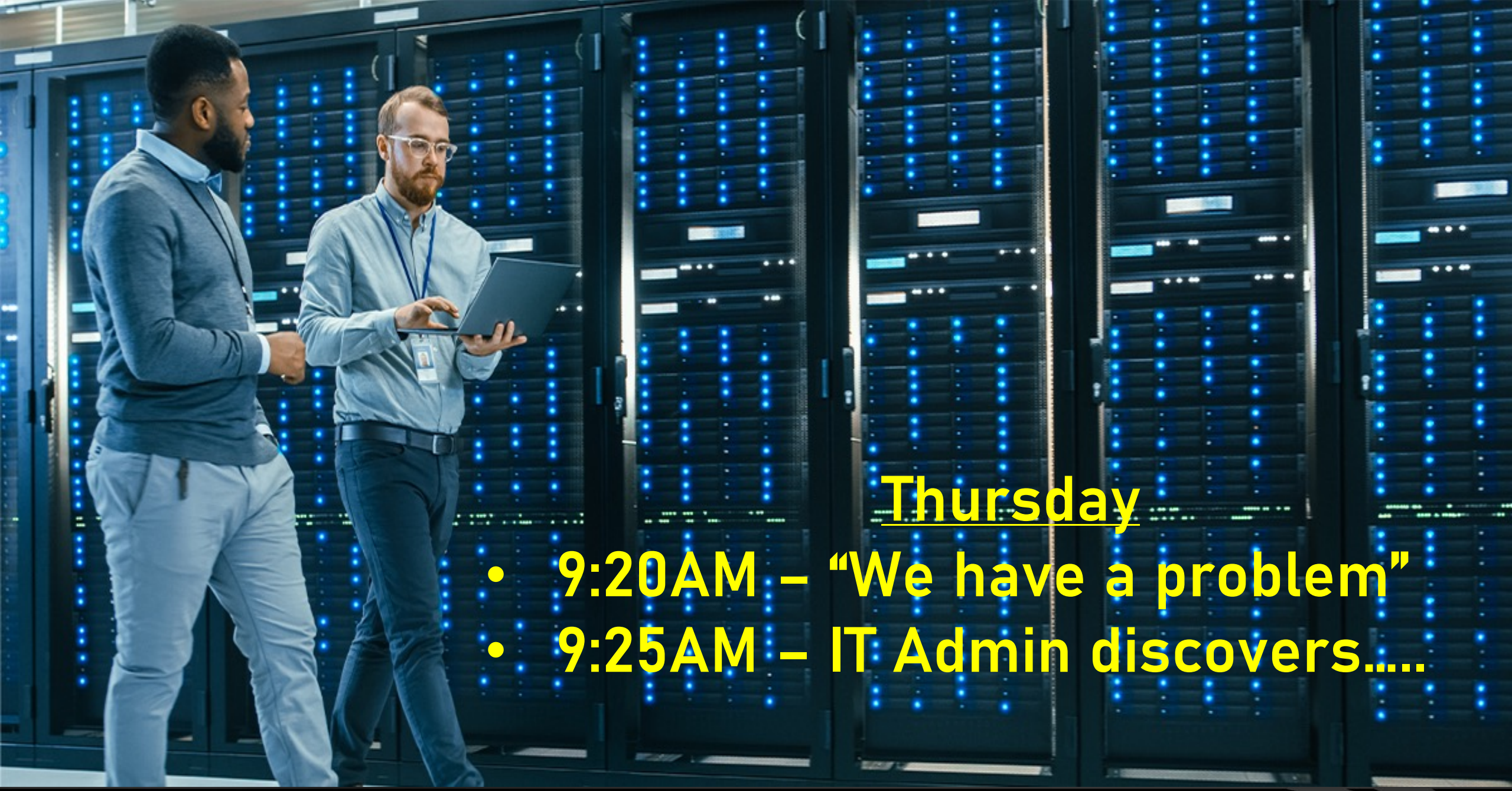
When It Happens To You – Our Experience

Protecting your organization from the inevitable

SPECTRA®

I’m here to tell the rest of the story…the Spectra experience



Thursday

- 9:20AM – “We have a problem”
- 9:25AM – IT Admin discovers…..

91C6E4-Readme.txt - Notepad (Not Responding)

File Edit Format View Help

```
Hi!
Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .91c6e4

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have be
Rebooting/shutdown will cause you to lose files without the possibility of recover

--
Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter

Do not try to recover your files without a decrypter program, you may damage them

For us this is just business and to prove to you our seriousness, we will decrypt
Just open our website, upload the encrypted file and get the decrypted file for fr
```

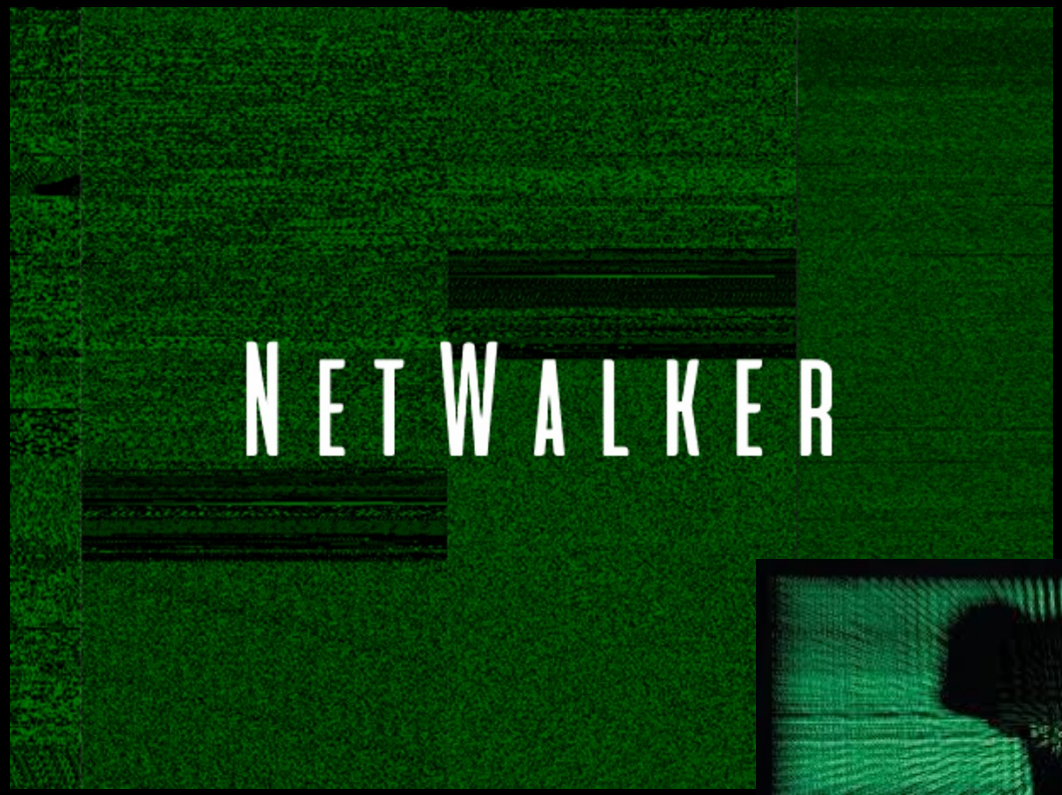
Thursday

- 9:20AM – “We have a problem”
- 9:25AM – IT Admin discovers……
- 9:30 AM – Yanking connections
- 10:45 AM – Datacenter is silent….
- 11:00AM – Complete panic and hysteria
- 12:00PM – 5:00PM - Controlled Damage Assessment
- 6:00PM – Spectra contacts FBI

6:00 PM Thursday

Spectra conducts call with FBI cyber security team

SPECTRA


NETWALKER


BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
1TROY OZ .999 FINE COPPER .MJB MONETARY METALS

$3.6M
5 DAYS

Spectra IT is notified = CHUBB Cyber Insurance in place

6:00PM Thursday

SPECTRA

- Conference call with Ankura, via CHUBB
- Ankura is well known at the FBI
- Immediate guidance to “stop the bleeding”
- SOC provided and at our disposal
- 24x7 around the clock work ahead

5:00AM Friday

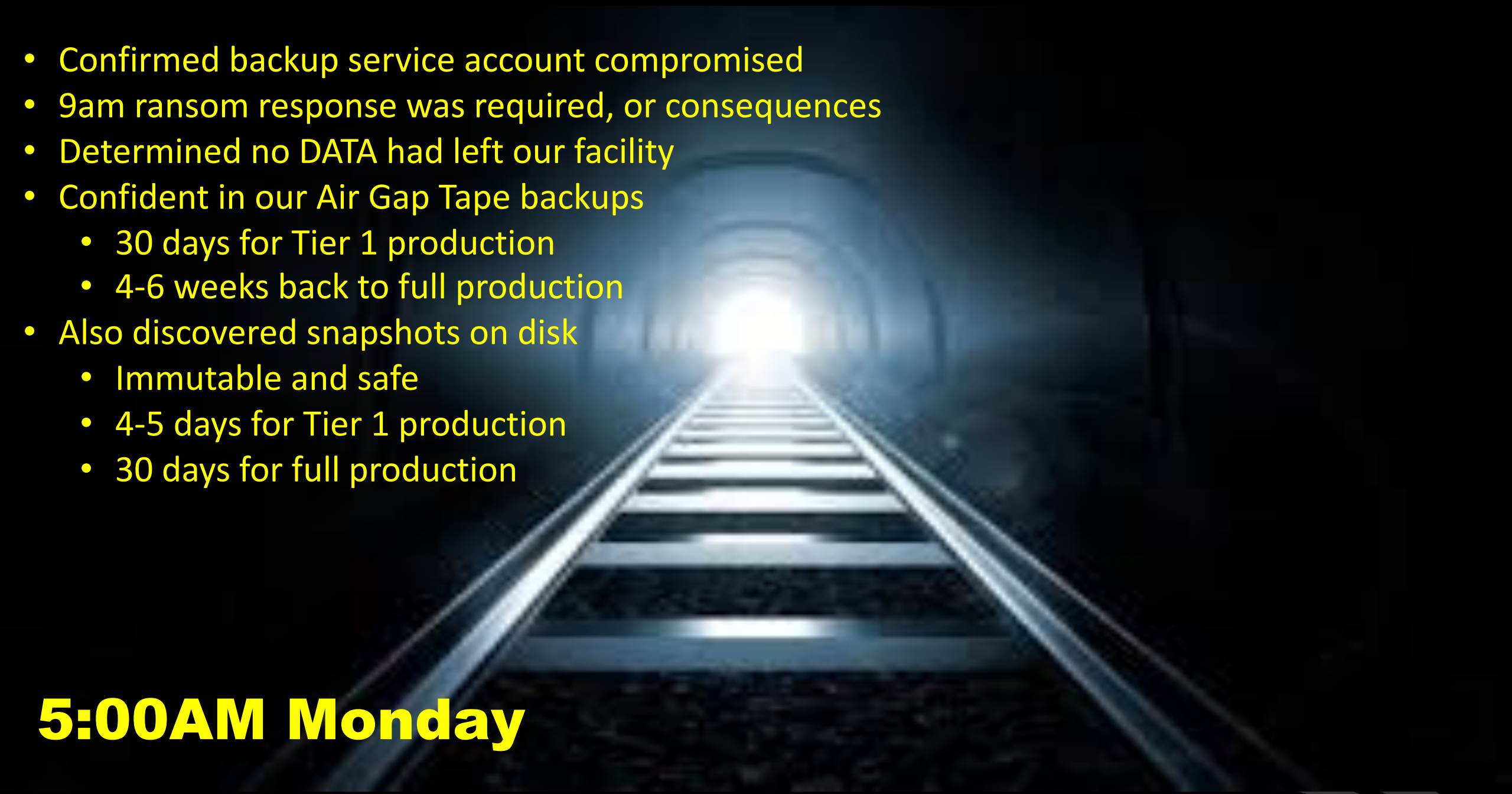
ankura

SPECTRA

Email is ALIVE!
“Quarantined”

8:30AM FRIDAY

However, Still a LONG road ahead… (Friday – Monday)



- Confirmed backup service account compromised
- 9am ransom response was required, or consequences
- Determined no DATA had left our facility
- Confident in our Air Gap Tape backups
  - 30 days for Tier 1 production
  - 4-6 weeks back to full production
- Also discovered snapshots on disk
  - Immutable and safe
  - 4-5 days for Tier 1 production
  - 30 days for full production

5:00AM Monday

Spectra Logic CEO Nathan Thompson, and IT Director Tony Mendoza

Spectra prevailed…

- ***Other than a few miscellaneous files, all data was restored***
- ***$0.00 was paid in ransom***

Tough Learning Experience – but beneficial (and a little luck)

- **A "virtual & off-site air gap" of our data provided a sound recovery from the attack**
  - **Virtual replicated Read Only Snapshots on BP NAS (ZFS Immutable Snapshots)**
  - **Off-Site "Air Gap" | SPECTRA Tape was a "no brainer" for safe and unaffected recovery**
- **Above allowed us to successfully restore our data | Did not pay ransom**
- **1st Line of Defense** - Threat Protection Software
  - **Arctic Wolf**, Crowdstrike, CarbonBlack, Varonis, SentinalONE, Sophos, Mimecast, …..
- **2nd Line of Defense** - Immutability at the data level
  - Virus, Ransomware, Hackers, Internal & External Bad Actors, Disaster

Ransomware Resiliency

Spectra Postmortem:

- Adopt a “not if, but when” mentality
- Balance Security with Productivity
  - We had threat prevention, endpoint virus protection and email filtering.
  - Complete “remote user” failure. Our fault.
- Vigilant education for end users – your employees
- Develop Exec Mgmnt sponsored Response/Action Plan
- Invest in Ransomware Insurance - CHUBB
- Evaluate/Invest in Threat Protection S/W
  - EDR – End Point Detection and Response
    - Monitors anomalies
  - MDR – Managed Detection and Response
    - Monitors anomalies and people
    - Arctic Wolf – Spectra Customer
- Take steps to limit Data Attack Surface
- Explore “Air Gap” & “Immutable” data storage/protection

Thank You!

SPECTRA