much more difficult
  - Third party is responsible for security of your data
  - You are responsible for encryption and credential storage

- Do it yourself
    - Uneasiness with third parties
    - Configure your own cloud so you are sure



References

Banks around the World. (2017). Home. Retrieved February 18, 2020, from https://www.relbanks.com/top-european-banks/assets

Cloudflare. (n.d.). What is the Cloud? Retrieved February 18, 2020, from https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

Goud, N. (2017, October 24). Top 5 Cloud Security related Data Breaches! Retrieved February 19, 2020, from https://www.cybersecurity-insiders.com/top-5-cloud-security-related-data-breaches/

Larson, S. (2017, July 12). Verizon customer data leaked through an online security hole. Retrieved February 19, 2020, from https://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html

McAfee. (n.d.). What is Cloud Security? How to Secure the Cloud | McAfee. Retrieved February 18, 2020, from https://www.mcafee.com/enterprise/en-us/security-awareness/cloud.html

Microsoft. (n.d.). What Is Cloud Computing? A Beginner's Guide. Retrieved February 18, 2020, from https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Morrow, T. (2018, March 5). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. Retrieved February 19, 2020, from https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

UpGuard$_1$. (2019, November 27). The RNC Files: Inside the Largest US Voter Data Leak. Retrieved February 19, 2020, from https://www.upguard.com/breaches/the-rnc-files

UpGuard$_2$. (2019a, November 20). The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans. Retrieved February 19, 2020, from https://www.upguard.com/breaches/cloud-leak-chicago-voters