VPNs in Higher Ed -- How Many is 2 Many?

BC Security Staff

(as told by the contractor)

Vendor Management Done Too Good

Our Servers

- We have lots of servers… ☹
- Most of them are in a data center, behind a firewall, accessible:
  - From the Internet
  - Only from campus
  - Only from the data center
- Some are in the clouds
- Some have good data; some others not so much

Who Accesses the Servers?

- Students
  - mail, class registration
- Staff
  - PeopleSoft, mail, tickets
  - Students posing as staff
- Contractors
  - random people fixing/breaking stuff
- Public
  - think www.bc.edu
  - We also have a big stadium…think hot dogs…

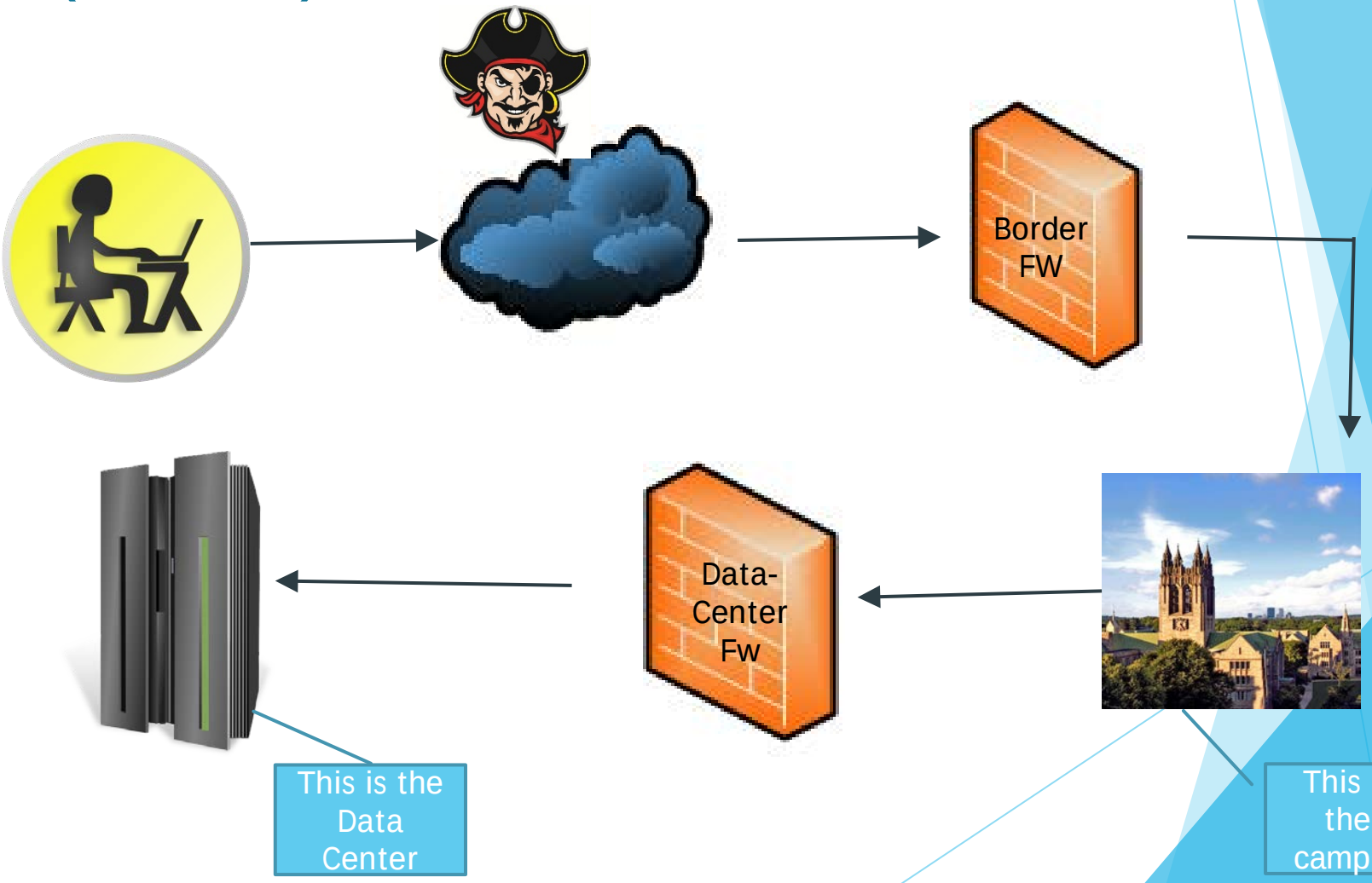
VPN is good

- We use VPNs because:
  - They hide your actual message content
    - Encryption
    - Useful for sensitive data or Starbucks sessions
  - Perform authorization by username rather than by only IP address
    - You login before we grant access
    - We now know you have some reason to visit us
    - We also know you have some affiliation with us!

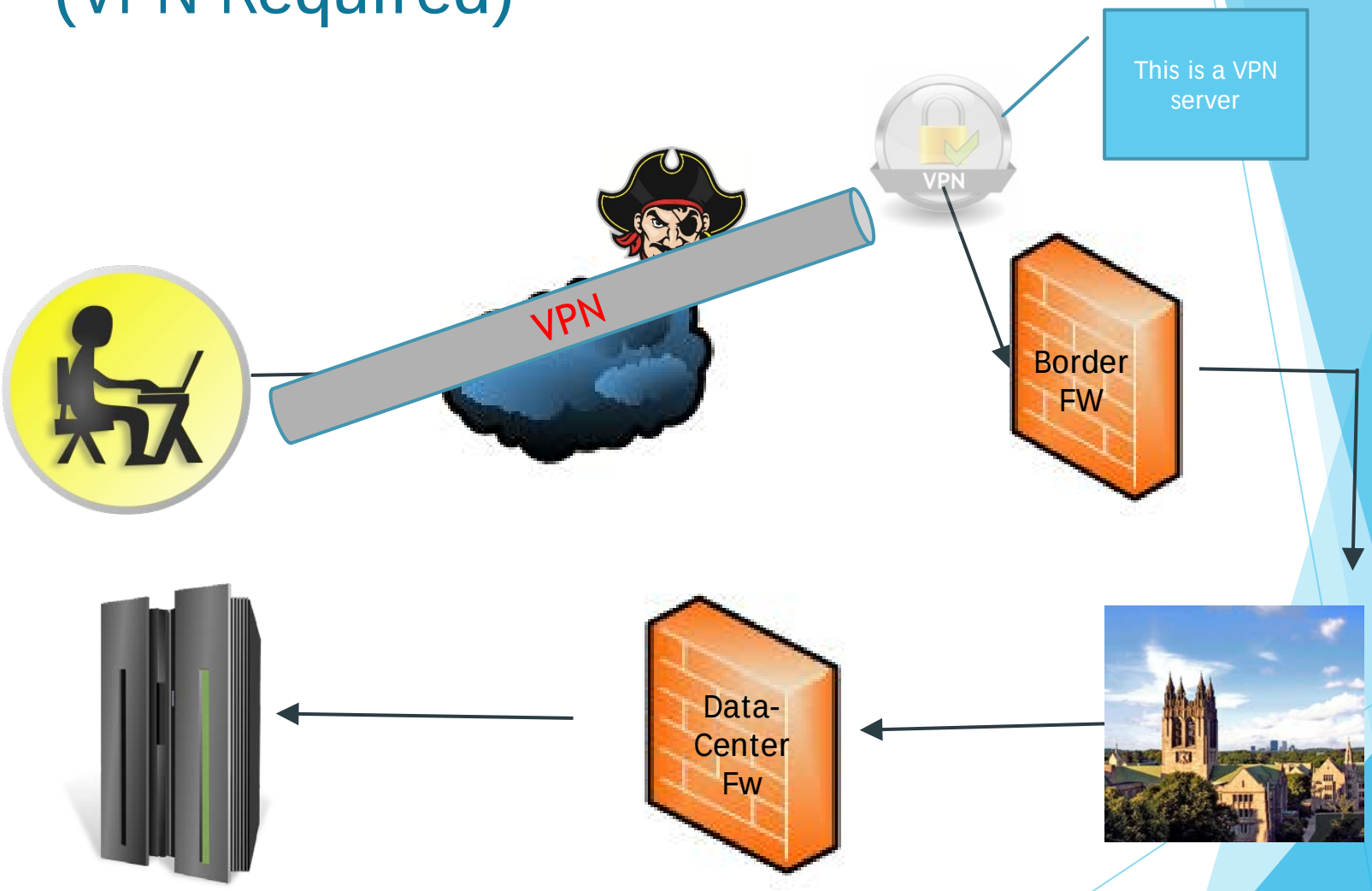
VPN is bad

- We dislike VPNs because:
  - Encryption
    - we don’t know really what you’re doing
    - At the internet border it’s all random data
  - User authentication
    - Compromised user accounts look like normal users

Servers open to the Internet (No VPN)



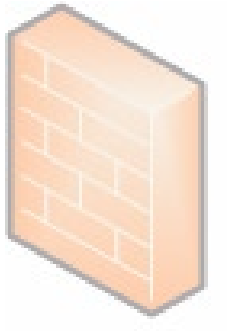
Servers that need/want protection (VPN Required)



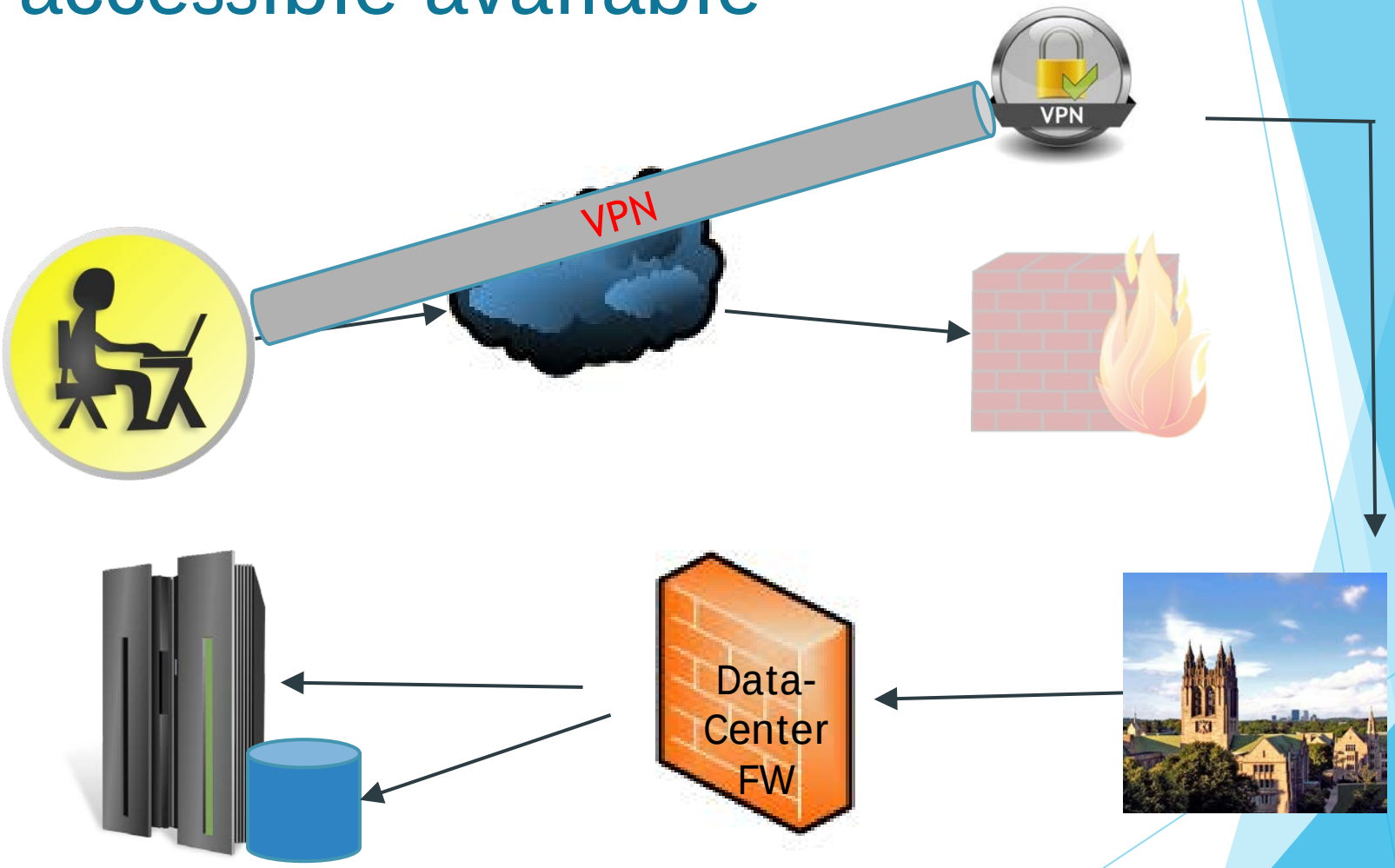
VPN #1. Commoners' VPN

- If you have a valid BC credentials, you can log into the VPN
  - students, applicants, alumni-ish
  - faculty, staff, long-term contractors
- It replicates access that would be available for you on campus
- Userids are centrally managed

Servers not located at BC but may get sensitive data



Make servers not Internet accessible available



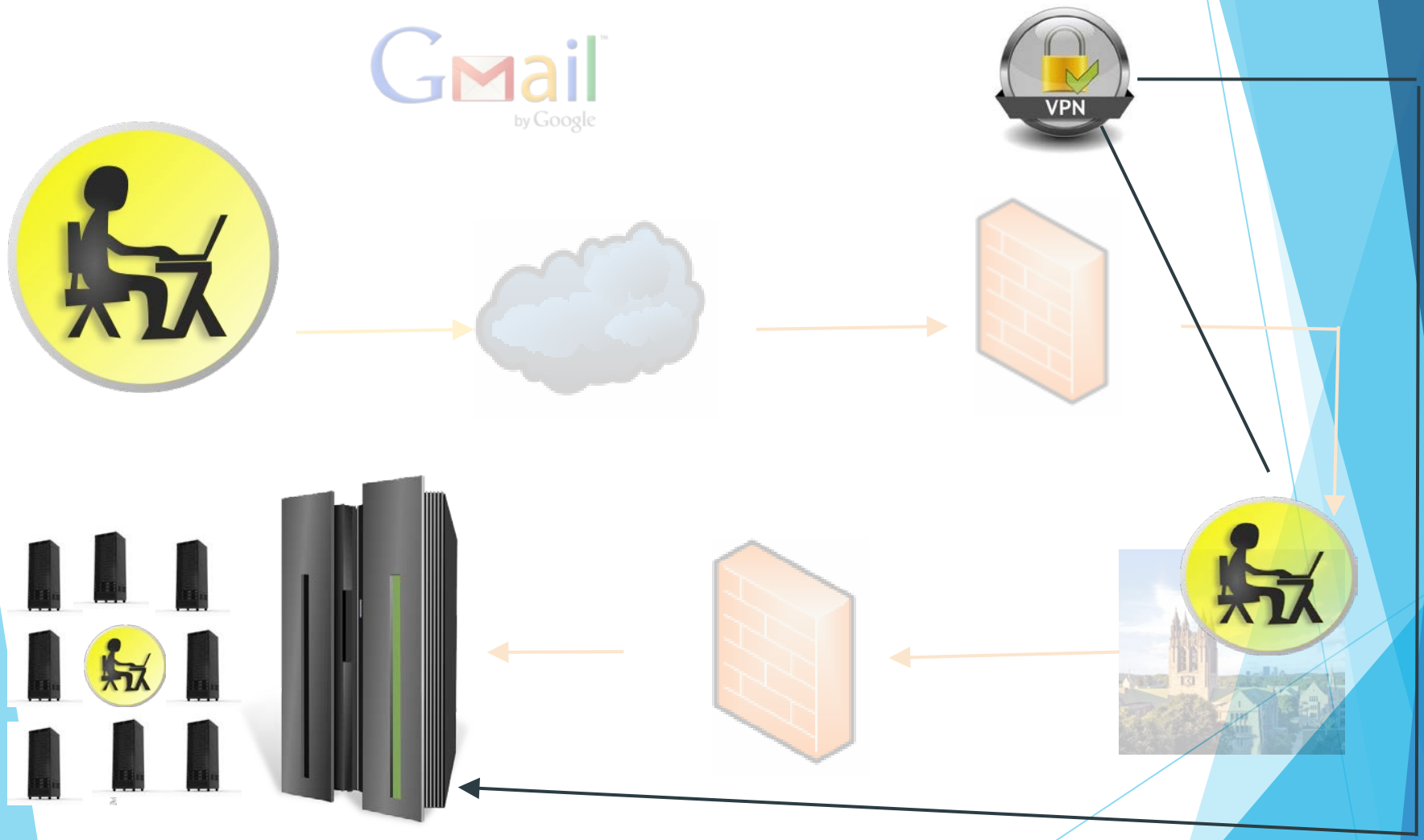
Why One VPN is bad

- Everybody gets the same access
  - Firewall rules are mostly IP based, not user based
  - VPN access into data center means students, applicants, etc., get access to it
- Maybe we need another VPN?

VPN #2. A VPN for IT Administrators

- IT staff do things that we don't want students to do
  - "Reboot", Add user account, Add software
  - Access *my* PII
- The IT VPN is for IT administrative staff
  - Less restrictive access to all servers in the DC
  - Access is also logged to Arcsight and other tools
  - Multi-factor authentication
  - Additional monitoring

Servers accessible via IT VPN



VPNs are cheap, let's do another one

- Amazingly, large hordes decided they were in IT so they could get IT VPN access.
  - The muti-factor token didn't even scare them off. ☹
  - "large hordes" circumventing the FW sounded bad
- We also have a large number of vendors that administer systems (think large hordes)
  - These users come and go quite quickly
- We need a way to give limited admin rights to a user, either internal or vendor

#3. The Vendor VPN

- You have to be approved by Security and manually added to the VPN user group
- No access to the internet (by default)
- Access to limited resources within DC via embedded FW rules with user to host mapping
  - 1 user : 1 host
  - 1 user : Multiple hosts
  - Multiple users : 1 host
  - Multiple users(Group): Multiple hosts

Now You Know Why We Have 3 VPNs

- But ……
- We also have PCI VPNs (#4) and SSH jump hosts (#5) and special VPNs (#6-?) and …
- And have you heard of redundancy?
  - VPNS * 2 == number of boxes we have to support

Where ~~Will~~ Did it End?

- Our security posture is vastly improved
  - We've learned a lot about our vendors
  - And their infected machines
  - And what they *really* do
- Our security staff is vastly crabby
  - Very heavy user support burden
- And it's now called the "Admin" VPN instead of "Vendor" VPN

What Did We Learn in 2014:

- Pay Attention to the Monitoring System:
  - Sony
  - JPMorganChase
- Vendors are Evil
  - Targĕt
  - Home Depot, Michaels, etc.

Restricting Vendor Access

A MULTI-YEAR EXTRAVAGANZA

As told by: Pat Cain

Co-storytellers

Nathan Hall, Jamie John, David Millar, Damian Cleary

(w/cameos by Mary Zhao & David Escalante)

Problem

- Vendors
  - Short duration at campus
  - Access to all kinds of stuff
  - Not known for their troubleshooting abilities
  - *&%$3ep*
  - Some regulations require limited access to things
- Who's a vendor?

The Original Plan – The Vendor VPN

- ITS security would admin accounts
  - We only have about 75 “vendors”
  - We can enable or turn on off users quickly
    - Who cares if their local system account is alive? They can’t get to it.
  - We can coerce vendors to sign NDAs and paperwork
- Not dependent on local sysadmins
  - Or LDAP or central services
  - We get visibility into our vendors actions
  - We get to enforce policy
- Not dependent on others to do the right thing

The New Plan – The ‘Admin VPN’

- Extended rules and VPN to campus areas
  - Not only DC
  - Dorm cameras, heating, cash registers, etc
- Not only vendors
  - Staff who needs admin access to ONE system
  - “I’m not a vendor”.
    - Fine. It’s now called “AdminVPN”.

The Good

- Quick turn on/off of user accounts
- Know all account holders
  - We can enforce policy. Want an account?
    - Sign the NDA and the security addendum
    - You been bad? Account, what account?
- Additional logging
  - Professors with sensitive data under their desk
- “Talk to the ~~Hand~~ VPN”, and only the VPN
  - Use the VPN NAT function in access rules
- PCI, HIPPA, GLB, etc. separation

The Bad

- Manual Administration is a pain
  - We have 472 “vendors” on the system
- Some vendors have bazillion systems to control
  - E.g., the MS SQL consultants (~40 systems)
- Some vendors have lots of employees
  - Some guys have 16 workers
  - Some vendors turn over staff quickly
- Some vendors don’t know how computers work

The Ugly

- Most people can't boot their computer without help
  - So let's have them debug their VPN connection
- Vendors come and go quickly
  - How fast can we add accounts or fw rules?
    - The dorm is broke. This guy needs access an hour ago.
  - Can we use a static "emergency" id+pw?
  - How fast can we turn them off?

The Plan v3 – (debug help)

- Improve user self-troubleshooting ability
  - “Am I blocked” website for IT staff
    - Have them help us debug the rules
  - Guidance for users on how to debug their connections
- Can we combine different VPNs into one?
  - Some users have accounts on multiple VPNs
    - How do we know which rules to enforce[

The Plan v3 – (automation)

- Security still generates user accounts
  - Accounts time out
- Identify IT staff who ‘control’ a server
  - *they* give access, turn users on and off
    - *they* get to talk to the auditors ☺
- Simplify usage and management
- Can we find a by-user FW-rule, user self-provisioning, good logging, robust product?
  - [If you know of one, please confess.]

Thank You

We're security@bc.edu

Let us know what product we should use for v3.

[Do you use clearpass? Like it's logs? I don't. Talk to me.]