Targeting Critical Infrastructure: Direct threats to Healthcare in Canada

Richard Staynings
Global Cybersecurity Healthcare Leader
Cisco

2017 CANADIAN CONFERENCE ON PHYSICIAN LEADERSHIP

FACULTY: Richard Staynings

Relationship with commercial interests:

- Employee of Cisco

CSPL
Canadian Society of Physician Leaders

SCLM
Société canadienne des leaders médicaux

joule
A CMA Company
Société de l'AMC

2017 CANADIAN CONFERENCE ON PHYSICIAN LEADERSHIP

Disclosure of Commercial Support

Potential for conflict(s) of interest:

- Richard is an employee of Cisco and holds stock in the company.

CSPL
Canadian Society of
Physician Leaders

SCLM
Société canadienne
des leaders médicaux

joule
A CMA Company
Société de l'AMC

Mitigating Potential Bias

- Content of this discussion is in relation to knowledge and awareness of cyber security

We live today in Wired World of interconnectivity !

Where almost **Everything** is connected

Internet Connected Devices

- In 2008 the number of things connected to the Internet surpassed the global human population

- By 2020, there will be in excess of 30 billion smart devices

Connected Cities

1 Citizen Services

2 Citizen Engagement

3 Parking optimization

4 Incident management

5 Public safety

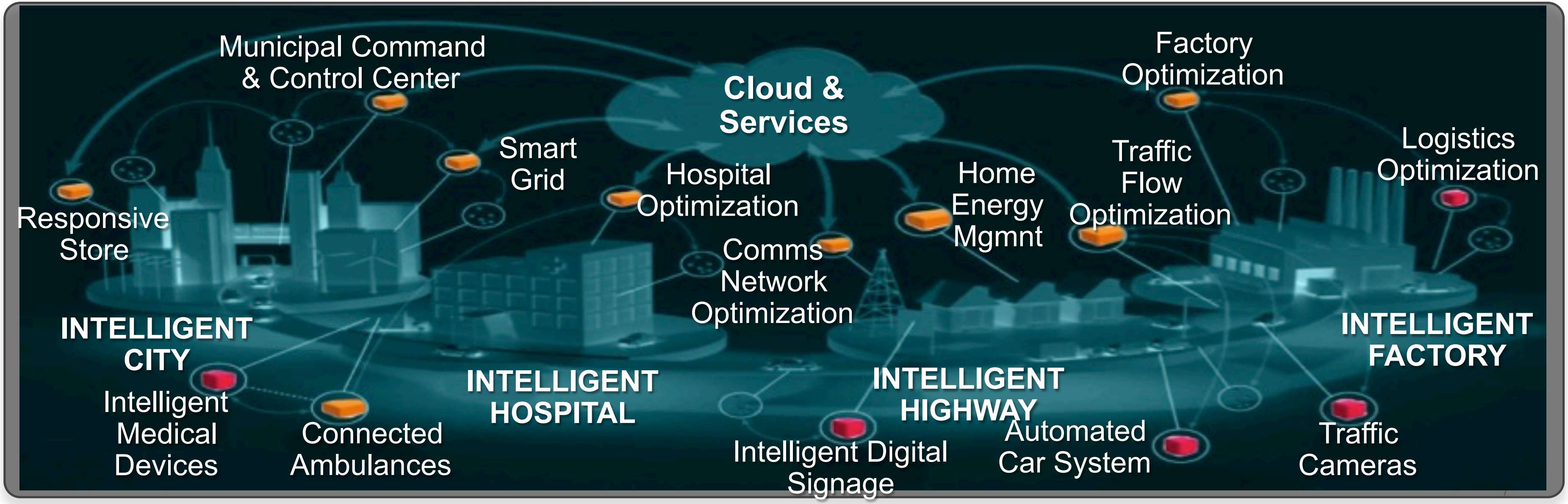
6 City lighting

7 Transportation

8 Sports & Entertainment

9 Education

10 Health & Wellness



Municipal Command & Control Center

Cloud & Services

Factory Optimization

Smart Grid

Hospital Optimization

Home Energy Mgmnt

Traffic Flow Optimization

Logistics Optimization

Responsive Store

Comms Network Optimization

INTELLIGENT CITY

INTELLIGENT FACTORY

Intelligent Medical Devices

Connected Ambulances

INTELLIGENT HOSPITAL

INTELLIGENT HIGHWAY

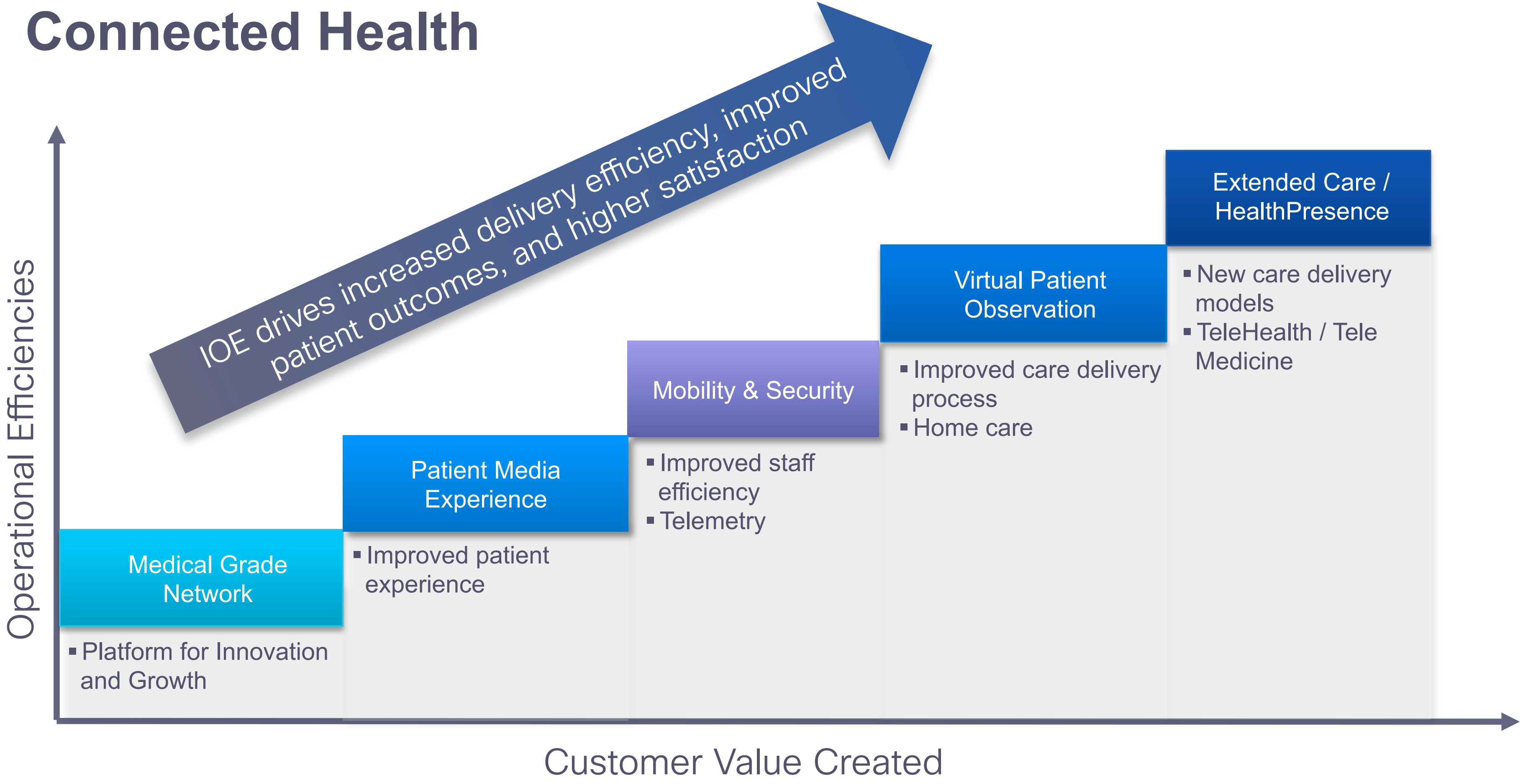
Intelligent Digital Signage

Automated Car System

Traffic Cameras

Source: Intel

Connected Health



IOE drives increased delivery efficiency, improved patient outcomes, and higher satisfaction

Operational Efficiencies

Medical Grade Network

- Platform for Innovation and Growth

Patient Media Experience

- Improved patient experience

Mobility & Security

- Improved staff efficiency
- Telemetry

Virtual Patient Observation

- Improved care delivery process
- Home care

Extended Care / HealthPresence

- New care delivery models
- TeleHealth / Tele Medicine

Customer Value Created

The Changing Face of ….. Security

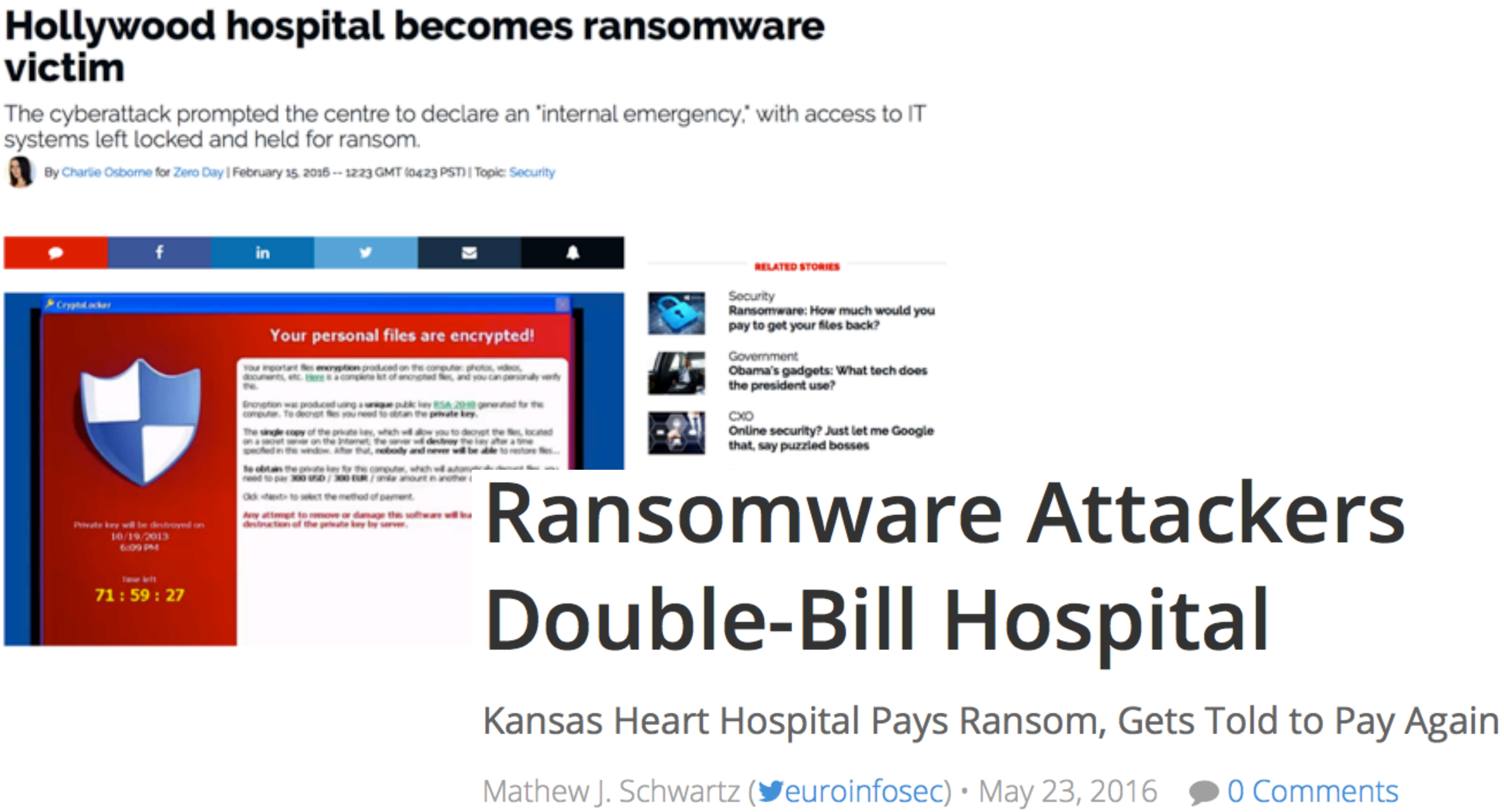
The Internet of EVERYTHING

What do we mean by Security?

- Confidentiality (privacy breach)
- Integrity (accidental or purposeful corruption of data)
- Availability (denial of service attack, DDOS, ransomware, etc.)

of data and systems

Healthcare is under attack!



Hollywood hospital becomes ransomware victim

The cyberattack prompted the centre to declare an "internal emergency," with access to IT systems left locked and held for ransom.

By Charlie Osborne for Zero Day | February 15, 2016 -- 12:23 GMT (04:23 PST) | Topic: Security

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another c

Click <Next> to select the method of payment.

Any attempt to remove or damage this software will lea destruction of the private key by server.

Private key will be destroyed on
10/19/2013
6:09 PM

Time left
71 : 59 : 27

RELATED STORIES

Security
Ransomware: How much would you pay to get your files back?

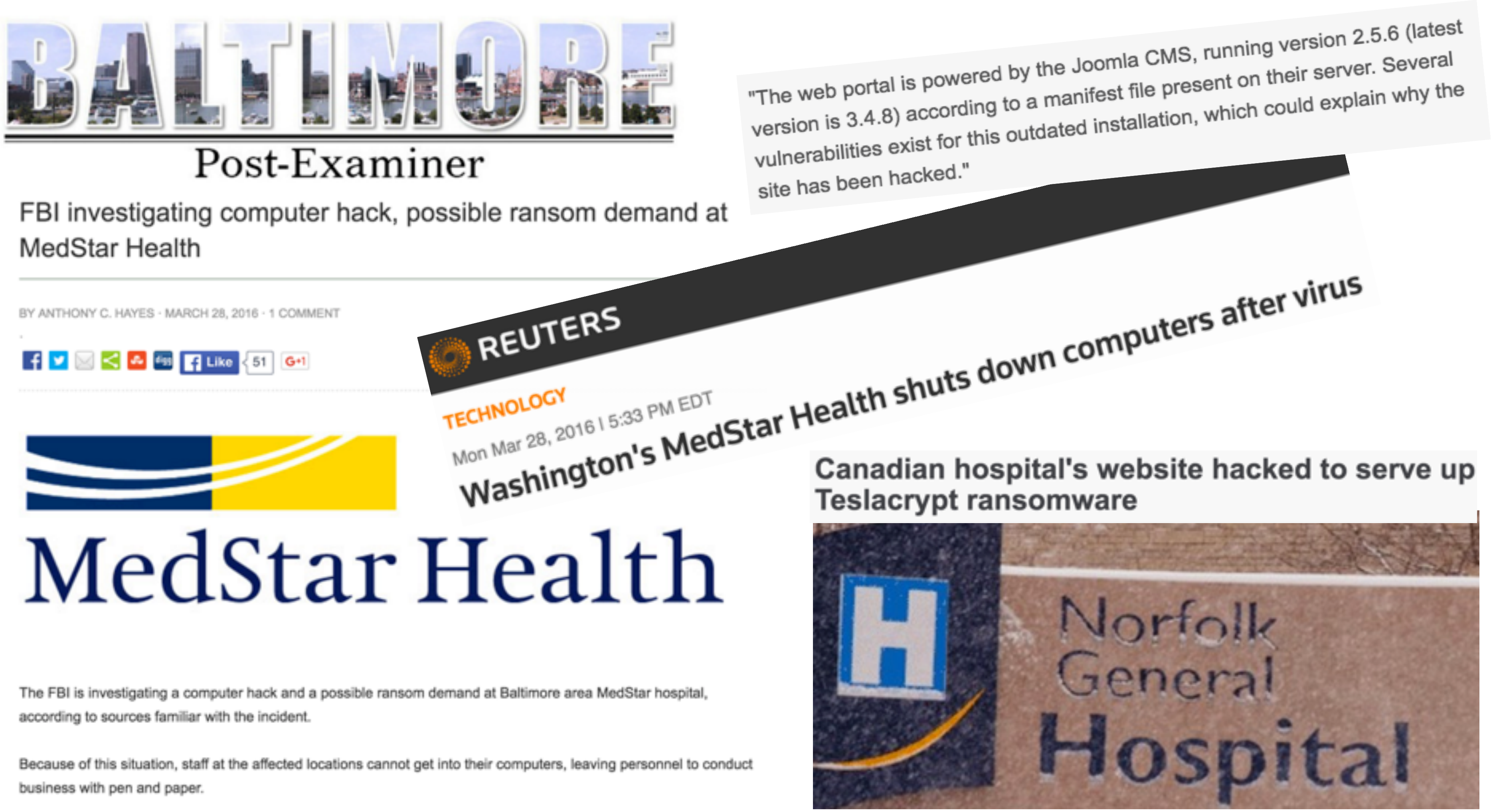
Government
Obama's gadgets: What tech does the president use?

CXO
Online security? Just let me Google that, say puzzled bosses

Ransomware Attackers Double-Bill Hospital

Kansas Heart Hospital Pays Ransom, Gets Told to Pay Again

Mathew J. Schwartz (euroinfosec) • May 23, 2016 0 Comments



FBI investigating computer hack, possible ransom demand at MedStar Health

BY ANTHONY C. HAYES · MARCH 28, 2016 · 1 COMMENT

The FBI is investigating a computer hack and a possible ransom demand at Baltimore area MedStar hospital, according to sources familiar with the incident.

Because of this situation, staff at the affected locations cannot get into their computers, leaving personnel to conduct business with pen and paper.

"The web portal is powered by the Joomla CMS, running version 2.5.6 (latest version is 3.4.8) according to a manifest file present on their server. Several vulnerabilities exist for this outdated installation, which could explain why the site has been hacked."

TECHNOLOGY

Mon Mar 28, 2016 | 5:33 PM EDT

Washington's MedStar Health shuts down computers after virus

Canadian hospital's website hacked to serve up Teslacrypt ransomware

KDH

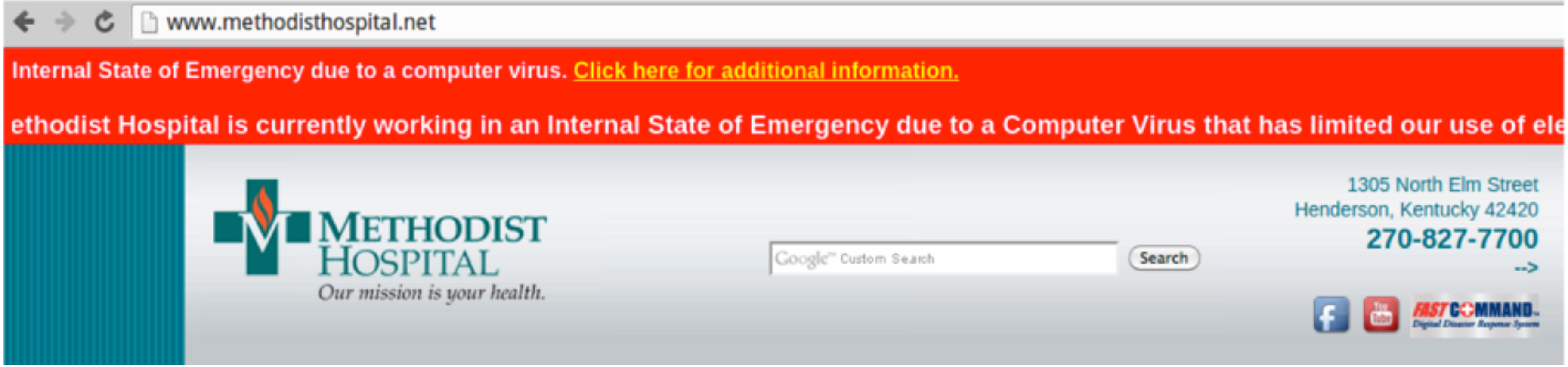
King's Daughters' Health

Community People. Quality Care.

KDH operates an 86-bed hospital and physicians' office in Madison, Ind. – Hit by Locky Ransomware March 30th on a single computer but shut whole network down

March 18- two of Prime Healthcare's hospitals in California - Chino Valley Medical Center and Desert Valley Hospital shutdown because of ransomware attack

March 16th, Kentucky Methodist Hospital – forced to shutdown computer systems when hit with Locky Ransomware.



www.methodisthospital.net

Internal State of Emergency due to a computer virus. Click here for additional information.

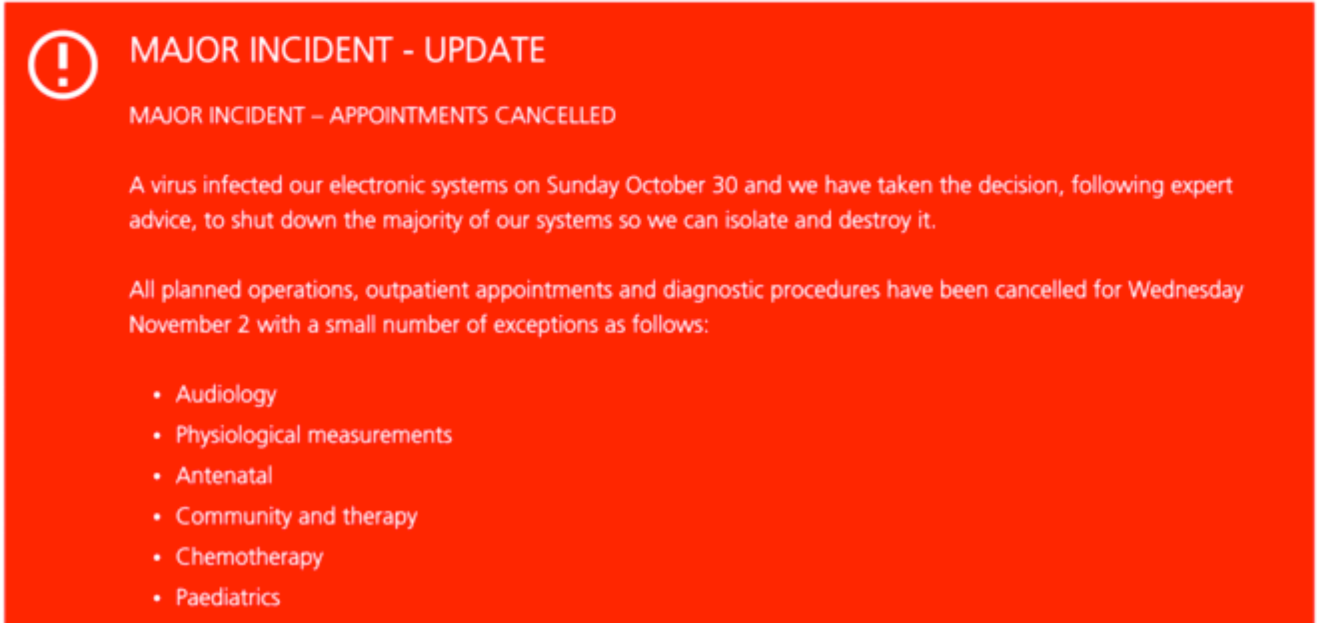
ethodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of ele

METHODIST HOSPITAL

Our mission is your health.

1305 North Elm Street
Henderson, Kentucky 42420
270-827-7700

Northern Lincolnshire and Goole NHS Foundation Trust cancels ALL operations after cyber attack



MAJOR INCIDENT - UPDATE

MAJOR INCIDENT – APPOINTMENTS CANCELLED

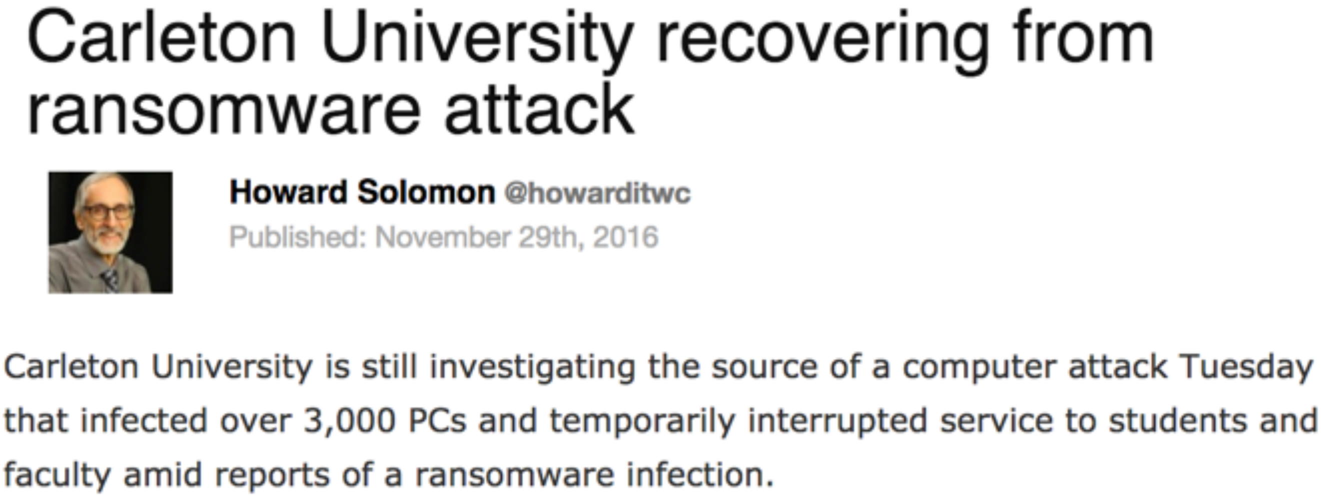
A virus infected our electronic systems on Sunday October 30 and we have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it.

All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday November 2 with a small number of exceptions as follows:

- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics

Patients told not to turn up for appointments or for surgery

IT WORLD CANADA

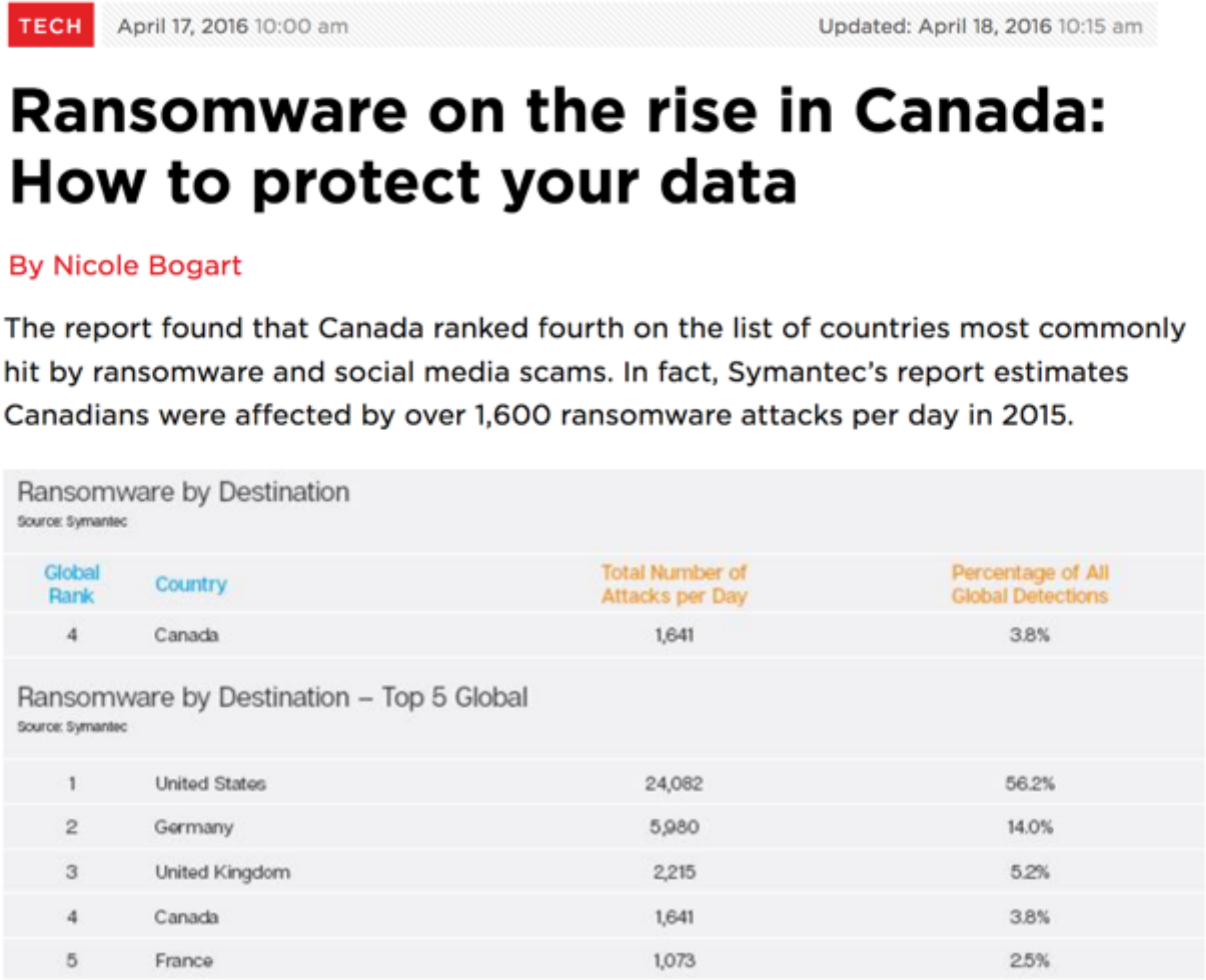


Carleton University recovering from ransomware attack

Howard Solomon @howarditwc
Published: November 29th, 2016

Carleton University is still investigating the source of a computer attack Tuesday that infected over 3,000 PCs and temporarily interrupted service to students and faculty amid reports of a ransomware infection.

Global NEWS



TECH April 17, 2016 10:00 am Updated: April 18, 2016 10:15 am

Ransomware on the rise in Canada: How to protect your data

By Nicole Bogart

The report found that Canada ranked fourth on the list of countries most commonly hit by ransomware and social media scams. In fact, Symantec's report estimates Canadians were affected by over 1,600 ransomware attacks per day in 2015.

Ransomware by Destination

Source: Symantec

Global Rank	Country	Total Number of Attacks per Day	Percentage of All Global Detections
4	Canada	1,641	3.8%

Ransomware by Destination – Top 5 Global

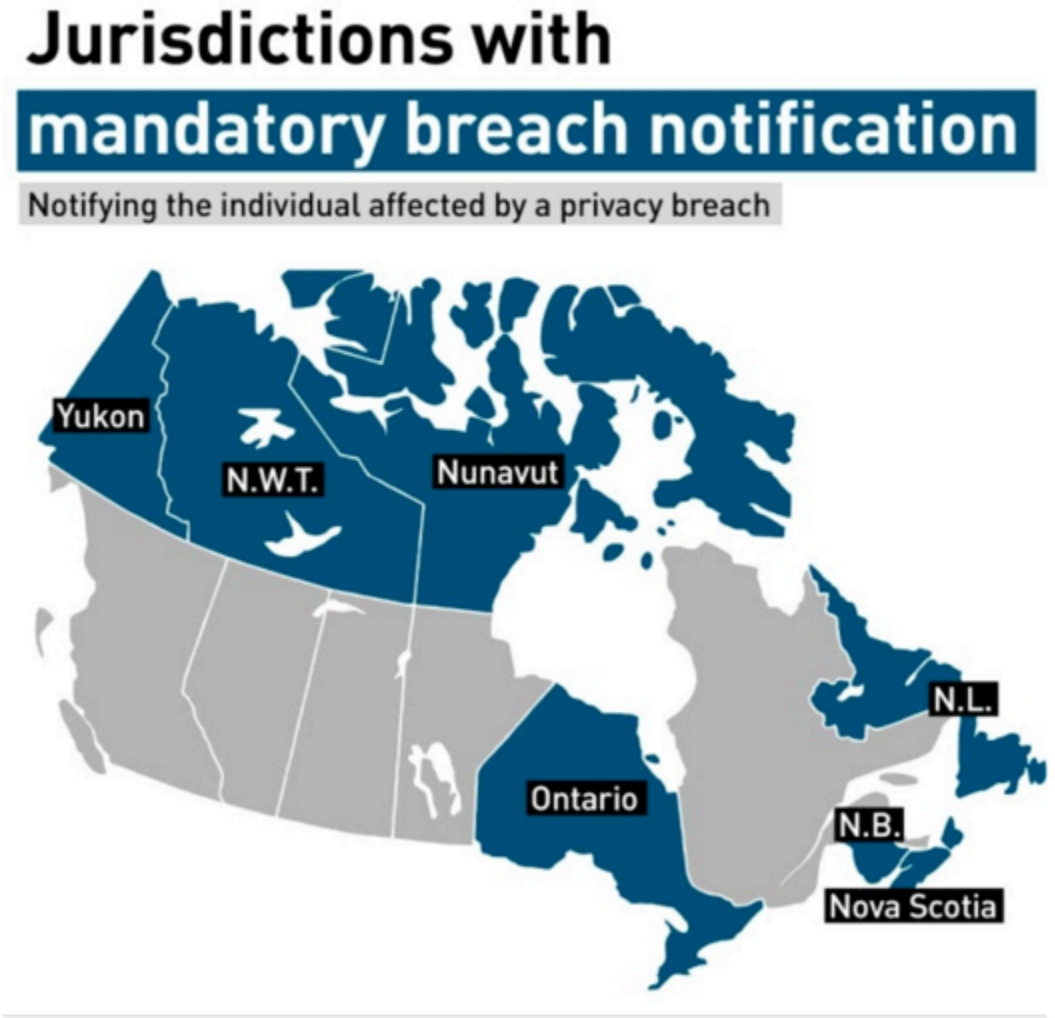
Source: Symantec

1	United States	24,082	56.2%
2	Germany	5,980	14.0%
3	United Kingdom	2,215	5.2%
4	Canada	1,641	3.8%
5	France	1,073	2.5%

The number of breaches and ransomware attacks in Canadian Health is much worse than most people think:

- No uniform Breach Notification Requirement

- Most breaches go undetected and unreported



Jurisdictions with mandatory breach notification

Notifying the individual affected by a privacy breach

Direct Attacks Generate Big Profits for **One Gang!**

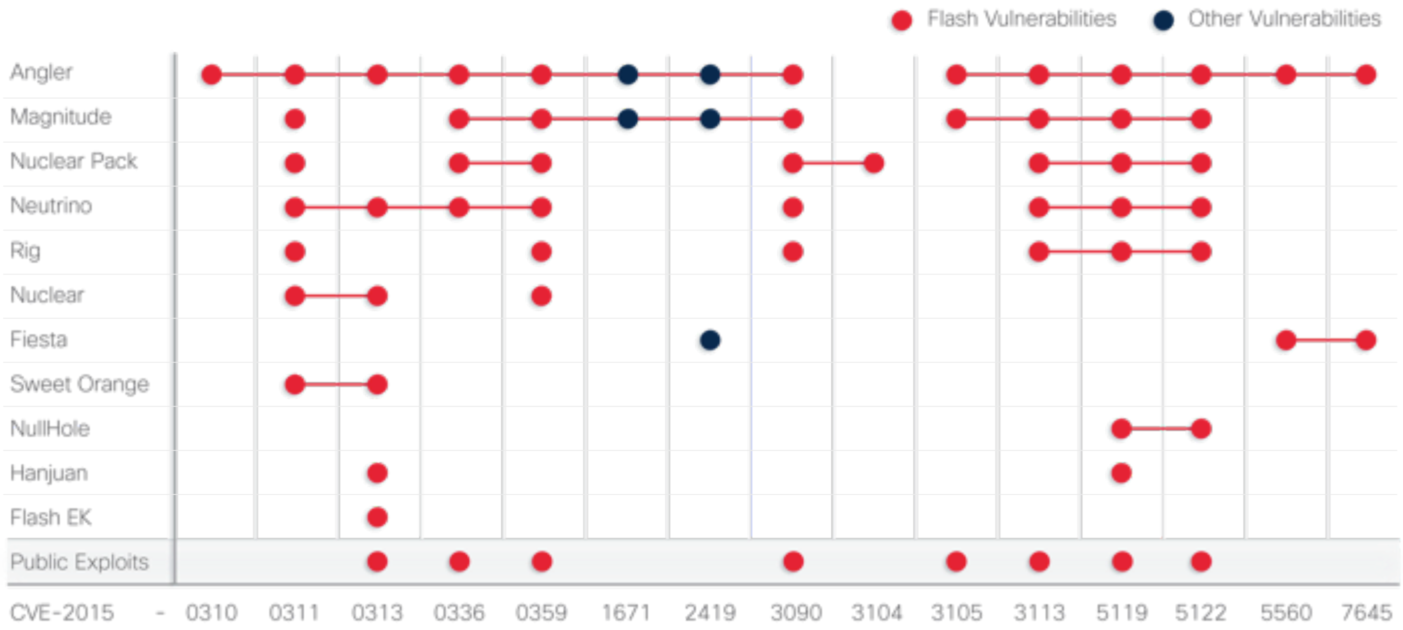
Angler / other ransomware attacks – Highly lucrative

$300 average ransom X 317.18 ransoms paid per day X 365 days in a year = $34M gross yearly income for ransomware per campaign

(Cisco 2016 Annual Security Report)

>> >> “Per Campaign!”

Hackers Love Flash! (The less patched the better!)



Flash platform is a popular threat vector for cybercriminals

Its not just about Ransomware!

IT WORLD CANADA

CANADIAN DDOS ATTACKS ON THE RISE

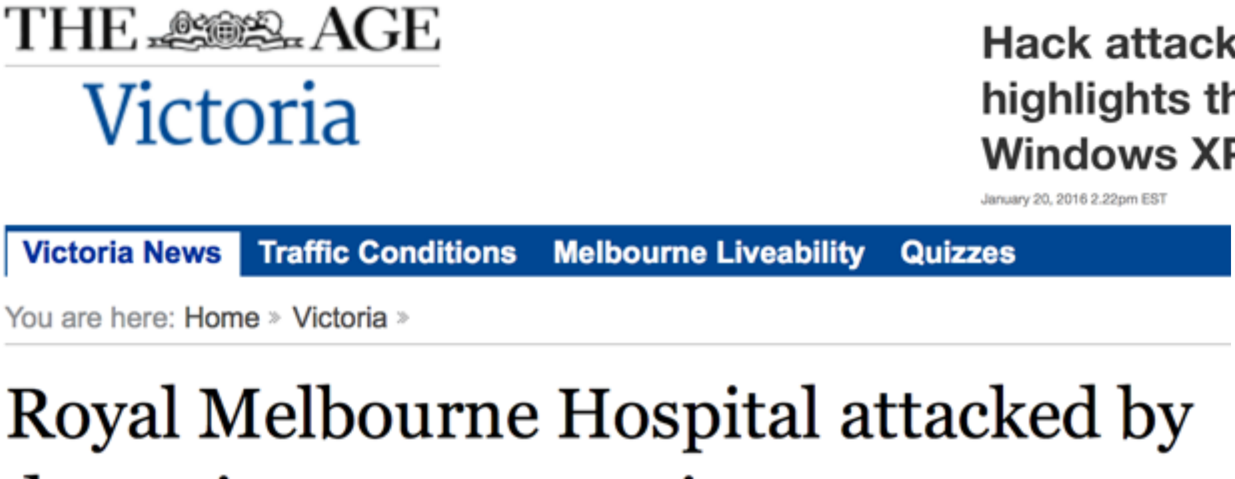
Publish on: **17 January 2017**

Category: SNAPI Guard,

How the ‘Internet of unpatchable things’ leads to DDoS attacks

Howard Solomon @howarditwc

Published: October 11th, 2016



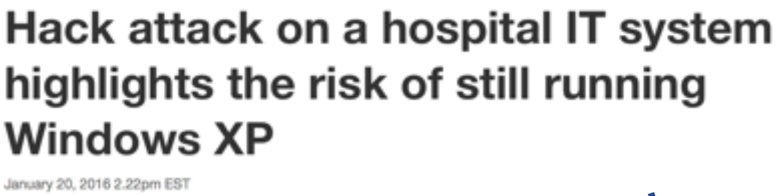
THE AGE

Victoria

Victoria News | Traffic Conditions | Melbourne Liveability | Quizzes

You are here: Home » Victoria »

Royal Melbourne Hospital attacked by damaging computer virus



Hack attack on a hospital IT system highlights the risk of still running Windows XP

January 20, 2016 2.22pm EST

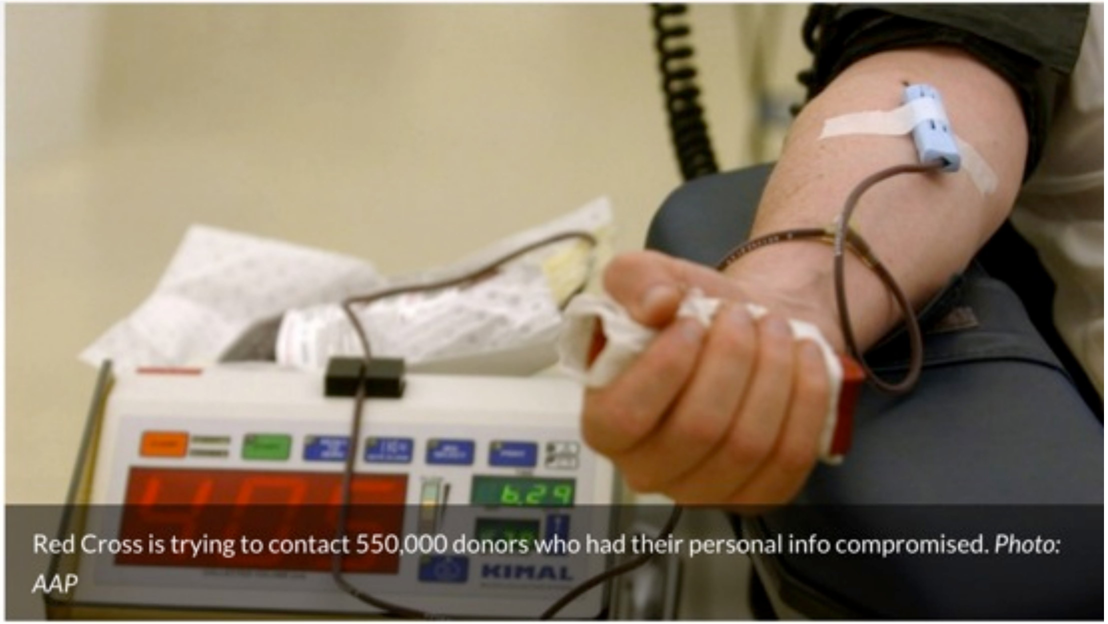
Signature Based Protection failure

Qbot virus still attacking Royal Melbourne Hospital

A computer virus that can steal passwords is still causing headaches at one of Melbourne's largest hospitals.

By Chris Duckett | February 2, 2016 -- 04:51 GMT (20:51 PST) | Topic: Security

Half a million blood donors hacked in massive security breach at Australian Red Cross



Red Cross is trying to contact 550,000 donors who had their personal info compromised. *Photo: AAP*

The Red Cross said it had been made aware that a file containing donor information was placed on an insecure computer environment and accessed by an unauthorised person.

The file was part of an online application to give blood used from 2010.

Red Cross chief executive Shelly Park has apologised to donors and said, to her knowledge, all copies of the data had now been deleted and the risk of misuse of the data was low.

Ms Park said the issue occurred due to human error.

Allow users to do their job – SECURELY!

THE NEWDAILY

Clinical Research?

Who’s Intellectual Property?

State Sponsored PLA
Cyber Espionage

Despite a US / PRC agreement Hacking Continues

Deep Panda
The hackers .. dubbed Deep Panda by CrowdStrike….said that the primary benefits of the intrusion seem to be “clearly aligned to facilitate theft of intellectual property and trade secrets”

…Former FBI special agent continued by saying that China's cyber-spying agencies have produced spectacular results in the past decade. “It's hard to believe China would agree to dismantle a large part of these organisations just because the US has asked them to do so. What's more, it's hard to believe the cyber-warriors who make up these organisations could be effectively contained.”

SC Magazine UK

China-USA non-hacking treaty 'already flouted' by Chinese hackers according to CrowdStrike data

Attacks are increasing in scope, size and frequency.

Its no longer a question of **“IF”** you get hacked
its now one of **“WHEN”** you get hacked
and ....”**HOW OFTEN”**

What has Changed and Why is Healthcare Under Attack?

In one line:

20 years of under-investment in Healthcare Security and an increasingly value-laden target

Healthcare is Seen as an Easy Target

Theft

- Theft of Medical Records - $45~$50* per
- Theft of full Identity – up to $500*
- Theft of clinical research / clinical trial data
- Theft of formulations / procedures

Malicious Attack – DOS / Integrity /

- Building Management Systems – Critical hospital systems – water, air, heat, mechanicals
- Medical Devices – to inflict patient harm / assassination / poisoning

* Figures in US dollars (2016)

Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Pause for Thought for a moment

Mindshare:

What keeps you up at night?

What Keeps Healthcare Senior Executives Up At Night?

Where do I Start?

- Holistic Security Planning & Road-Mapping
- Do mØre with le$$
- Where to focus scarce resources?
- Consume key security functions as a service?

IoT Device Security

- How do I secure the un-securable?
- Medical Devices / Labs
- Building Management Systems

How Can I defend Against an Attack?

- Security Operations / Incident Response
- Threat expertise... ?
- CSIRT... ?

Healthcare needs to Plan Much Better!

- Too busy implementing Security tools to actually managed security risks and threats
- Failure to understand what “Business Risk Reduction Benefits” tools provide
- The “Shiny Object” (shopping list) approach to Security
- We need to focus on **reducing risks**
- Follow a Security Framework:
  - ISO 27002
  - NIST SP800-53 & 66

There is no point blowing all your budget on the world's most secure front door if you can't afford window locks!

Security Network Segmentation

The need to segment flat healthcare networks has never been more urgent

The IOT / Medical Device Challenge

- 20% growth per annum in number of medical devices
- No common standards or security
- Windows Embedded 2009, (Windows XP)
- Dumb devices unable to support AV or End Point Protection
- Limited CPU and memory unable to sustain malware or DOS
- Half Life – Medical Devices last for up to 20 years
- Easiest way to infiltrate a healthcare network is via a medical device / medical device network – 802.11 40 bit WEP or RJ45 port
- Maximum patient harm can be an attack on a medical device

The Next Level of Ransoms…won’t be against data

It will likely be leveled directly against Hospital Building Management Systems and Medical Devices

The Next Level of Ransoms…won’t be against data

- IoT services we can’t do without:
  - HVAC,
  - Elevators / Lifts,
  - Water Management,
  - Electrical supply,
  - etc.

Imagine a man-made Hurricane Katrina….

…. A Cyber Attack against our Healthcare IOT Systems

The Next Level of Ransoms…won’t be against data

- Could Patient lives be held to ransom by compromised Medical Device?

In 2014, the Federal Bureau of Investigation issued a report that predicted hackers could assail medical devices

In 2015 they issued an alert warning companies and the public about cybersecurity risks to networked medical devices and wearable sensors

Cyber Assassin

You don’t need James Bond to carry out assassinations when you own the medical device targets are attached to

Russian Oligarch,
Mafia Boss or
innocent victim?

How Secure is your ICU?
How confident are you
about
the security of your medical
devices?

What if the NICU was compromised ?

Cybersecurity Risks in Medical Devices are Real

To address the cybersecurity threat, in December 2016 FDA issued Guidance on Postmarket Management of Cybersecurity in Medical Devices.

The agency highly recommends that both hospitals and medical device manufacturers implement a proactive, comprehensive risk management program that includes:

- Implementing the National Institute of Standards and Technology (NIST) Framework on Critical Infrastructure Cybersecurity
- Establishing and communicating processes for vulnerability intake and handling
- Adopting a coordinated disclosure policy and practice
- Deploying mitigations that address cybersecurity risk early and prior to exploitation
- Engaging in collaborative information sharing for cyber vulnerabilities and threats

The Weakest Link

So how can we go about protecting these simple networked devices in our healthcare environment? There are too many to manage individually!

We need to SEURELY SEGMENT them but in such a way that it doesn’t impede patient care.

Options:

1. Proxy traffic – simple, cheap, but doesn’t scale
2. Infrastructure Enclaving (firewall & switch ACLs, VRF, MPLS, etc.) – inflexible, expensive to run & maintain and impedes the business
3. Dynamic policy-based segmentation – define once, apply globally

Pause for Thought for a moment

Security Operations Centers

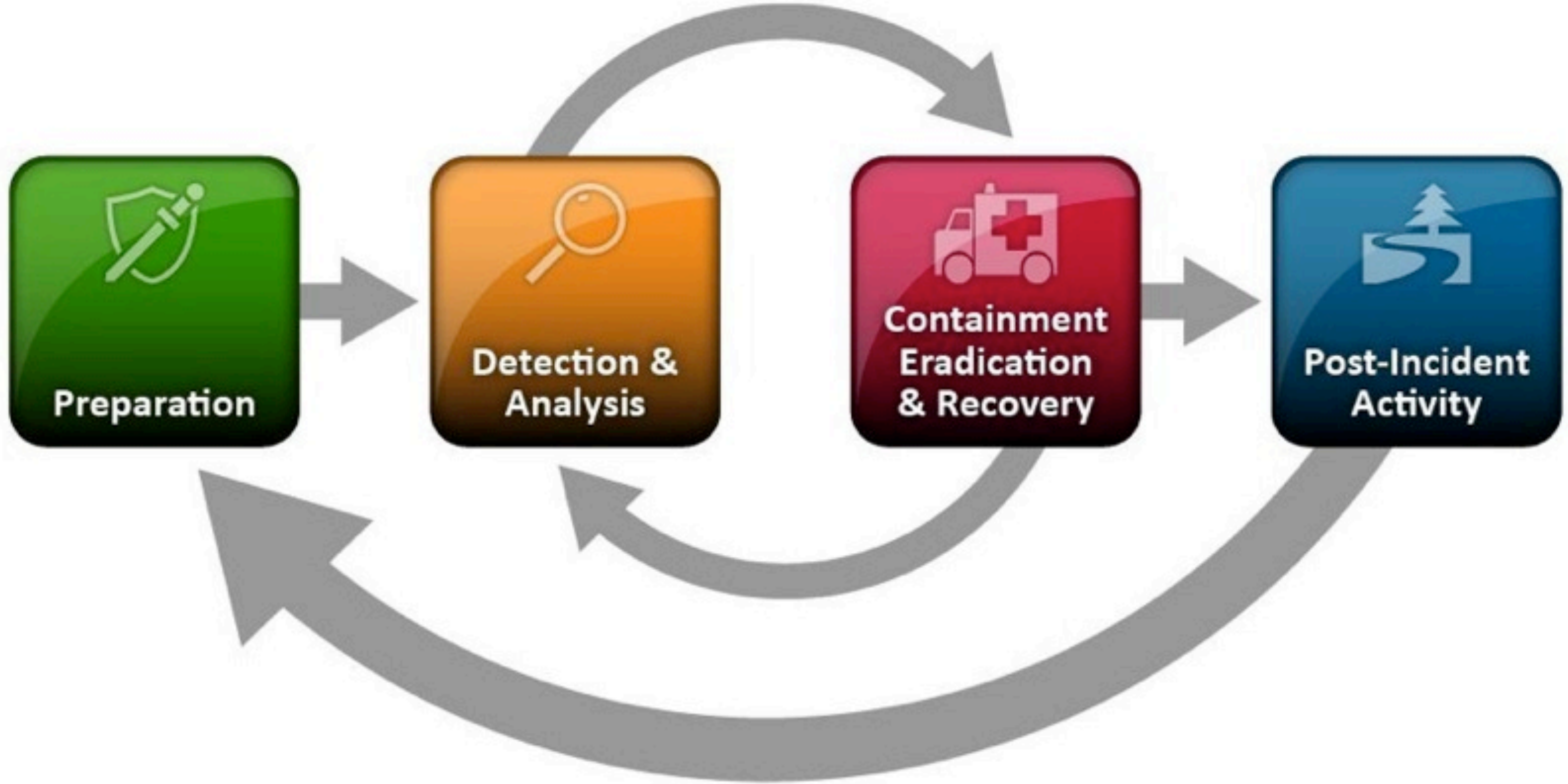
Identifying Attacks

Does it make sense for Healthcare IT to play in SecOps?

Is it a Core Competency?

- Threat intelligence
- 24 by 7 Security Operation Center Management
- Security Incident Response

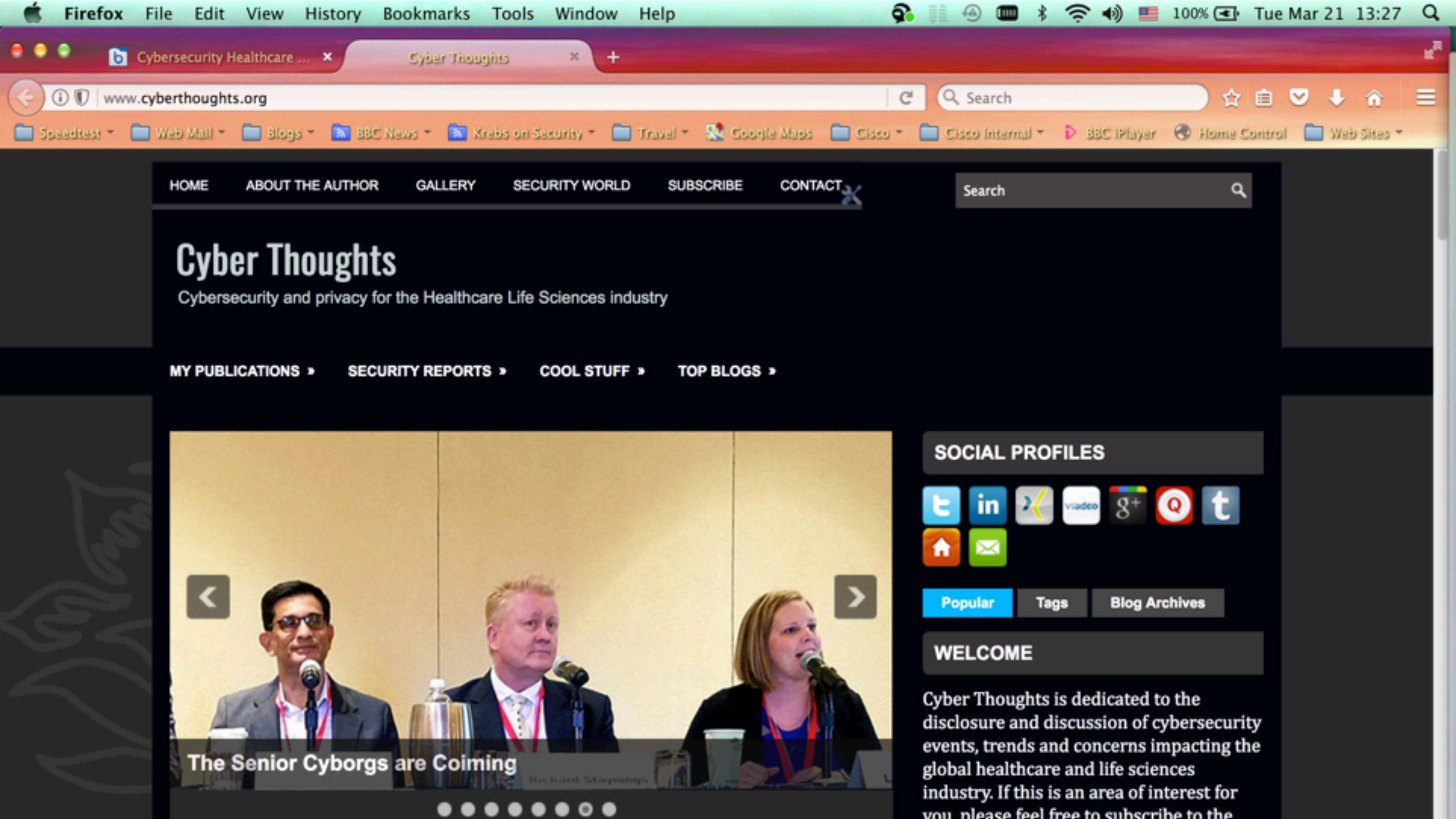
Security Incidence Response Team



Winners and Losers

Mean Time to Detection

Its all about
Blocking Attacks



Cyber Thoughts

Cybersecurity and privacy for the Healthcare Life Sciences industry

WELCOME

Cyber Thoughts is dedicated to the disclosure and discussion of cybersecurity events, trends and concerns impacting the global healthcare and life sciences industry. If this is an area of interest for you, please feel free to subscribe to the

Thank You

@rstaynings

cyberthoughts.org

Richard Staynings
Security Principal and Director ... Security Advisory Services, Cisco
25 March 2015
Security World Conference, Hanoi, V...
intel
cisco
SINCE 2007
SECURITY