STATE OF MOBILE HEALTH

CYBERHEALTH

Emerging threats and opportunities in an increasingly connected world

GORA DATTA
gora@cal2cal.com

@ HL7 SAN DIEGO WGM SEPT 13, 2017

- ✓ HL7 International Ambassador & Speaker
  - (founding) Co-Chair HL7 Mobile Health Work Group
  - HL7 2009 Volunteer of the Year Award Winner
- ✓ US Delegate to ISO/TC215 Health Informatics
- ✓ Chair IEEE Orange County
- ✓ (founding) Co-Chair IEEE OC CyberSecurity
- ✓ Senior Member IEEE
- ✓ Senior Member ACM
- ✓ US (DHHS) SENIOR HEALTH-IT SME
- ✓ EHR MACRA & Meaningful Use Expert
- ✓ ICT Expert - Asian Development Bank, World Bank
- ✓ Group Chairman & CEO CAL2CAL Corporation

TALK ABSTRACT

- With the phenomenal rise of mobile devices globally in the past decade, we have now entered the digital age – the agricultural age, the scientific age, the industrial age, the information age and now the digital age! This global transformation is bringing a change that is impacting our world in every way - how we interact, play, read, write, watch, study, research, work or even relax. Soon we will live in a world which is interconnected through the Internet of Things (IoT).
- Healthcare access & delivery is going through a seismic change…rapidly moving from paper to digital health. Health information technology (Health IT) is making it possible for health care providers to better manage patient care through secure use and sharing of health information. However, recent news headings (e.g. WannaCry ransomware attacks in May 2017) are amply demonstrating the wake-up call….cybersecurity is redefining this changing world of digital health.
- In this talk, we will review the digital health transformation that we are undergoing, the challenges of cyber-health that faces us and the mitigation that is critical in the 21st century IoT world we live in.

21st CENTURY WORLD

WHAT WAS NOT THERE IN 1917!

- NO Commercial Airline flights
- NO Penicillin
- NO (rotary dial) telephone
- NO TV
- NO Computers
- NO Internet
- NO Facebook
- No Snapchat
- NO Twitter…..(no Social Media)

LIFE IN THE FAST (MOBILE) LANE!
21st Century Living

1. Next generation: “iPAD™” kids
2. Blurred Lines:
   - Impact of Social Media
   - Concept of Privacy, Security, Access
3. Are we there yet: I want it NOW
4. Take Charge: Consumer in control
5. Gene to genes: from Star-Trek (Gene Roddenberry) to Genetic Health – life imitating art!
6. Space – The Final Frontier

…..21st CENTURY LIVING (cont.)

7. Back to the Future: Longitudinal Record
8. Live long & prosper: from provenance to preservation
9. Emerging Areas: IoT, Big Data, Cloud, AR/VR/MR
10. Global Village: Urban, Rural, Remote, Underserved
11. l'addition s'il vous plaît: Mobile micro-payments
12. Take care: CyberSecurity, Blockchain
13. “Watson dating Alexa?”: Machine Learning, AI, Bots

MOBILE & IoT REVOLUTION!

- Mobile phone market
  - first billion mobile phones: 20 years
  - second billion phones: 4 years
  - third billion: 2 years
  - Fourth & fifth billion: 1 year – in 2013
  - 2014: nearly One Billion “smart” mobile phones sold globally
  - 2015 – > 1.2B units
  - 2016 – > 1.5B units
- IoT connected world by 2020
  - Projected to be 50 Billion devices

21st CENTURY HEALTHCARE

Changing Landscape: Paper to Digital

- Stage 1: capture coded data
  - 1) Capturing health information in a coded format,
  - 2) Using the information to track key clinical conditions;
  - 3) Communicating captured information for care coordination purposes;
  - 4) Reporting of clinical quality measures and public health information.
- Stage 2: share information
  - Focus on interoperability, disease management, clinical decision support, support for patient access to their health information, transitions in care, quality measurement, research, and bi-directional communication with public health agencies.
- Stage 3: convert data to knowledge
  - Focus on achieving improvements in quality, safety and efficiency, focusing on decision support for national high priority conditions, patient access to self-management tools, access to comprehensive patient data and improving population health outcomes.

What is driving this phenomenal growth?

- KEY DRIVERS
  - Increasing global population
  - Aging population (not only a developed world issue)
  - Higher Life Expectancy (people living longer)
  - Increasing Chronic diseases*: e.g., diabetes, obesity, heart disease etc.
  - Emergence of Personalized medicine
  - Global reach of diseases
  - Technological advances

[Chronic Disease is a long-lasting condition that can be controlled but not cured]

DOLLAR$ and NO CENTS!

HEALTHCARE MARKET SIZE

- US GDP (2016)
  - $18.6T (=$18,569.1 Billion)*
- US Healthcare spending: 18% of GDP = $3.3T
  - (> ∑ of healthcare spending of rest of the world!)
- US Projected GDP by 2022
  - $23T
- US (projected) healthcare spending in 2020

  20% of the GDP = $4.6T

* https://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm

WORLD OF CYBERSECURITY*

- Ransomware damage cost: $325M in 2015 - $5B in 2017 (15x incr)
- 2016 Global “Cost” of cybercrime: $3T
- By 2021, this impact is expected to go up to $6T
- CyberSecurity spending to cross $1T by 2021 (currently around $80B)

NOW THE OPPORTUNITY

- Cybersecurity unemployment rate
  - 0 …..yes Zero!
- Cybersecurity jobs: Currently at around 1.2M / by 2021 – 3.5M!
- Online presence: from 2B today to over 4B by 2020

* http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

CYBERSECURITY EVENTS* OF THE PAST ~~YEAR~~ FOUR MONTHS

* https://www.identityforce.com/blog/2017-data-breaches

1. Docusign (5/17/17)
2. OneLogIn (5/31/17)
3. Kmart (5/31/17)
4. University of Oklahoma (6/14/17)
5. Washington State University (6/15/17)
6. Deep Root Analytics (6/20/17)
7. Blue Cross Blue Shield / Anthem (6/27/17)
8. California Association of Realtors (7/10/17)
9. Verizon (7/13/17)
10. Online Spambot (8/30/17)
11. TalentPen and TigerSwan (9/2/17)
12. Equifax (9/7/17)

CYBERHEALTH

US HIPAA BREACH DEFINITION

Under HIPAA (Health Information Portability & Accountability Act), a breach is defined as

"…the acquisition, access, use or disclosure of PHI in a manner not permitted under [HIPAA] which compromises the security or privacy of the PHI."

PHI=Protected Health Information

https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf

HEALTHCARE BREACHES OF 2017*

http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

1. Peachtree Neurological Clinic (177k patient)
2. UC Davis Health (15k patients)
3. Verizon (14m customers)
4. BUPA Global Health Insurance (108k customers)
5. Indiana Medicaid (1.1m)
6. Cleveland Medical Associates (22k patients)
7. Airway Oxygen (500k patients)
8. California-based Dougherty Laser Vision

HEALTHCARE BREACHES OF 2017* (cont#2)

9. Feinstein & Roe MDs in Los Angeles (6k patients)
10. La Quinta Center for Cosmetic Dentistry (6.3k patients)
11. Coliseum Pediatric Dentistry of Hampton, Virginia
12. Torrance, CA Memorial Medical Center
13. Molina Healthcare (4.8m patients)
14. WannaCry ransomware – NHS, England & Scotland + 150 other countries <<<<<<<<<<May 2017
15. New Jersey Diamond Institute (15k patients)

http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

HEALTHCARE BREACHES OF 2017* (cont#3)

16. Harrisburg Gastroenterology (93k patients)
17. Bronx-Lebanon Hospital Center (10k to million patients)
18. Aesthetic Dentistry, NY (3.4k patients)
19. OC Gastrocare (34k patients)
20. Tampa Bay Surgery Center (142k patients)
21. 500k children record from various pediatrics offices
22. Lifespan (20k patients)
23. HealthNow Network (918k patients)

http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

HEALTHCARE BREACHES OF 2017* (cont#4)

24. Harrisburg Gastroenterology (93k patients)
25. ABCD Children‘s Pediatrics (55k patients)
26. Washington University School of Medicine (80k patients)
27. Metropoliton Urology Group (18k patients)
28. Denton Health Group (7 years of EHR backup data)
29. Brand new Day Health Plan (14k patients)
30. Singh and Arora Oncology Hematology (22k patients)

http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

HEALTHCARE BREACHES OF 2017* (cont#5)

31. Verity Medical Foundation-San Jose Medical Group (1ok patients)

32. CoPilot Provider Support Services (220k patients)

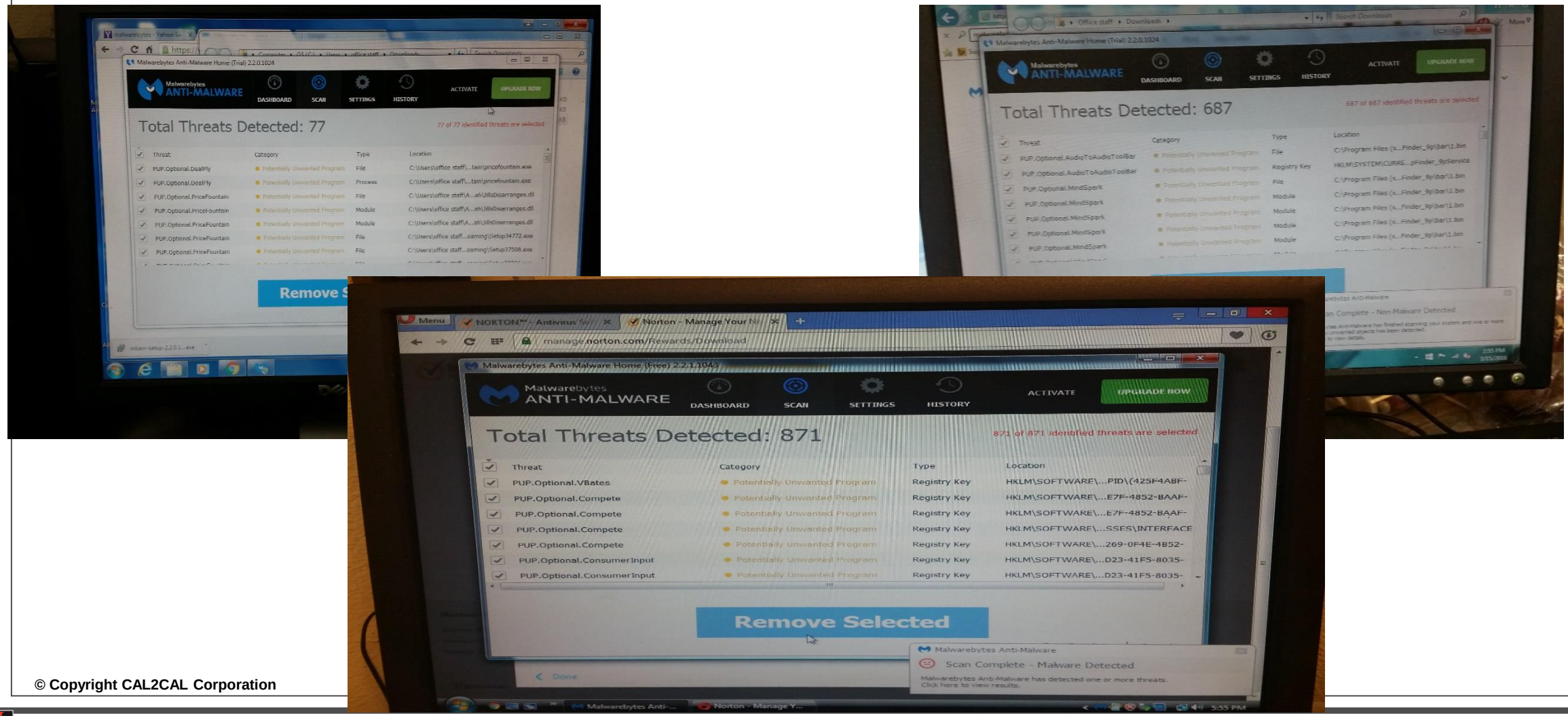
33. Cancer Services of East Central Indiana-Little Red Door ($43K ransom)

http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

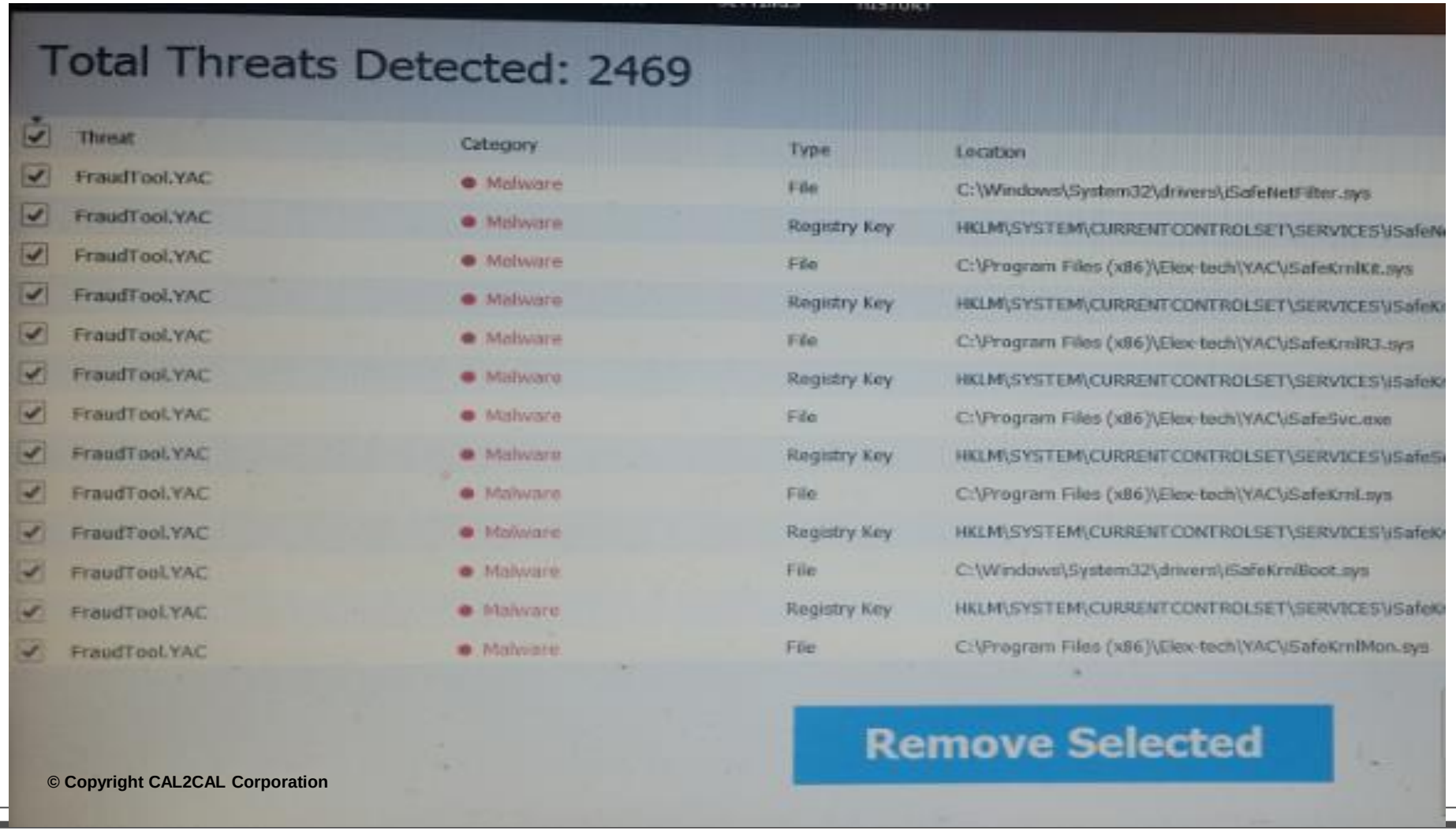
ANATOMY OF AN ATTACK*

* https://www.sonicwall.com/SonicWall.com/files/95/9546a705-3f0b-412e-a2cf-1d4f7d4ab026.pdf

A REAL WORLD STORY

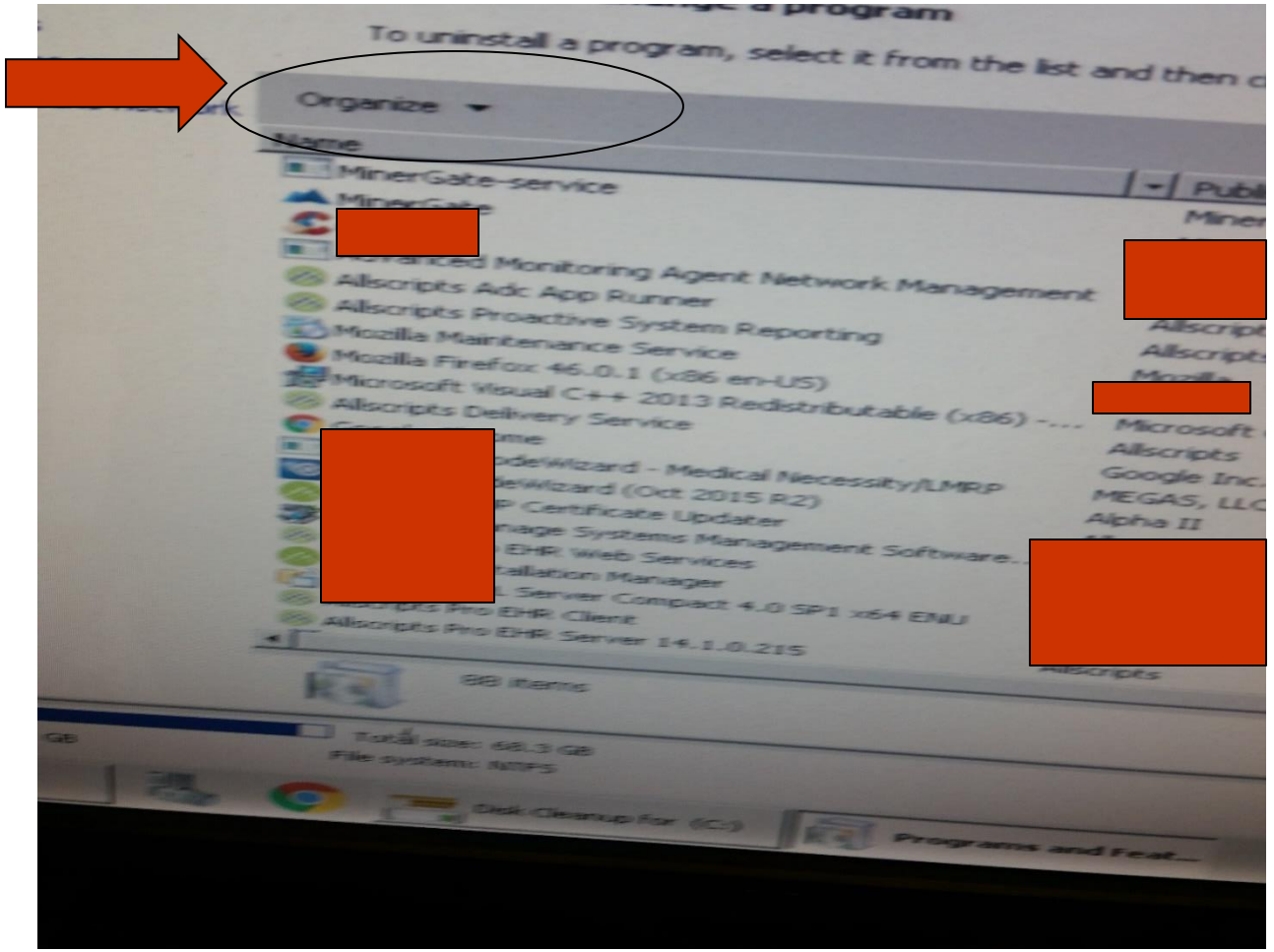


A REAL WORLD STORY (cont#2)



A REAL WORLD STORY (cont#3)

MinorGate

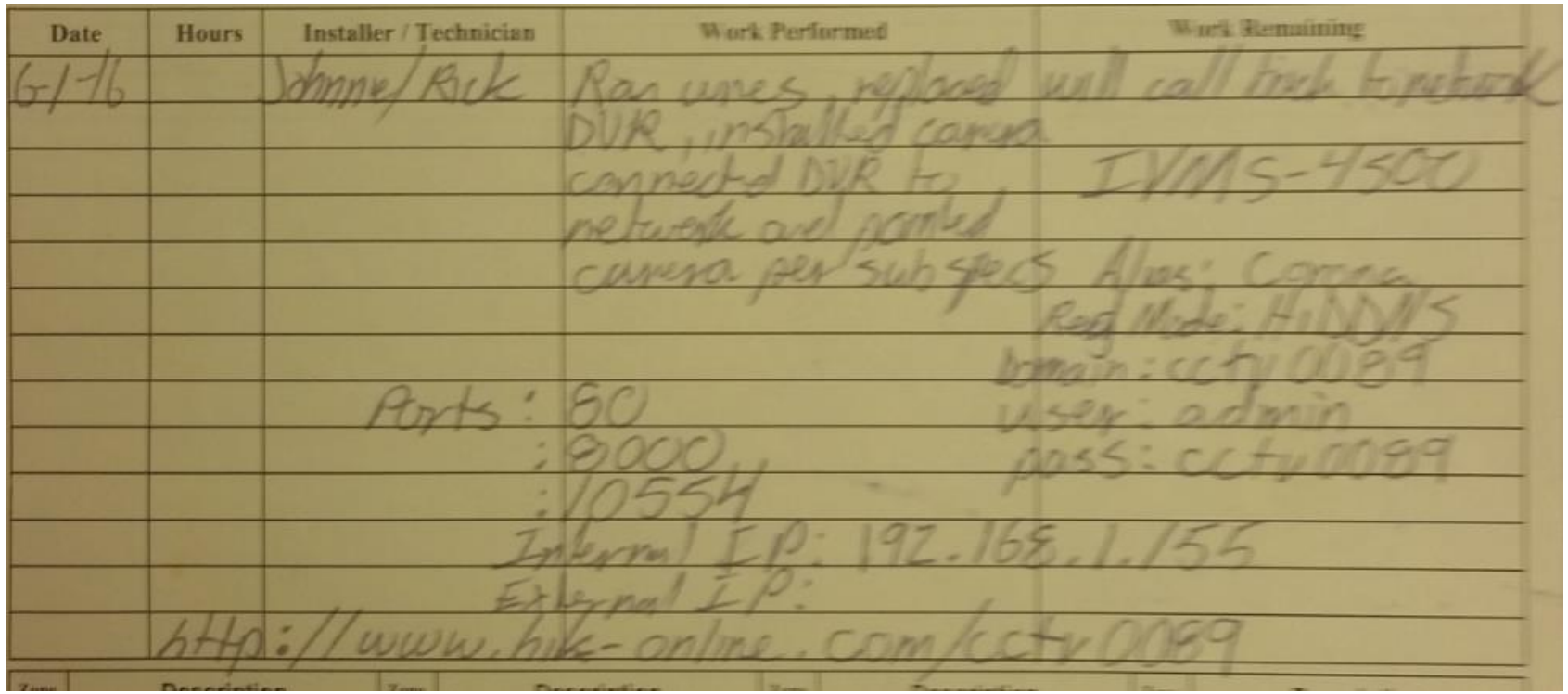


A REAL WORLD STORY (cont#4)

NICE PICTURE!

A REAL WORLD STORY (cont#5)

CCTV installation is a good idea?….WELL…..



Date	Hours	Installer / Technician	Work Performed	Work Remaining
6/1/16		Johnnie/Rick	Ran wires, replaced DVR, installed camera connected DVR to network and ported camera per subspecs	will call back to finish IVMS-4500
				Alias: Camera Reg Mode: HiDNS domain: cctv0089 user: admin pass: cctv0089
			Ports: 80 :9000 :10554	
			Internal IP: 192.168.1.155	
			External IP:	
			http://www.hik-online.com/cctv0089	

These were manufacturer supplied details. The Practice has since updated these.

TELL-TALE: Elementary my dear Watson!

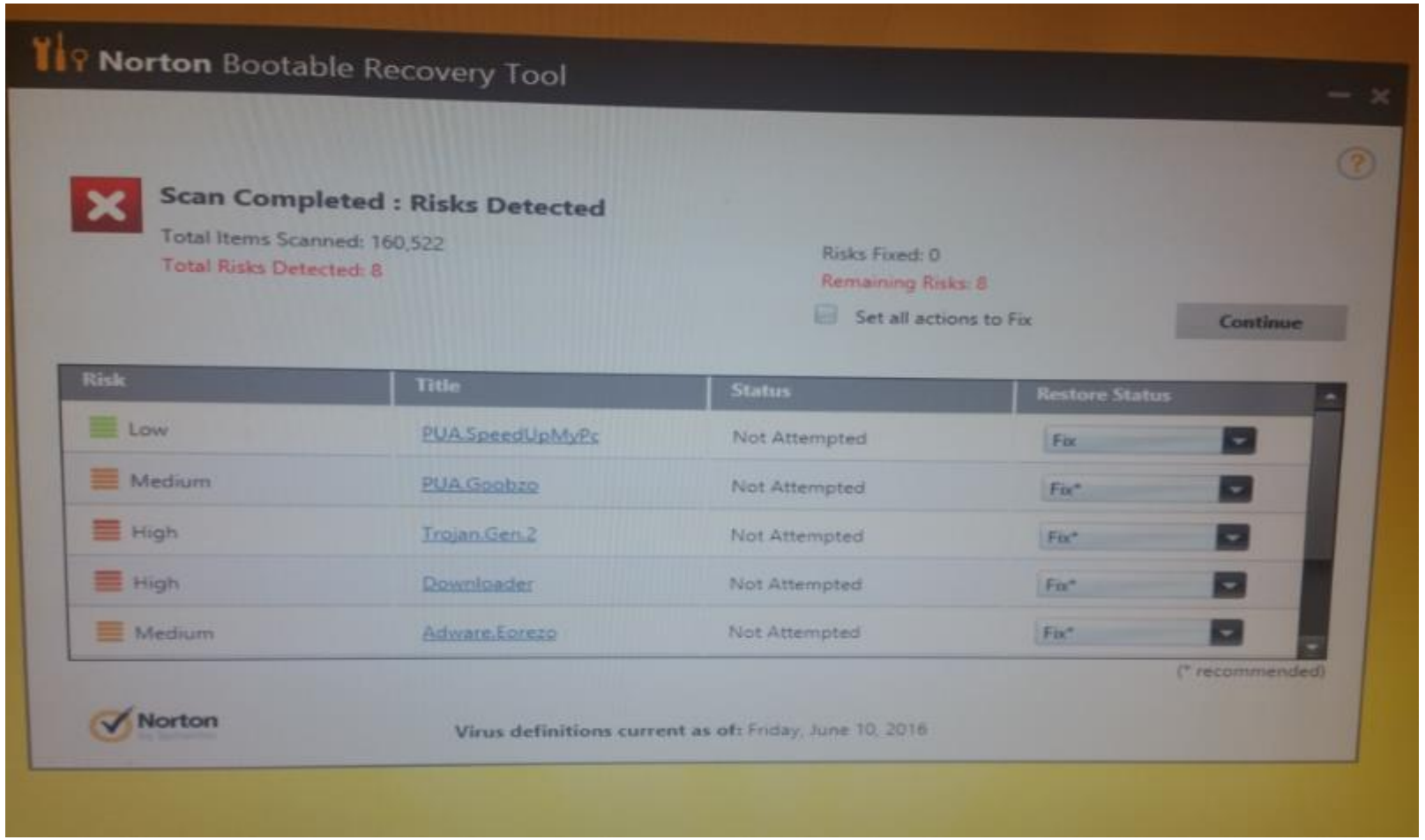
- Disk is corrupted or some message asking to call Microsoft Support at 1-800…. NOW
- Application showing a user (that you don't know of) is logged-in
- PC behaving strange/sluggish – can't really say what is wrong but the feel of it
- It's been a while since upgrades were run or AV was run
- Staff not trained on Security Risk Analysis

Next Steps…..(technical)

- Clear you calendar for the next many hours (days)!
- Ring-fence & isolate the impacted device(s)
  - No internet connection
- Figure out how to restart the device to boot mode - F2, F8, bang on all function keys! ☺
  - There is no standard
  - Change to boot off USB drive first
- Have your “Swiss army knife” ready way-way before….huh?

SWISS ARMY KNIFE

A bootable* portable disk that you have created!



* https://support.norton.com/sp/en/us/home/current/solutions/v72380755_EndUserProfile_en_us

Next Steps…..(administrative)

- Know your Federal as well as State laws regarding data breach
- Inform your Provider(s)/Management immediately of any incident
- Inform the EHR vendor, ASAP
- Follow steps learnt during Security Compliance training

REMEMBER: What applies for patients, applies here as well!

PREVENTION IS FAR-FAR BETTER THAN CURE

SECURITY RISK ANALYSIS (SRA)

- HIPAA Compliance
  - Primarily, HIPAA rules apply to a Practice's security compliance and risk management activities.
  - It also specifically serves to protect the EHR and to keep practice's sensitive data (also known as electronic Protected Health Information, ePHI) secure.
  - Security compliance and a Security Risk Analysis (SRA) is NOT optional for the small (with annual receipts of $5M or less) and medium sized health care providers.

Security Risk Assessment (SRA)

Implement policies and procedures to prevent, detect, contain, and correct security violations [45 CFR §164.308(a)(1)(i)]

- Administrative-Does the practice supply proper training, on-going audits, vulnerability scans, follow best practices?
- Physical-Does the practice secure critical infrastructure, i.e., workstations, files, devices, cabinets, doors, lab equipment?
- Technical-Does the practice secure Wi-Fi, devices, gateways?

SRA: ASSESSMENT#1

ADMINISTRATIVE SAFEGUARDS

These safeguards establish standards and specifications for the health information security program that include the following:

- Security management processes to identify and analyze risks to e-PHI and implementing security measures to reduce risks
- Staff training to ensure knowledge of and compliance with the policies and procedures
- Information access management to limit access to electronic health records to protect health information, including the information in EHRs
- Contingency plan to respond to emergencies or restore lost data

SRA: ASSESSMENT#2

PHYSICAL SAFEGUARDS

These safeguards control physical access to your office and computer systems. Examples of required physical safeguards include:

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users
- Workstation use policies to ensure proper access to and use of workstations

SRA: ASSESSMENT#3A

TECHNICAL SAFEGUARDS

These safeguards include hardware, software, and other technology that limits access to e-PHI.

- Access controls to restrict access to PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper e-PHI alteration or destruction
- Transmission security measures to protect e-PHI when transmitted over an electronic network
- Monitoring file integrity

SRA: ASSESSMENT#3B

TECHNICAL SAFEGUARDS (cont.)

- Implementing file versioning systems
- Implementing file integrity testing capabilities
- Monitoring user activity
- Managing configurations
- Utilizing database rollback tools
- Managing virtual machine integrity through snapshots and versioning

SRA: RISK MITIGATION

- Continuous monitoring
- Maintaining ongoing awareness help reduce organizational risk:
  - assets,
  - individuals, and
  - other organizations
- Protective measures involve a combination of prevention, avoidance, deterrence, detection, recovery and correction.
- Data interoperability and cybersecurity are intertwined, requiring both communication and understanding of agreed upon security and privacy policies.

SECURITY RISK ANALYSIS

CAL2CAL corporation

COMPREHENSIVE SECURITY STANDARDS AND PROTOCOL
FOR THE PROTECTION OF ELECTRONIC HEALTH INFORMATION
FOR [COMPANY]
A Security Compliance Approach

Revision 2 June 2016

SECURITY STANDARDS AND PROTOCOL
FOR THE PROTECTION OF ELECTRONIC HEALTH INFORMATION

TABLE OF CONTENTS

The next few slides are for illustrative purposes only.

SECURITY RISK ANALYSIS (cont#2)

SECURITY RISK ANALYSIS (cont#3)

SECURITY RISK ANALYSIS (cont#3)

Health IT Security Policies and Procedures

EDITION: Jan 2, 2015

Table of Contents

1. HIT Policy List & Overview (this document)
2. Acceptable use
3. Backup
4. Confidential Data
5. Data Classification
6. Email Policy
7. Encryption
8. Guest Access
9. Incident Response
10. Mobil Device
11. Network Access
12. Network Security
13. Outsourcing
14. Password
15. Physical Security
16. Remote Access
17. Retention
18. Third Party Connection
19. VPN Access
20. Wireless Access

Signature:

Policy Document Set APPROVED: Managing Physician/ Privacy & Security Officer

KEY TAKEAWAYS!

- Changing Landscape: Paper to Digital
- World of IoT & Mobile
- Life in 21st century: not your parent's world!
- Understand the expectations of the current (and future) generation
- CyberSecurity is the unwelcomed but a permanent roommate
- Healthy advice: Prevention is always better than cure

SUMMARY!

- As we transition to a digital record framework; use of Mobile Technology leads the way (in access, capture and dissemination of information)
- As Mobile & IoT Devices become more and more ubiquitous, accessing our Information is only a few tap/swipe/transmit away!
- “WASH YOUR HANDS” – CYBER HYGIENE is critical in the world we live in
- LIFE IN 21st CENTURY
  - Cloud connected, IoT driven, micro-services enabled cyber-safe Digital world

THANK YOU

gora@cal2cal.com