



INTERPOL

Cybercrime and electronic evidence in the cloud- challenges

Sungjin HONG
Digital Crime Officer
Cyber Directorate

Contents

- **Referential Cases**
 - Access
 - Size of data
- **Challenges**
- **Silver lining**

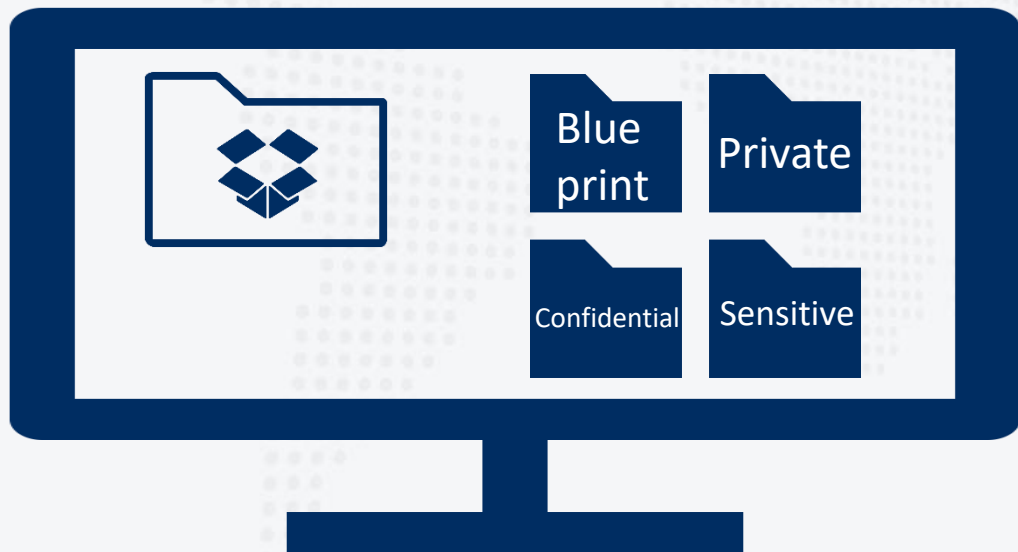
- **Korean Nuclear Powerplant case**

- On December 23, 2014, Korea Hydro & Nuclear Power (or KHNP) announced that its systems had been compromised.



- **Korean Nuclear Powerplant case**

- The group insisted that they gained access to the internal system and stole blueprints of nuclear reactor, details on various support systems, and personal data on over 10,000 employees. The stolen data also was distributed through Dropbox etc.



- **Korean Nuclear Powerplant case**

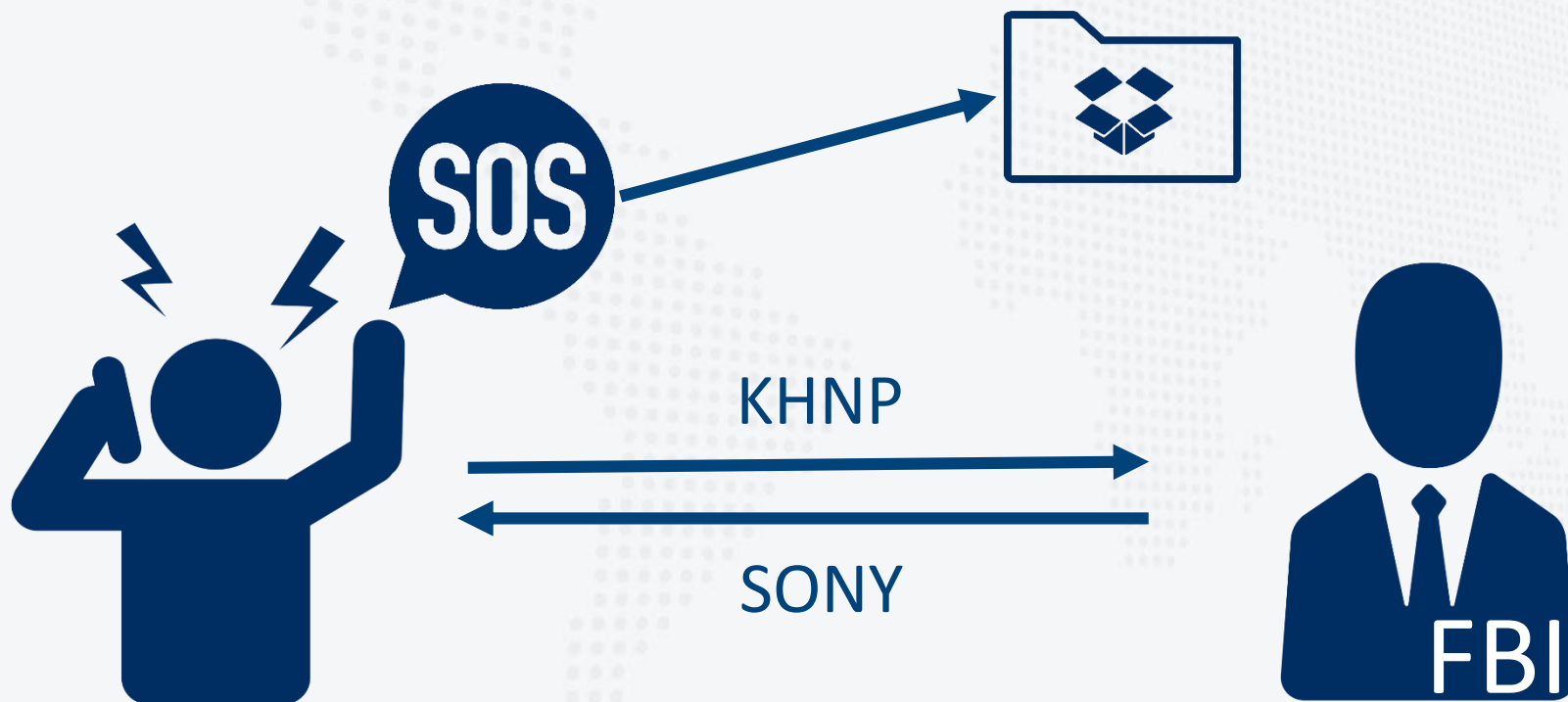
- The subject also posted on its Twitter that they would release additional data and explode the power plant unless the power plans is not stopped till Christmas



- **Korean Nuclear Powerplant case**

- Two solutions

- Emergency data disclosure request
- Joint operation with FBI



- **Soranet case**

- The biggest community offering obscene material including Child Abuse Material and prostitution agency since 2000



- **Soranet case**

- They used a bullet-proof hosting service of Netherland



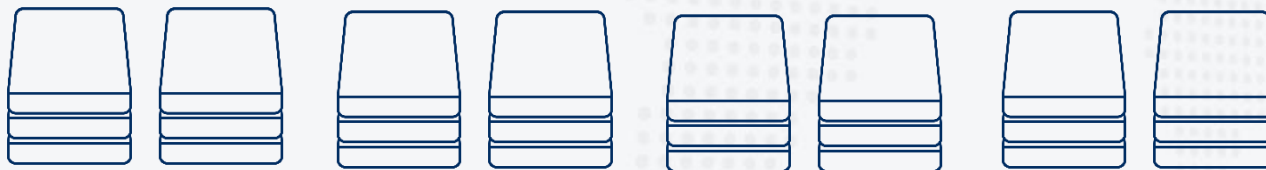
- **Soranet case**

- Finally, the Dutch police succeed to shut it down and copied the whole data



- **Soranet case**

- The size of data is 120 TB. The Korean Police's Digital Forensic unit got new agony



- **Stage of Challenges**

- Access

- Different or multiple jurisdiction
- International cooperation such as MLAT
- Chain of Custody

- Analysis

- Size
- Decrypted
- Deleted

- **Warrant**

- Google, MS, FB and Twitter etc

- Admit data disclosure request based on a warrant issued by its own countries' criminal court

- But, extent of data is limited on user information and logs, not includes contents information

- Amazon, Oracle, Dropbox ?

- **MLAT**

- It's a bit nervous things to do as a cybercrime investigator

On July 26, 2011, the subject compromised a server of SK Communications and exfiltrated 36 million users' information

We found that the perpetrator used IP addresses belonged to USA and request logging information during July 2011.



USDOJ sent something
pursuant your MLAT
request



Good News!!!



October 2012





Electronic and
Physical...

Where is the electronic
data we requested?



What's wrong with me?

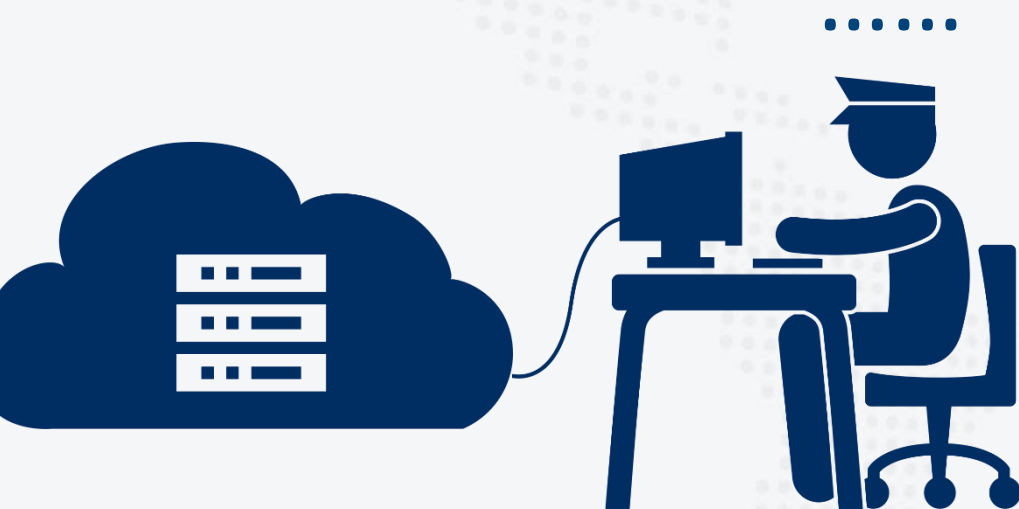


The boss ordered you type them in an Excel file



- **Chain of custody**

- We don't have enough knowledge about each cloud service's system
- Without owner's cooperation, nothing will be done



You'll
Never find
That..



- **Too big data size? Decrypted? Deleted?**

I cannot find any decryption key for the server

I cannot recover any deleted files

Company policy..

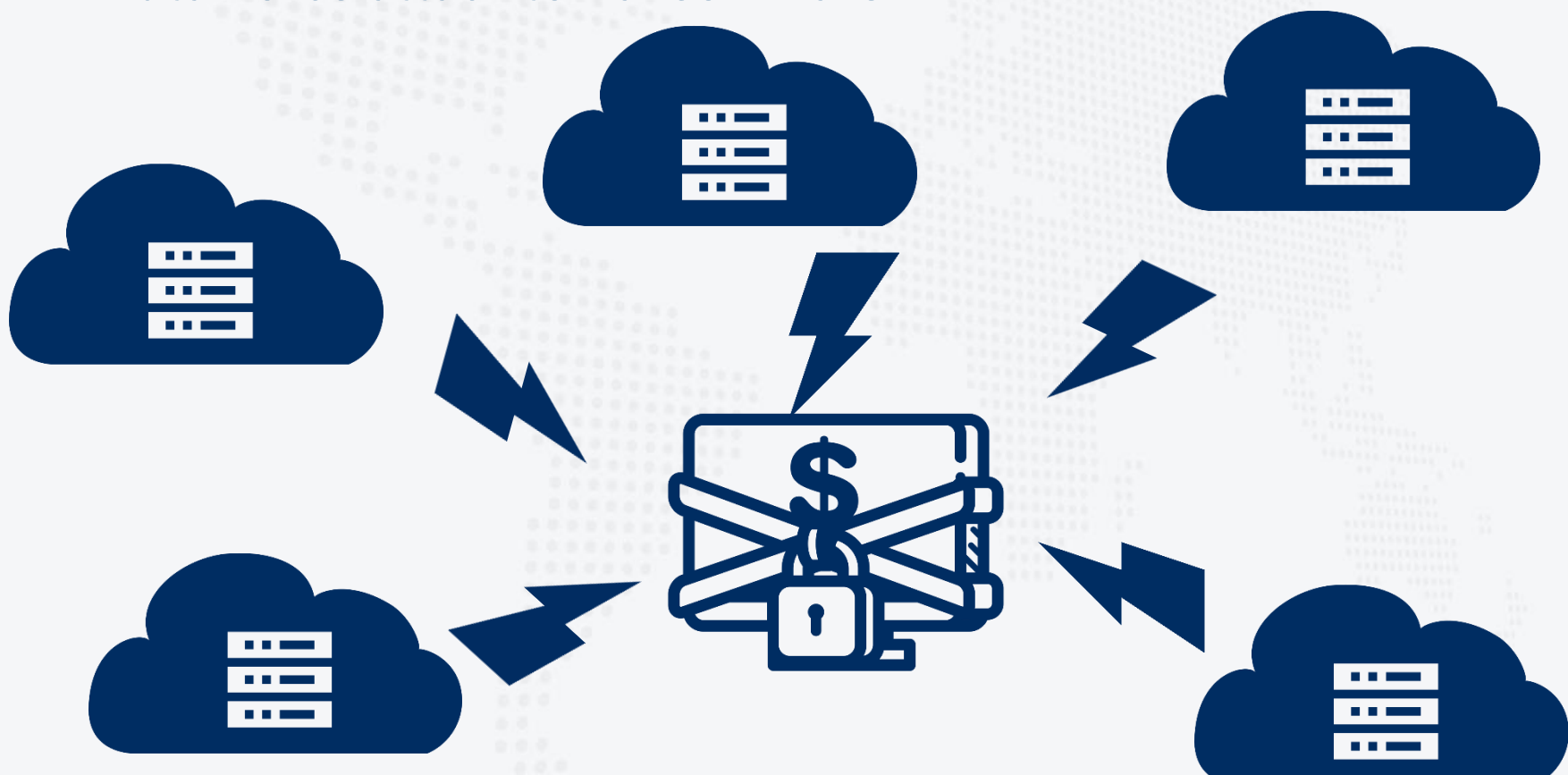
So, we're loved by criminal customers...



- **It's just a kind of tool.**

- Good or Evil depends on who uses

- Cloud computing environment can extradite digital forensic etc
- Brutal force attack to Ransomware?



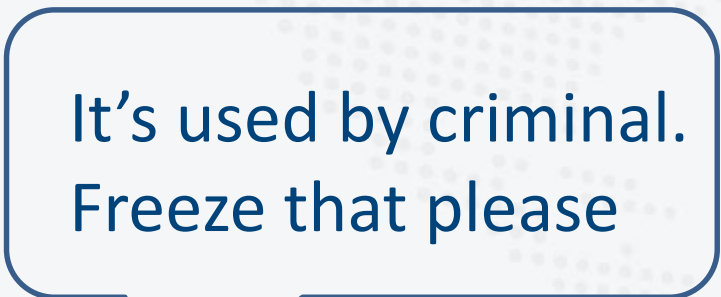
- **It's just a kind of tool.**
 - Good or Evil depending on who uses
 - Enable speedy exchange of data in MLAT



- **It's just a kind of tool.**

- Good or Evil depending on who uses

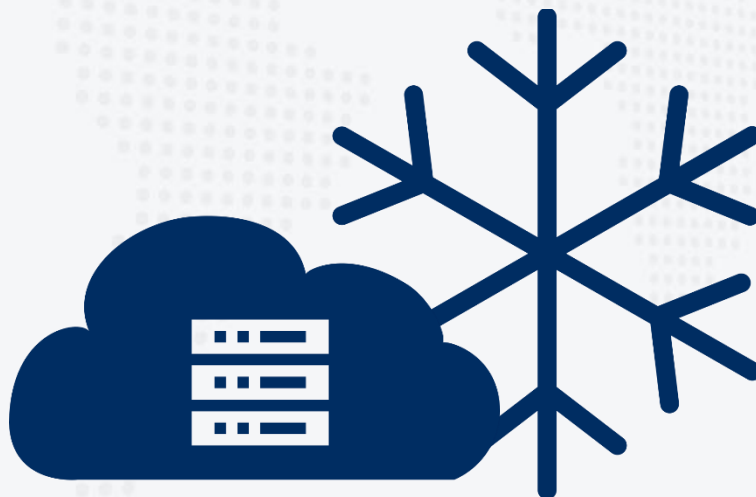
- By Preservation request, crime scene can be preserved



It's used by criminal.
Freeze that please



Yep. Piece of cake





INTERPOL

نشكركم جزيل الشكر على انتباهكم

Thank You-Merci-Gracias

s.hong@interpol.int