Virginia Information Technologies Agency

Cyber Security: How to Avoid Being the Next Headline

Michael Watson
Chief Information Security Officer

COVITS 2012
September 6, 2012

Title of Slide

- Summing up the job in one sentence
  - My job is to protect Commonwealth data and IT services
- It's a big job – how do you do it?
  - First know where the data resides
  - Days of a solid border are gone (mobile devices, laptops, cheap attached storage, etc.)
  - Expect the data is out there and adjust security controls to provide best protection possible
- Understand that at some point you will be breached
  - I know this session is about keeping out of the headlines but let's be upfront and honest - it should also include if you're in the headlines how to get out quickly
  - Accept it, and realize that you just need to keep calm, or freak out ahead of time, however you want to handle is fine just figure out how to prepare
  - Companies often end up in headlines because they are holding close to the vest – people wonder what is being hidden (trust no one)
- After understanding that you will be breached try to figure out why you'll be breached
  - What makes you a target and what data do you have that is valuable
    - Understand Motives
      - Financial
      - Political/Hacktivist
      - Espionage/State Secrets – aka Cyber Warfare
  - What is your high risk data
  - State has most types of data imaginable
    - PII and PHI
    - Critical Infrastructure Information
    - Criminal Justice Information
    - Credit Card/Financial Account data
    - Control Systems access and data

- Then it's being ready for the breach
  - Aiming for the model company
    - Cool Calm and Collected
  - Be sure to know what was taken – adds to user confidence
  - Hopefully it isn't your most valuable data (that doesn't mean it won't be PII)
  - It's all about me
    - Companies have thefts all the time – Cyber is different because the thefts don't typically involve the end user
    - How are you going to address fixing me – Credit monitoring, refund of lost money, free service, etc.
    - Understand it will be and should be painful
  - Good PR is critical – don't hide if you aren't sure you aren't sure how bad it is, say so
    - Disclaimer: If you haven't put any effort into cyber security I'm sorry you're out of luck and hopefully the bad guys haven't sunk your business
  - Don't avoid the I'm sorry – own up to mistakes
    - RSA example
    - People may not like it at first, but open and honest breeds respect and loyalty (knowing is better than not knowing)
  - Try and track costs
    - Hard to do and hard to benchmark – over time yields results
    - Don't be afraid to make up a number just document how you got there
      - Acknowledge it won't be perfect
    - Recognize whether additional investment would have helped or not
- If everything goes right, you may only be in the headlines for a couple of days
  - Accept the fact that if you are a big public company you're likely going to end up in the news – in my case Government will likely end up there
  - Don't give them anything to report on – doing the right thing isn't interesting news
  - Turn it into something about how good your security is and that rapid and complete response was possible
    - No such thing as bad PR
    - Hard to convince agency heads and CEO's sometimes, but honesty along with preparation goes a long way

Title of Slide

Source: http://viewsoflajolla.com/

CoVA IT Infrastructure

Computers
- 57,977 PCs
- 3,485 servers

Mailboxes
- 59,866 accounts

Disk storage
- 1.4 petabytes

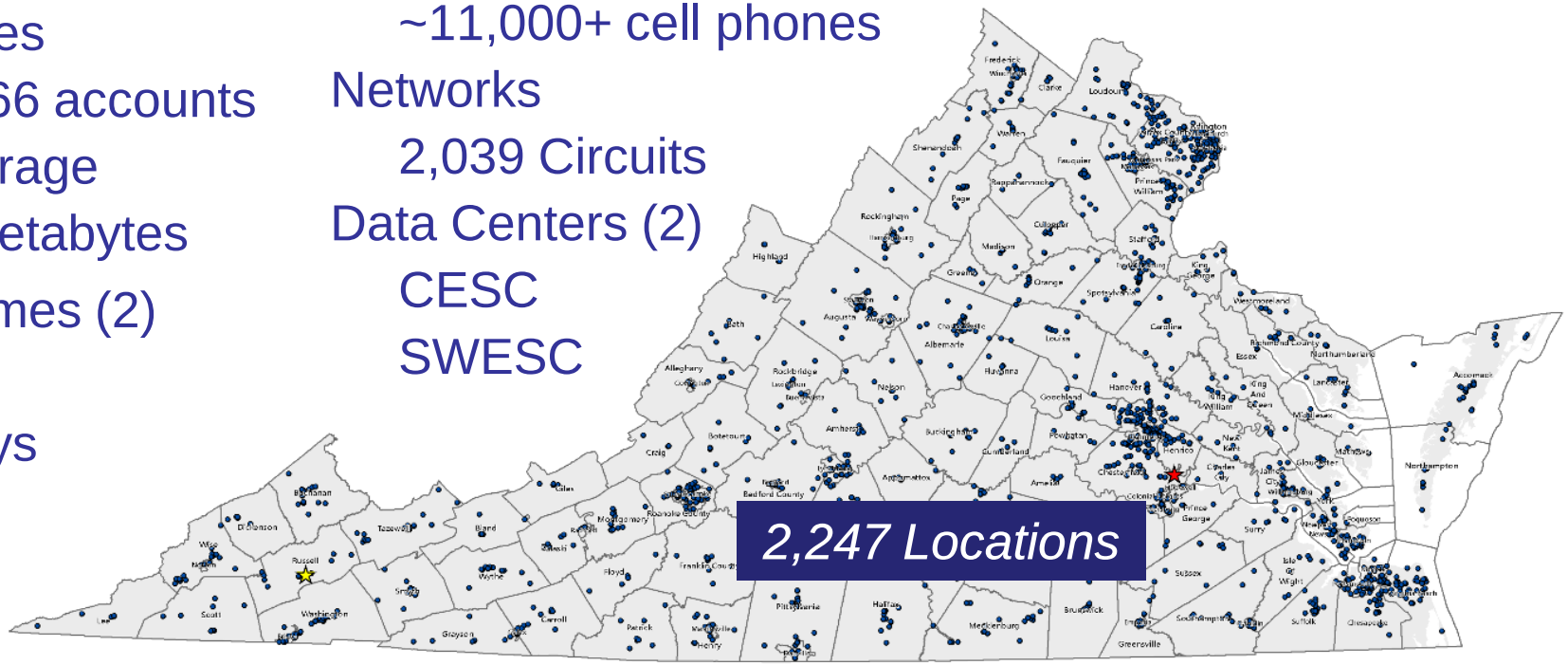
Mainframes (2)
- IBM
- Unisys

Communications
- ~55,000 desk phones
- ~3,600 handhelds (PDAs)
- ~11,000+ cell phones

Networks
- 2,039 Circuits

Data Centers (2)
- CESC
- SWESC

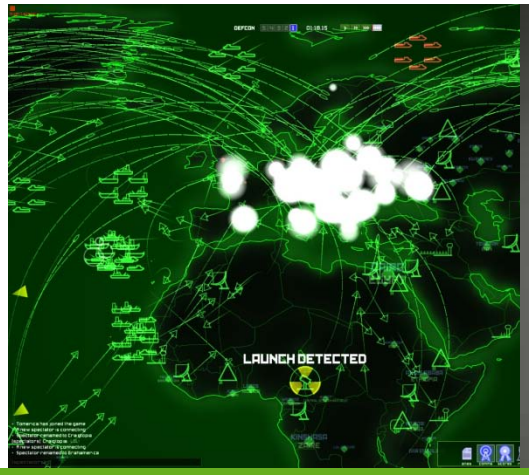
Printers
- 5,674 network
- 22,000+ desktop



Source: Em and Ernie's Flickr photostream

KEEP
CALM
AND
CARRY
ON

FREAK
OUT
AND
CRY
A LITTLE


LAUNCH DETECTED

Source: http://www.ereleases.com/