LIRNEasia
Pro-poor. Pro-market.

Safety of information in a tech driven world

Rohan Samarajiva

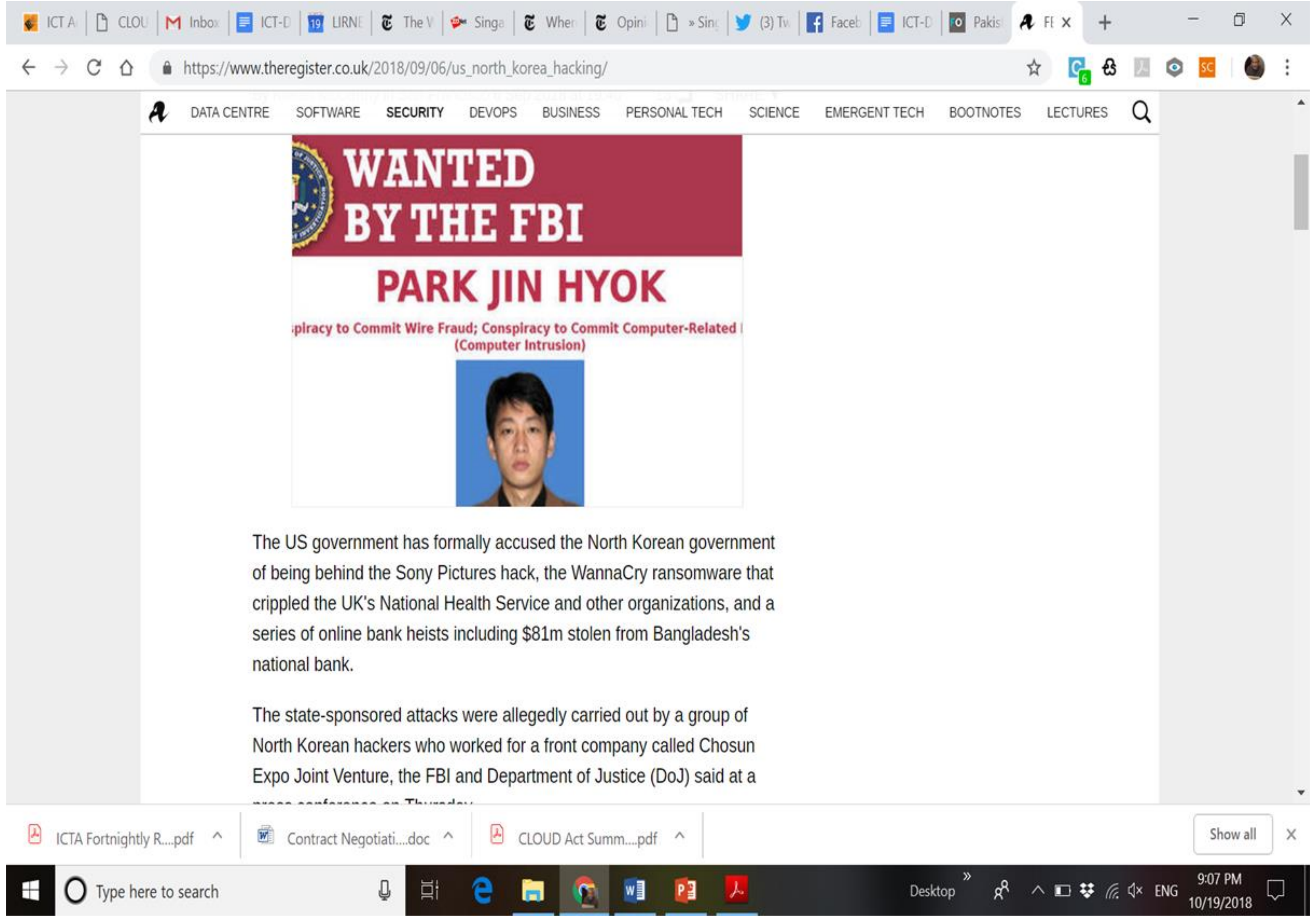
Institute of Chartered Professional Managers

27 August 2021

Examples of risks to organizations

- Sony Pictures hack
  - Systems infiltrated through a spear-phishing attack and then personal emails from senior executives were leaked online, causing immense embarrassment. Copies of upcoming movies were also placed online.
- WannaCry ransomware that crippled the UK's National Health Service and other organizations
- Series of online bank heists including $81m stolen from Bangladesh's national bank

North Korean fingerprints on Sony hack



WANTED BY THE FBI

PARK JIN HYOK

spiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related (Computer Intrusion)

The US government has formally accused the North Korean government of being behind the Sony Pictures hack, the WannaCry ransomware that crippled the UK's National Health Service and other organizations, and a series of online bank heists including $81m stolen from Bangladesh's national bank.

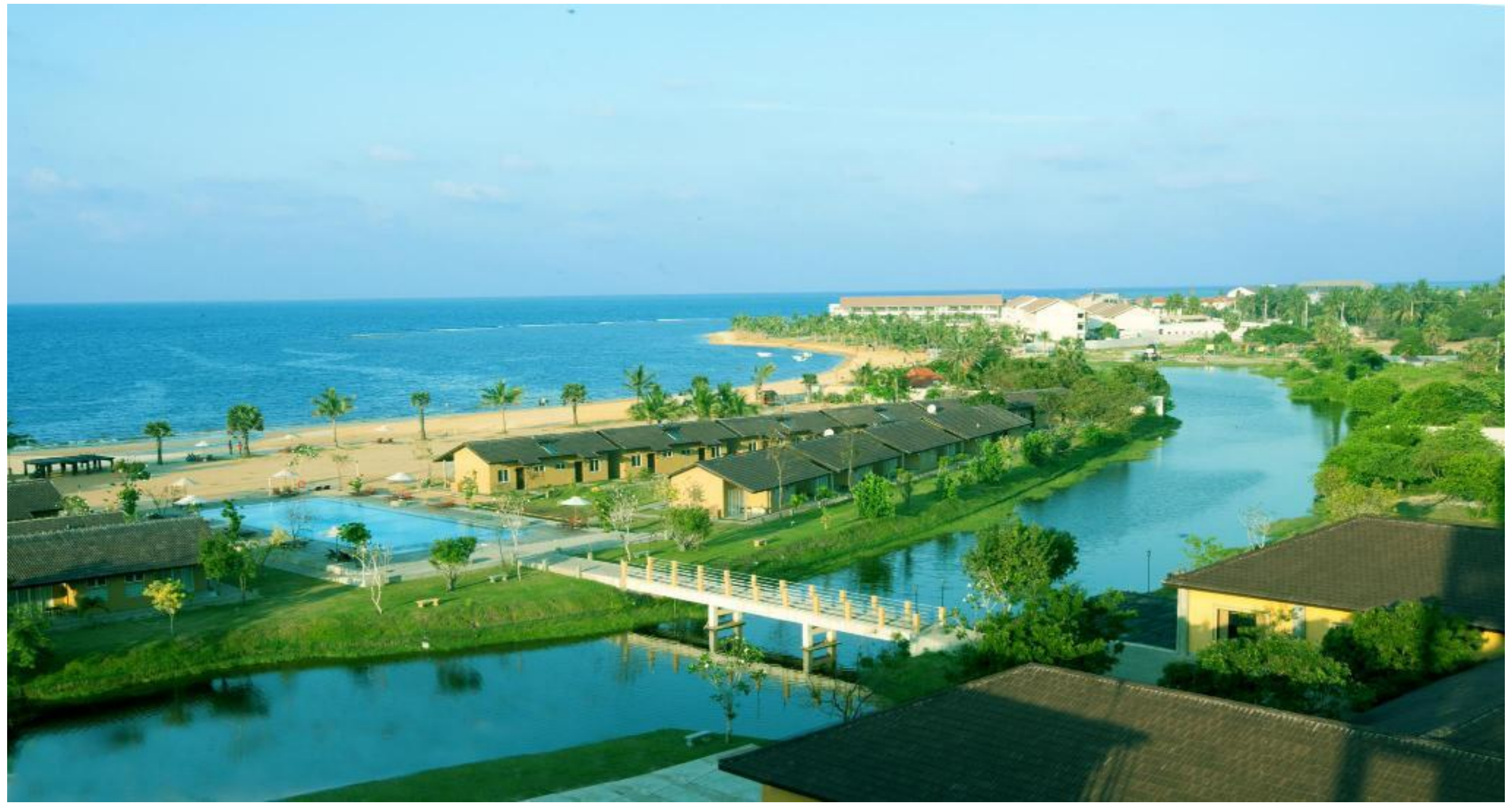
The state-sponsored attacks were allegedly carried out by a group of North Korean hackers who worked for a front company called Chosun Expo Joint Venture, the FBI and Department of Justice (DoJ) said at a

LIRNEasia
Pro-poor. Pro-market.

How do many think about risk as managers?

- When budgets and deadlines are tight, not much incentive to think about downside risks & allocate resources to manage them
  - “Not this year, but the next”
  - “We’ll find the money in the next budget cycle” . . .
- When thinking about risk, many tend to think in terms of CY*
  - Performative actions that can be used to show the individual took the necessary precautions

Cabana-style hotel, with no vertical evacuation facilities & only a footbridge across croc infested waterway built on east coast within 10 years of 2004 tsunami



I was advising a large organization re partnership involving large realtime data flows

- "How can we get the data stored on premises? Then we'll have control"
  - I asked them to think about
    - What a data breach would mean to them, to those they were accountable to?
    - Is the data solely on your premises; do you have staff inside the data center?
    - What kinds of entry/exit controls can you put in place for the on-site data center? How secure will be your logs? Can they be tampered with?
    - Where will the backups be?
    - What kinds of random inspections will you include in the agreement?
    - Do you have the people with the skills to check on compliance? Who will check the checkers?
- Final decision was for on-site data center and requirements for access logs to be kept on servers controlled by my "client"
- Given their lack of capacity, I believed the on-site data center would not reduce risks and would increase their costs
  - But on-site was performatively better ➔ safety theater

Security/safety theater

- Security theater is the practice of organizations or security teams implementing publicized or superficial measurements that create an atmosphere of safety that may only achieve the appearance of heightened security. While actual security processes can be measured based on the probability of various risks and how equipped a group is to handle them, **security theater is based on a psychological feeling**. The term was first coined by the computer security expert, Bruce Schneier, and has since been adapted to describe a variety of scenarios.

https://whatis.techtarget.com/definition/security-theater

Location of data

Missing files on NMRA cloud: Service provider had no backup

- Would it have been any different if there was no backup done for data stored on a server onsite?
  - But isn’t the first reaction that of blaming cloud storage?
- What are the responsibilities of the cloud provider versus the user of the partitioned storage? What were the legal agreements?
- What if the data center caught fire? Was backup that was not used in the same location?

- The loss of an estimated two terabytes—or 2,000 gigabytes—of classified information from the Lanka Government Cloud (LGC) risks endangering the business relationships of local drugs companies with their foreign principals, industry sources warned this week.
- The files comprised information pertaining to the formulation of drugs and other confidential supporting documents uploaded via the National Medicines Regulatory Authority (NMRA) portal.
- The impact of the data loss is still unclear to private sector drugs companies, the sources said. The Sri Lanka Chamber of the Pharmaceutical Industry (SLCPI) alone has around 60 members, excluding smaller entities that also routinely seek NMRA registration for their medicines. Some are still in the process of notifying their principals that the files they submitted were “deleted”.
- There is no indication, however, that the files were stolen. Information was sketchy as the case has been handed over to the Criminal Investigation Department. But Epic Technology Group–commonly known as Epic Lanka–which secured the contract from NMRA to digitalise drugs registration, has maintained that an employee deleted the data. The circumstances remain unclear.

Sunday Times, 15/08/21

Thinking that privileges on-site extended to in-country, following India and China

- 26. (1) Where a public authority process personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Authority . . .

. . . .

- (3) A controller or processor other than a public authority may process personal data -
- (a) in a third country prescribed pursuant to an adequacy decision; or
- (b) in a country, not being a third country prescribed pursuant to an adequacy decision, only where such controller or processor ensures compliance with the obligations . . .

Data Protection Bill Draft of 2021

Are the options open to India & China also available to smaller economies?

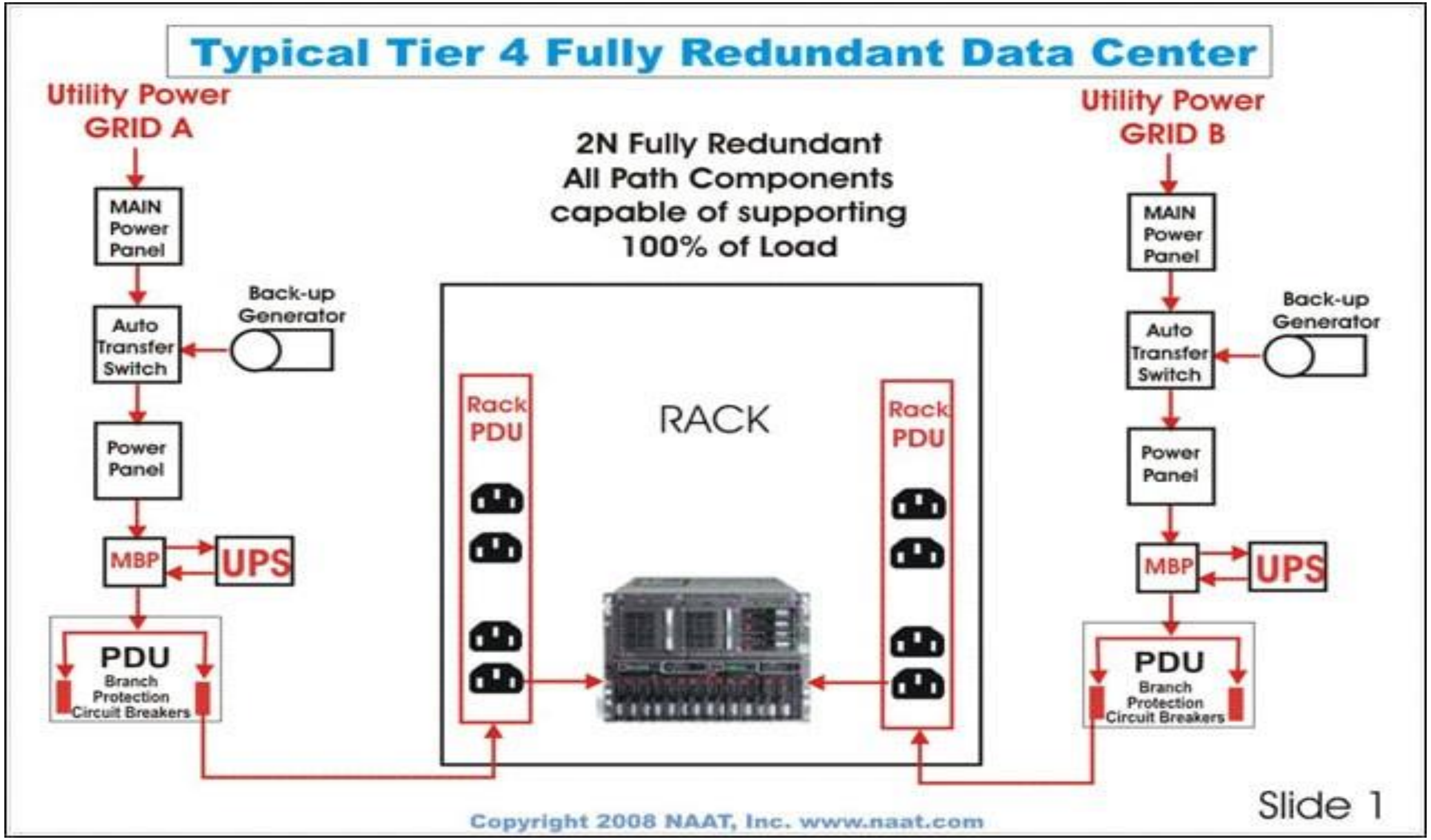
- Compelling data localization will drive up costs, and may compromise security even in large economies
  - Unless the data centers are maintained at highest levels
  - But would they still be operated by US-incorporated firms or by their subsidiaries?
  - Will Indian-owned firms have the same capabilities and resources as AWS?
- Will the MNC cloud operators agree to data localization demands by small economies?
  - If their services are not available, only option will be poorly resourced locally-owned data centers

Why does data location matter?

- Never clear why data localization is being promoted
  - Risk reduction?
  - Industrial policy?
  - Lawful access?
  - Fear of lawful or other access to public authority data by other governments?
  - Surreptitious access?
- Sri Lanka, at present has only two Tier-III Data Centers in Pitipana & Pothuarawa (plus smaller, older centers in Colombo and Welikada)

LIRNEasia
Pro-poor. Pro-market.

Tier definitions by Uptime Institute


Typical Tier 4 Fully Redundant Data Center
Utility Power GRID A
Utility Power GRID B
2N Fully Redundant All Path Components capable of supporting 100% of Load
MAIN Power Panel
Back-up Generator
Auto Transfer Switch
Power Panel
MBP
UPS
PDU Branch Protection Circuit Breakers
Rack PDU
RACK
MAIN Power Panel
Back-up Generator
Auto Transfer Switch
Power Panel
MBP
UPS
PDU Branch Protection Circuit Breakers
Rack PDU
Slide 1
Copyright 2008 NAAT, Inc. www.naat.com

What can be done?

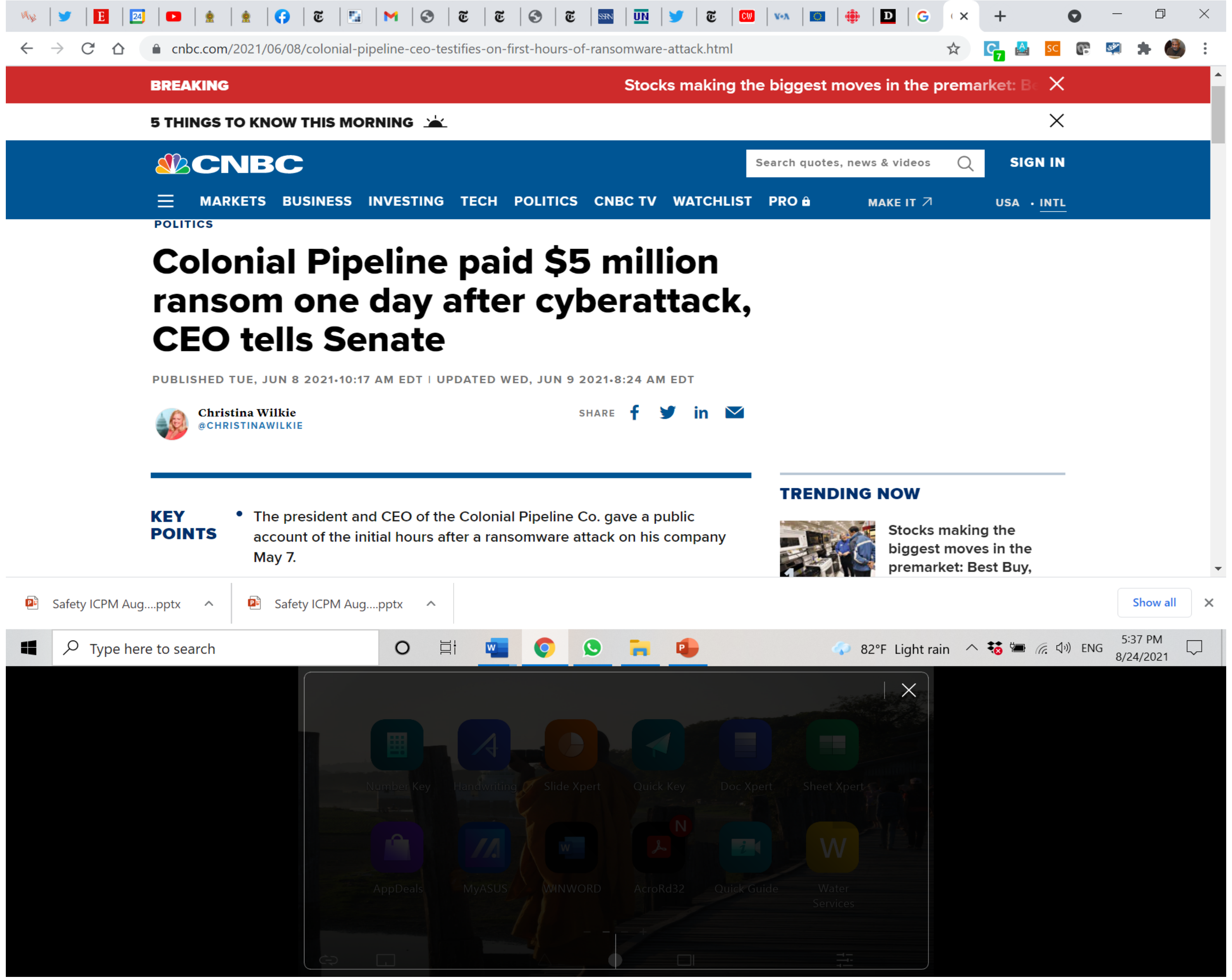
Reducing risks associated with data storage

- Old ways were not riskless, but it’s natural to expect more from new technology
- Back ups and disaster recovery facilities essential
  - In locations that are physically separated; are distant from the ocean, rivers etc.
- Most complex systems involve multiple actors. Who is responsible for what? What consequences flow when responsibilities breached?
  - Lawyers who can talk to engineers are a critical asset
- Think through what the consequences of a data breach would be
  - What would be effect on business continuity?
  - On trust of customers/suppliers?
  - Legal implications?
- Ransomware

Ransomware has got smarter

- Ransomware has gotten smarter and more frequent

- Ransomware is neutralizing backups via
  - Deletion or corruption
  - Time delayed detonations



Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021·10:17 AM EDT | UPDATED WED, JUN 9 2021·8:24 AM EDT

Christina Wilkie
@CHRISTINAWILKIE

KEY POINTS

- The president and CEO of the Colonial Pipeline Co. gave a public account of the initial hours after a ransomware attack on his company May 7.

TRENDING NOW

Stocks making the biggest moves in the premarket: Best Buy,

Prevention and recovery

Preventive measures

- Hardened systems
- Dynamic defenses, if on cloud
- Liability assigned to those with responsibility
- Reporting requirements
- Periodic, random audits
- Resilience built into design

Curative measures

- Rapid response from skilled professionals
- Assistance from government

What can be done by the manager in charge?

- How do I stop it?
  - You probably can’t, for certain . . .
    - There is no patch for human errors
    - People are the weak link
    - Malware finds a way to get through
    - Training is crucial but not infallible
  - But you can make yourself costly to hack!
    - Good backups threaten criminal’s revenue stream
    - Multifactor authentication for backup and restore
  - Arrangements to recover
    - 3-2-1 Back up Architecture & variations thereof

Beyond safety theater

- While actual security processes can be measured based on the probability of various risks and how equipped a group is to handle them, security theater is based on a psychological feeling.
  - Schneier refers to the psychological comfort given to the general public by performative actions
  - Within organizations, safety theater gives psychological comfort to decision makers that they have done something
  - For those who know better (the line managers) it’s CY*:
    - I sent you the memo; I gave you the options; you chose this; I am not to blame

Major US pipeline company which had to shut down for a week (and pay ransom of USD 5 m) because of a ransomware attack in mid 2021