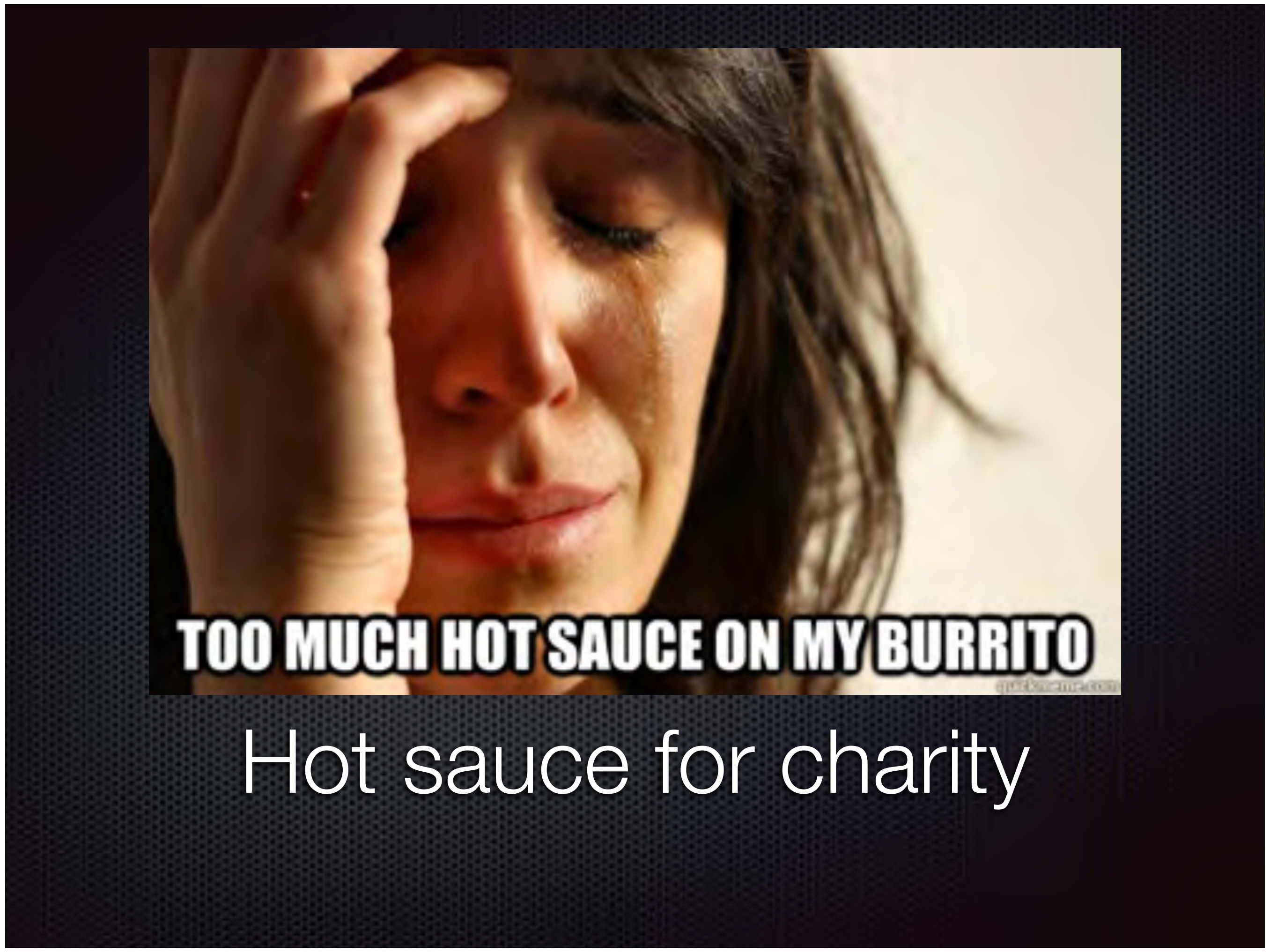
Blue Team Hell: A story of ISPs, Healthcare, and Education

Amanda Berlin

@Infosystir

Blue team
started at ISPs
Healthcare
Purple team
Windows Admin
Network Security
Jack of all trades
very visual - All the memes!!



Hot sauce for charity

that’s not Charity

Adult Supervision Required

If you’re squeamish… you might want to look away and maybe do the earmuffs thing

All men must choose between two paths.

Good is the path of honour, heroism, and nobility.

Evil... well, it's just cooler.

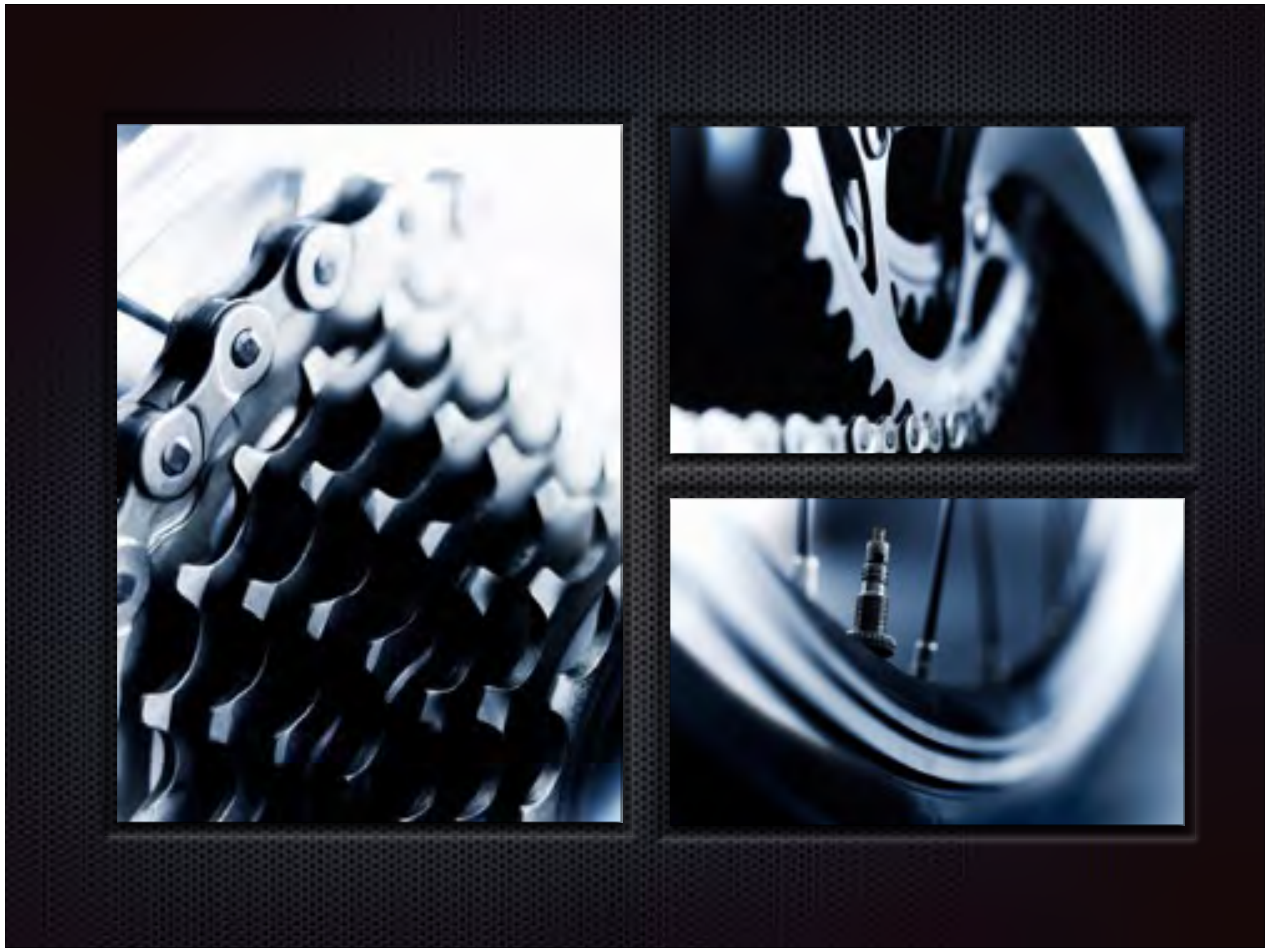
Blue & Red

One of my favorite kid's movies ever. Great quote that applies to defense and offense

Your circumstances may be bad.....
...but are they pitchfork in the ass bad?

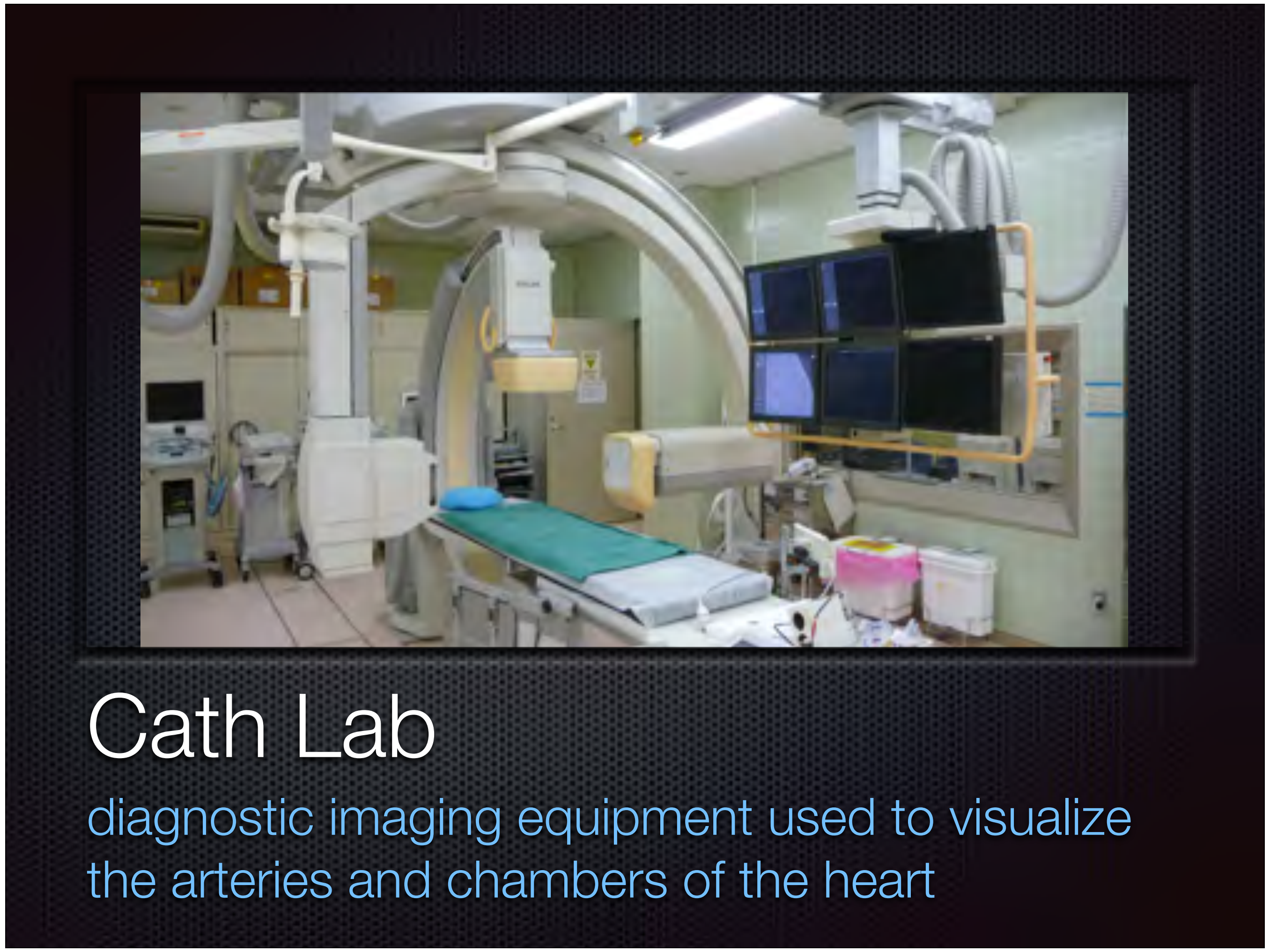
1. preface with that all I’m bringing up has been engineered and fixed or I wouldn’t bring it up.
2. Imagine yourself walking into this environment with no help (at first)
3. Hadn’t started in infosec yet
4. Knew these were bad, and it got worse
5. Guy didn’t grow with the environment
6. Started out with everyone in the dept as a domain admin and non-dept people knowing “INFO”
7. Start with some things we didn’t have

1. A/V - production servers had anti-virus installed sometimes. But if it were to cause performance problems it would be uninstalled or disabled. Servers that were required to remain logged in with domain admin due to the way the application interacted with the desktop.
2. WSUS. All windows environment. WSUS was there, just not really operational or managed.
3. Visibility. No clue what software, how many servers/switches/pcs. What vendor equipment was on our network, what data was passing over it.
4. decent datacenter (waterlines above, open ports, door access, cable mgmt)



pictures of server racks here

1. backups
2. DMZ
3. segmentation, open ports and vlan1 everywhere!
4. At one point this was so incredibly bad. That our public facing web server was on a dual homed windows 2003 server. This Windows server had a database backend that our third party web developers would access with vnc. The database was on microsoft sql 2000 located on our domain controller. These same domain controllers contained the dhcp zones for our publicly accessible non-password protected, unencrypted wifi. Once we had an issue with our guest wifi and had an older lady call us up at the helpdesk asking when her internet would be back up and functional. She was located across the street.



Cath Lab

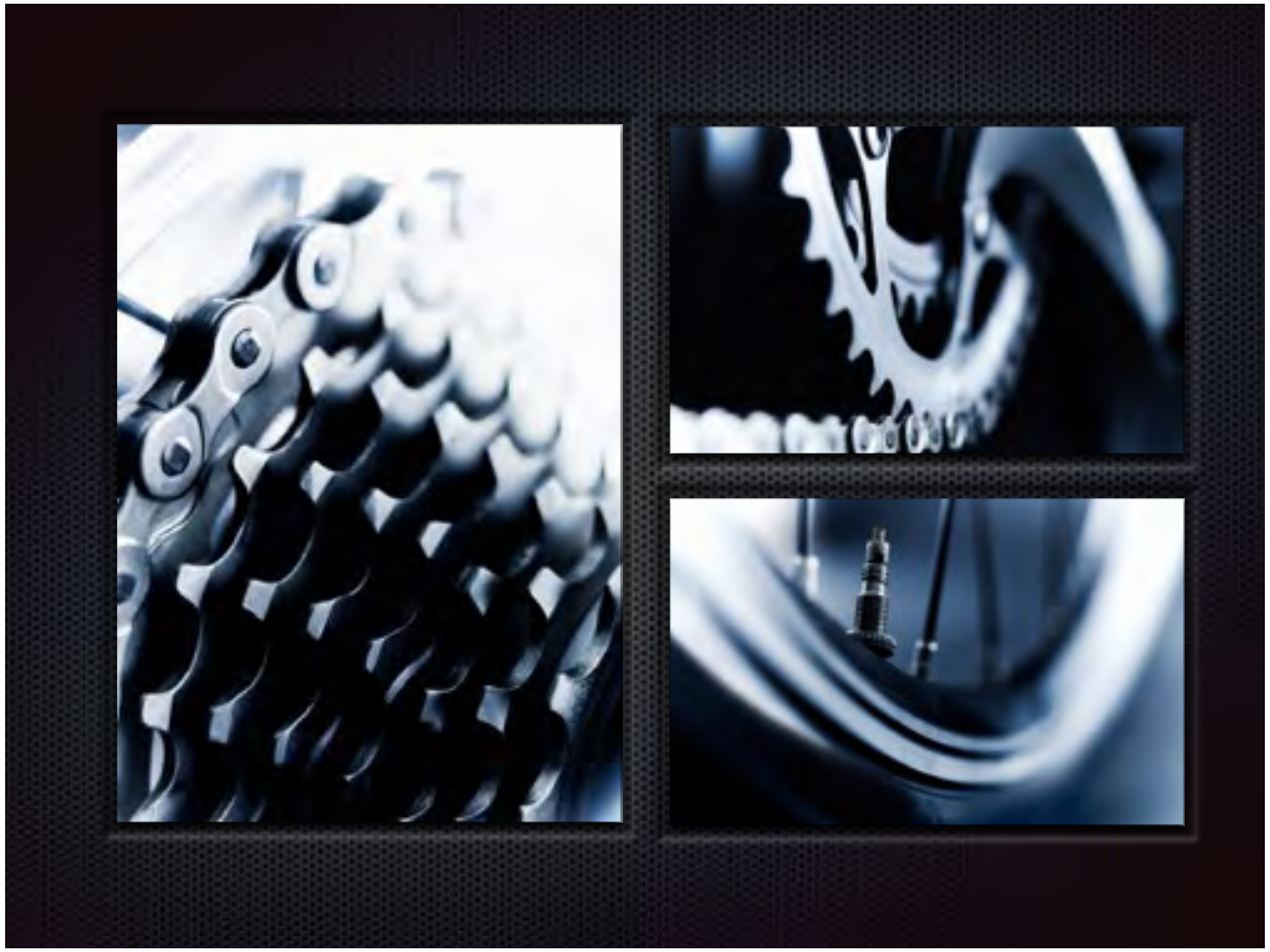
diagnostic imaging equipment used to visualize the arteries and chambers of the heart

1. Lots of big named vendors supply cath lab equipment.
2. One night we ended up with our night operator calling about rapidly locked out accounts
3. Due to lack of visibility we made a quick vbs script to unlock
4. Turns out this vendor shipped us boxes infected with conficker.
5. Scan everything before it hits your production network.
6. Turns out you get an amazing discount on your software licensing and hardware when you can prove a billion dollar company infected your network!
7. onto things that we did have

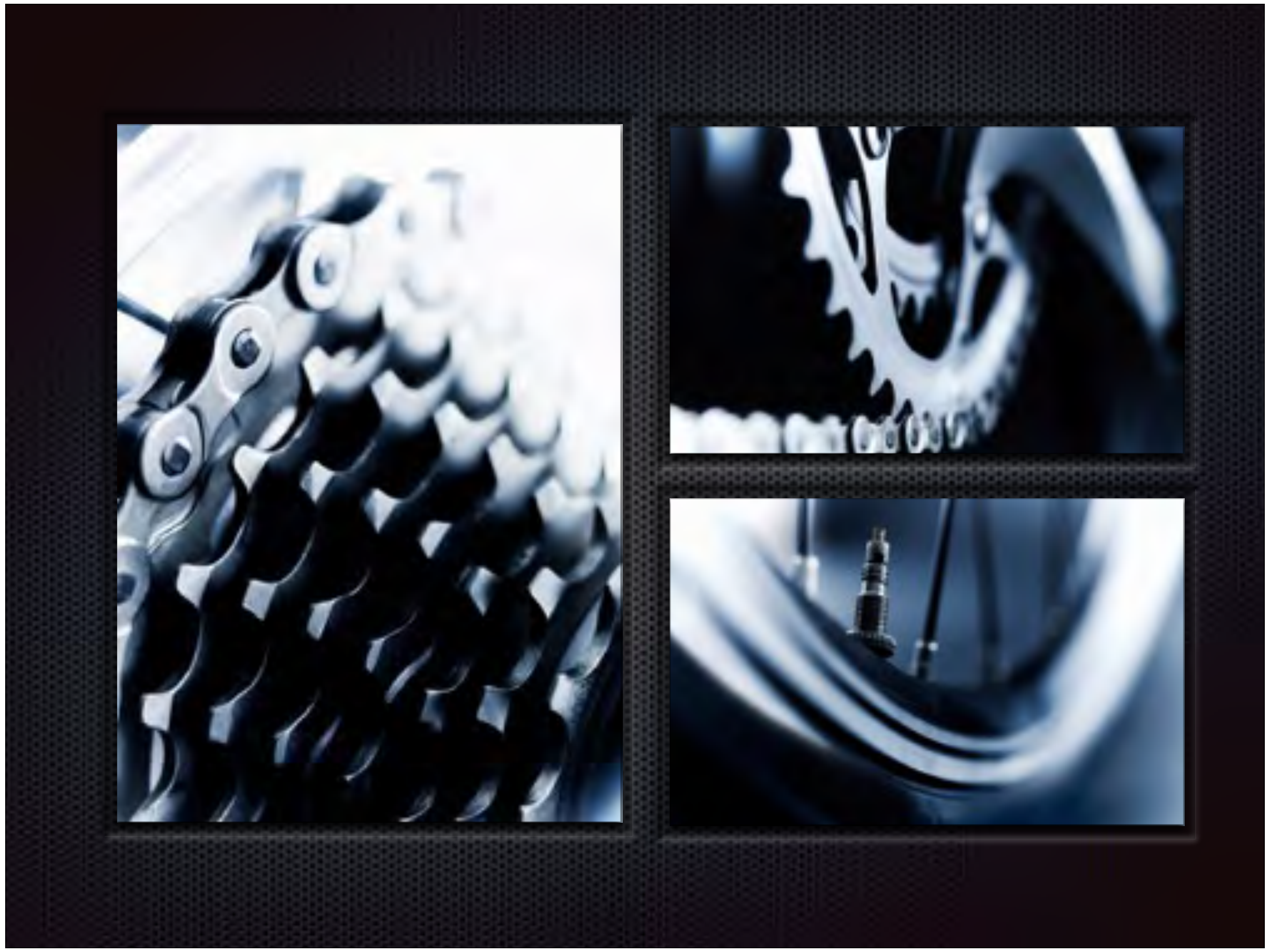
User name: Administrator

Password:

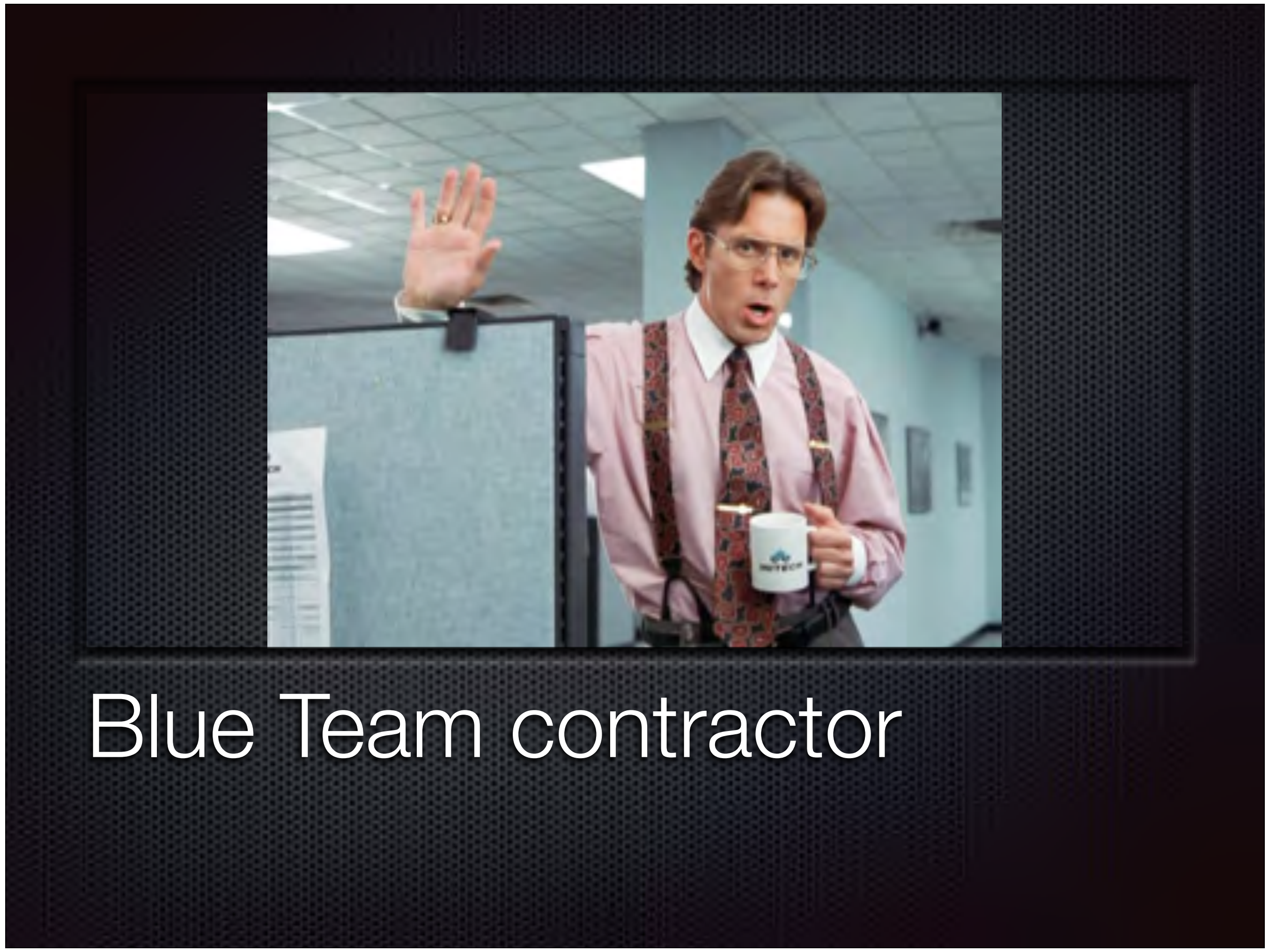
1. ms08-067
2. conficker
3. windows 2000/xp rampant



1. Password protected excel 2002 with all of our organizational passwords
2. Water spouts (literally)
3. no password policies/password reuse constantly/no password on sa



1. Best alerting system ever = APC UPS
2. Phone system for our switch board that could be taken down by a port scan.
3. bedside usb card readers that used keyboard emulation to type in credit card data
4. Pharmacy tablet sending PCI data wirelessly in the clear.



Blue Team contractor

I kid you not this is what he did all day. Ask @z0rlac and he can back me up.

We provided internet connections for multiple offsite locations as well as allowed them to colocate in our datacenter, offered them services, as well as applications. After I had purchased a vulnerability scanner and shown them what shodan could do I was then instructed to run vulnerability scans across our connections with the businesses just as an added bonus to them.

Personal Massager

Deep, Satisfying Massage... Feel Good, Feel Relaxed.

Massage away stress and tension. Deep penetrating massage soothes aching muscles and helps stimulate circulation. For use on neck, shoulders, back – anywhere on your body. Uses 2xC batteries (not included). Features variable speed setting in deluxe model.

#33840 Regular 7" Massager.....$24.95
#33841 Deluxe 9.5" Massager....$29.95

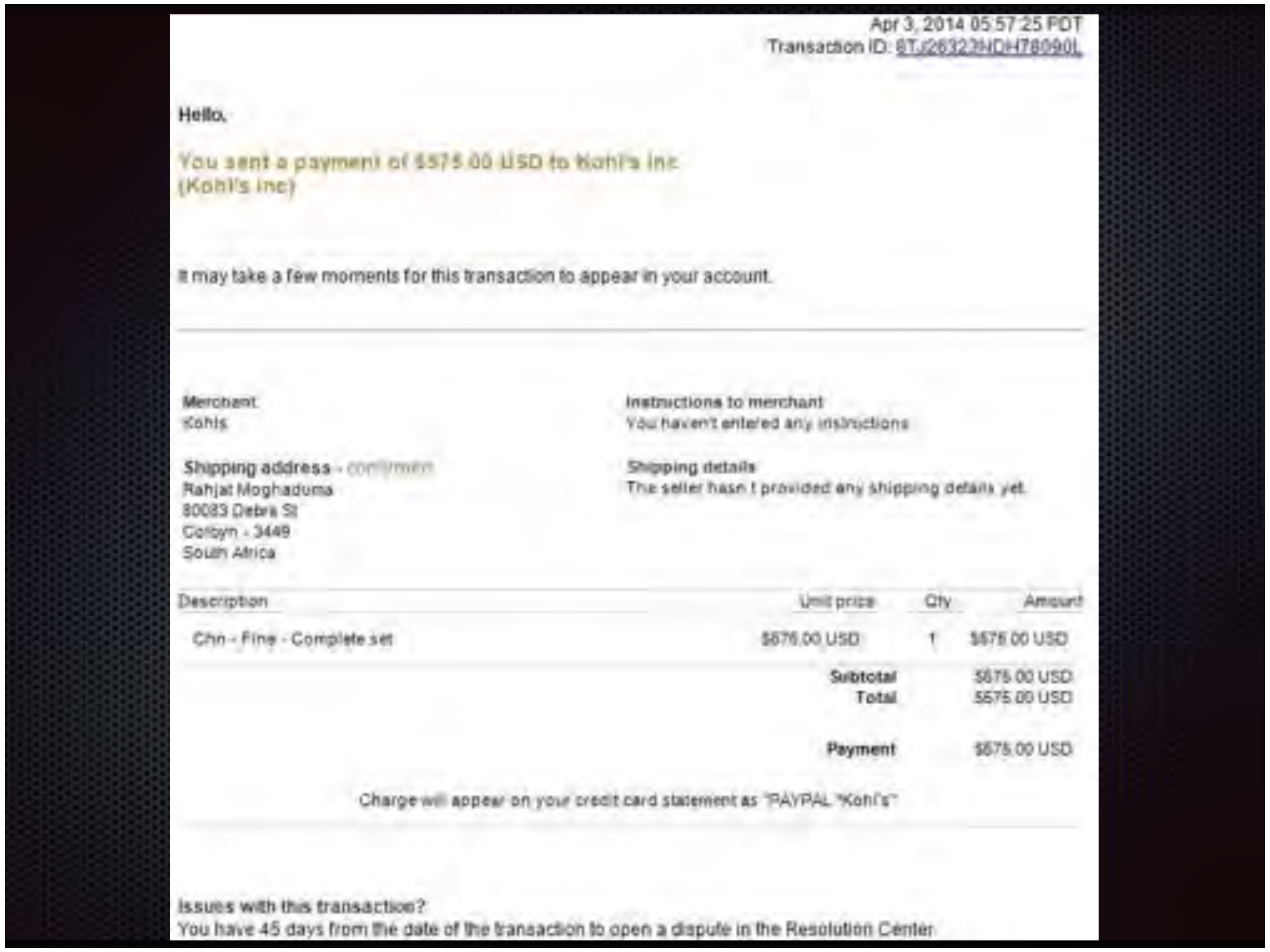
My personal fails

I have had personal massager fails… but that's a whole other talk.

FORTINET
Enterprise-Class Protection
Lowers Infrastructure Costs
Reduces WAN Costs
Dual WAN Links
FortiGate Firewalls
Firewalls, Managing & Analysis, Secure Messaging

masscan = bad idea

can bring fortinet’s and checkpoint’s to their knees



Apr 3, 2014 05:57:25 PDT
Transaction ID: 8TJ26323NDH78090L

Hello,

You sent a payment of $575.00 USD to Kohl's inc
(Kohl's inc)

It may take a few moments for this transaction to appear in your account.

Merchant
Kohls

Instructions to merchant
You haven't entered any instructions

Shipping address - confirmed
Rahjat Moghaduma
80083 Debra St
Colbyn - 3449
South Africa

Shipping details
The seller hasn t provided any shipping details yet.

Description	Unit price	Qty	Amount
Chn - Fine - Complete set	$575.00 USD	1	$575.00 USD
	Subtotal		$575.00 USD
	Total		$575.00 USD
	Payment		$575.00 USD

Charge will appear on your credit card statement as "PAYPAL "Kohl's"

Issues with this transaction?
You have 45 days from the date of the transaction to open a dispute in the Resolution Center

I have another talk about this entire purple team exercise that grew into a security awareness program. I go into this program in detail in the talk, however about half way through I decided to use a fake Paypal/Kohl's receipt as a phish for click baiting. I inadvertently had a user cancel her paypal and Kohl's card and open up fraud cases with their support. Before she even realized that it came from a google address to her work email that wasn't even tied back to her personal account.

http://infosystir.blogspot.com/2015/02/the-path-to-fixing-security-awareness.html
Also the talk is on irongeek's site/youtube channel and a link on my blog. It's called "Shooting Phish in a Barrel and other bad puns"