

DeepPanda Paging Dr. Smith



Melissa L. Markey, Esq.
Hall, Render, Killian, Heath & Lyman, PC
1512 Larimer Street Suite 300
Denver CO 80202
248-310-4876



A Brief Introduction...

The Threats



- Ransomware
- Business Email Compromise
- Phishing/Whaling/Vishing/Pharming
- Spoofing
- Botnets
- Malware
- Logic Bombs
- Trojans, Worms, Viruses
- Identity Theft
- Cyberstalking
- Fraud, Extortion, etc.
- DDoS attacks
- Social Engineering
- Fileless Attacks
- Medjacking
- Dronejacking

The Players

- FBI/Cyber Action Teams
- Department of Justice
- DoD/DCIS
- Secret Service
- Electronic Crimes Task Force
- US Postal Inspection Service
- Internet Safety Enforcement Team
- AG
- State Police
- Local Police
- Interpol
- FTC
- ATF
- Internet Crime Complaint Center

Is This Real?

- How real is the threat of cybercrime against a healthcare provider?
 - Sometimes the healthcare provider is the target
 - Healthcare providers are a treasure-trove of ID theft information
 - Celebrity patients, public health emergencies... all are fodder for the media
 - Healthcare has all the best data
 - Sometimes the healthcare provider is just collateral damage
 - Lots of computers to be taken over by a botnet
 - Because it's there...

Hospital as a Target

- Israeli Hospital Hacked



Infections Shut Down Services



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 a number of exceptions as follows:

- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics
- Gynaecology
- Immunology
- Cardiothoracic and vascular appointments

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.) You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have **3 days** to submit the payment. After that the price will be **doubled**. Also, if you don't pay in **7 days**, you won't be able to recover your files **forever**.

How Do I Pay?

Send 0.3 BTC to this address: [QR Code](#)

Bitcoin ACCEPTED HERE

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

A Reader's Comment:

- "...It's the computer system that has a virus not the doctor. The patient knows what time their appointment's for and may already have arranged to take time off work. The doctor knows what time they have a clinic....."
- "...a hospital should not be totally dependent on functioning IT systems. It sounds like the decision of an administrator totally divorced from any perception of patients' circumstances..."

It's More Than The EMR...



It's More Than The EMR...

medRAD

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.

Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29

Your files will be lost on
5/15/2017 03:02:31
Time Left
06:19:34:29

Send \$300 worth of bitcoin to this address:
13AM4VWZdhuYgXeQepoHkH5Quy6NgsEb94

Check Payment **Decrypt**

Contact Us

occurred

injection.

system to use.

and contact Services at

Contact Service

via VirtualCare, or refer

to the operations manual or the internet at:
<http://www.radiology.bayer.com>

Patient ID:
DOB:
Weight:

Procedure

Accession:

Fluids

Fluid A:

Fluid B:

Events

Patient Worklist

Status

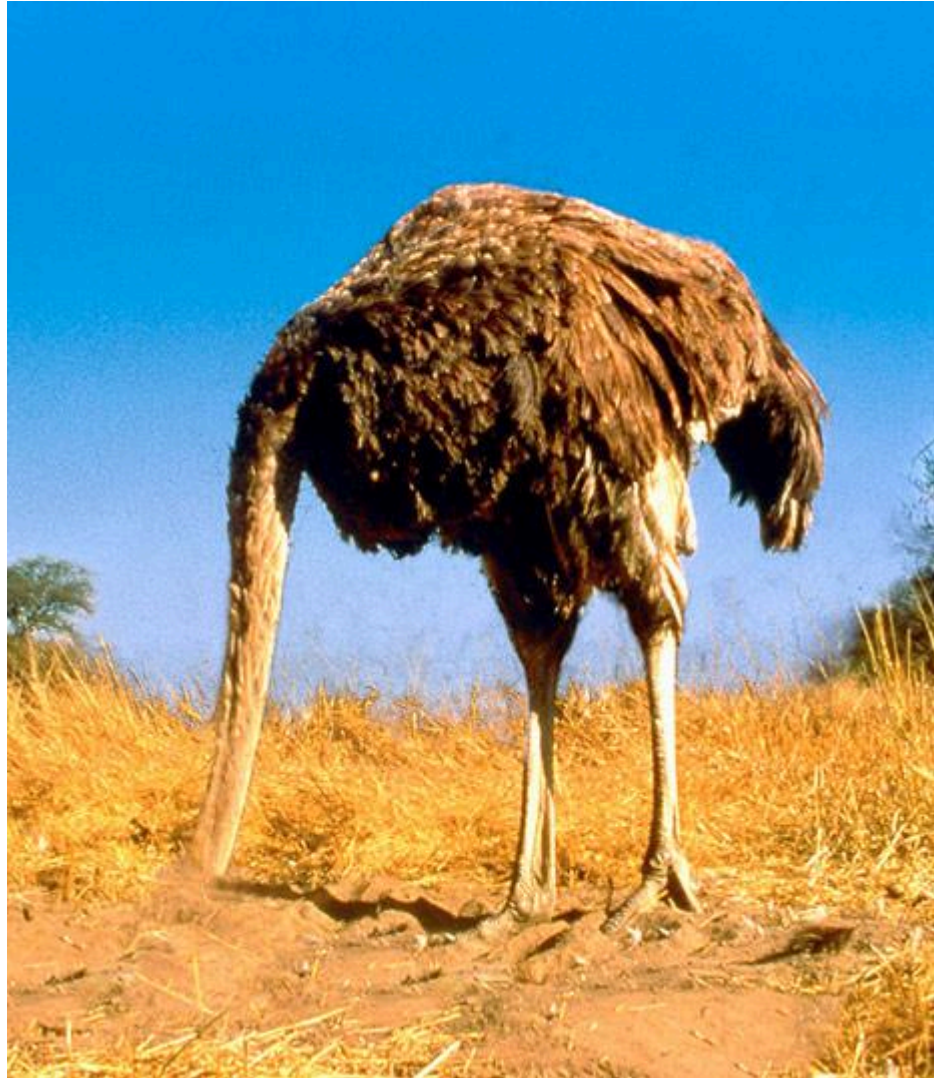
Hospitals as Collateral Damage



Health care as a target: A piece of critical infrastructure



Not an Effective Security Stance





Motivations

Cybercrime: Drivers



■ **Big Business**

- Cyber crime damage costs to hit \$6 trillion annually by 2021
- Global ransomware damages in 2017 estimated to exceed \$5 Billion, 15X higher than 2015's \$325 Million
- Entrepreneurial, with a developing supply chain, sales and distribution structure
 - Dark Web offers everything for sale, from exploits to hacker services to rent-a-botnet

Cybercrime: Drivers

- **The Case of the Stolen IP Trove: Economic Espionage**



Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Huang Zhenyu



Wen Xinyu



Sun Kailiang



Gu Chunhui

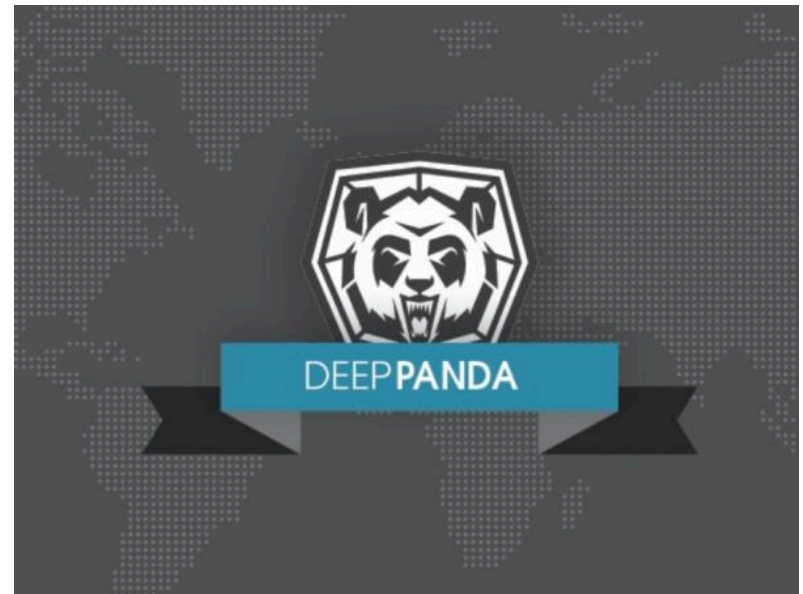


Wang Dong

Cybercrime: Drivers



- **The Case of the Evil Panda: Traditional Espionage**
 - Deep Panda
 - A hacking group variously described as a Chinese People's Liberation Army unit, or aligned with the PLA
 - Also thought to be responsible for Desrubi password-stealing Trojan and the Terracotta VPN, used to launch cyber attacks
 - Set up websites that duplicated legitimate websites, with a few changes...



Cybercrime: Drivers



■ The Case of the Exposed VIP: National Security



Venezuelan Presidency/Zuma Press

Venezuelan President Hugo Chávez addressed a gathering in Caracas this week, after formally kicking off his 2012 re-election campaign Sunday.

■ Reports of Chávez's Illness Cloud Campaign

“Documents from intelligence services of two countries suggest Venezuelan President Hugo Chávez's cancer has spread to his bones and is more aggressive than his government has reported.”

Source: The Wall Street Journal (November 19 – 20, 2011)

Cybercrime: Drivers



The Case of the Unhappy Activist

IN DEPTH

Activism's slippery slope: Anonymous targets children's hospital



MORE LIKE THIS

The processes and tools behind a true APT campaign: Weaponization and delivery



Britain's GCHQ victimized Anonymous supporters with DDoS attack

Info sec industry still struggles to attract women

on DG Answers →

Converting Slideshows into .mp4's

Cybercrime: Drivers

The Case of the (Un)Lucky Bus Passenger



Cybercrime: Drivers



The Case of the Angry Employee



INDEPENDENT

News

Voices

Sports

Culture

Lifestyle

Tech

US election



Disgruntled worker 'tried to cripple UBS in protest over \$32,000 bonus'

An employee at the investment banking giant UBS was so angered by his "meagre" annual bonus that he unleashed a [computer virus](#) designed to cripple the company, a New Jersey jury has been told.

The 63-year-old former computer programmer Roger Duronio denies planting a so-called "logic bomb" that brought down 2,000 computers across UBS's stockbroking unit Paine Webber and cost the company \$3.1m to repair. About 17,000 UBS brokers across the US were unable to trade shares for more than a day, costing the company even more in lost [business](#).

In court yesterday, Mr Duronio's lawyers pointed to a string of holes in IT [security](#) at UBS, and suggested that senior executives were aware the security lapses had opened "doors to hackers". Mr Duronio claims that someone else planted the virus.

Cybercrime: Drivers

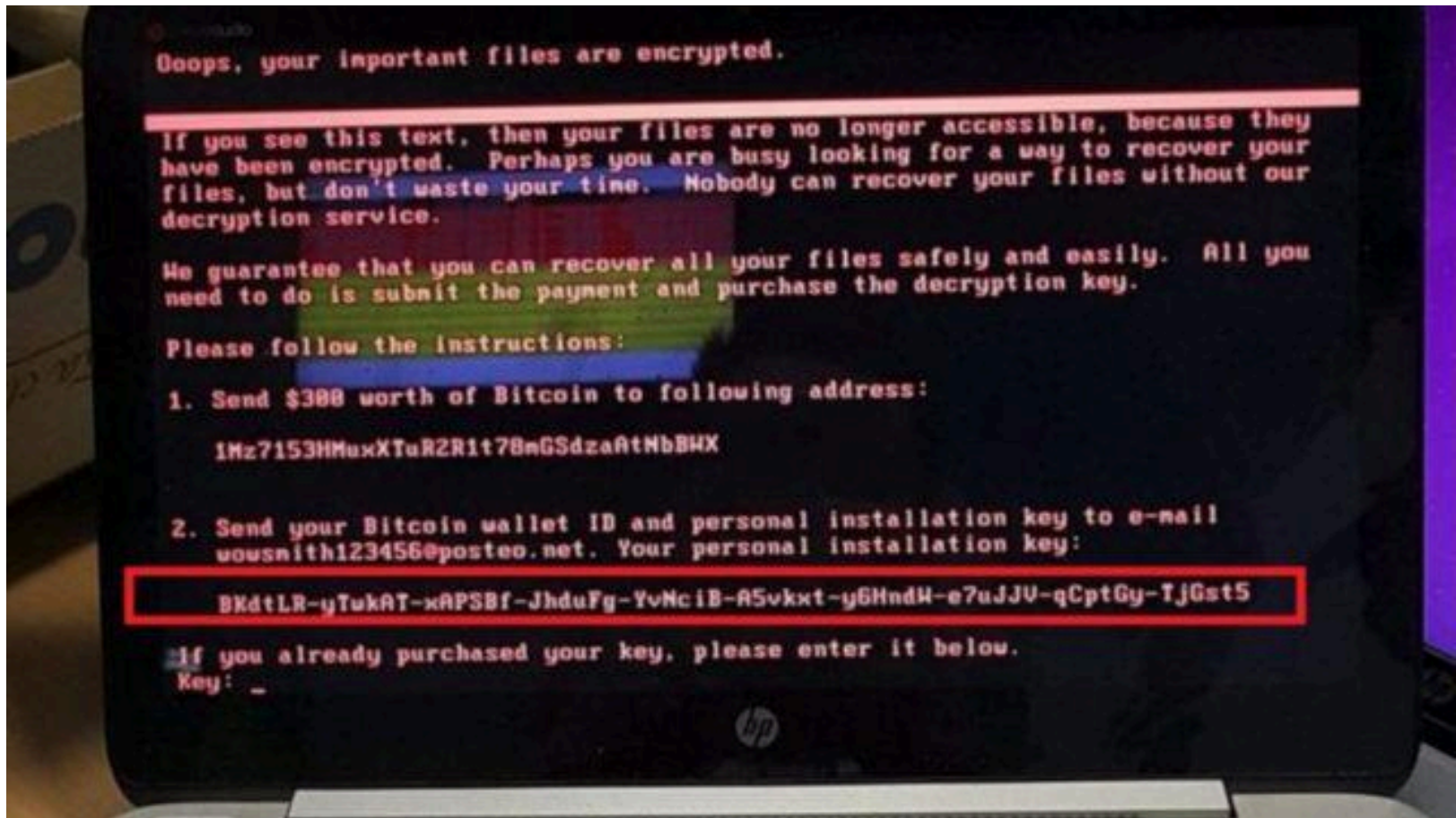


The Case of the Leaking PACS



Cybercrime: Drivers

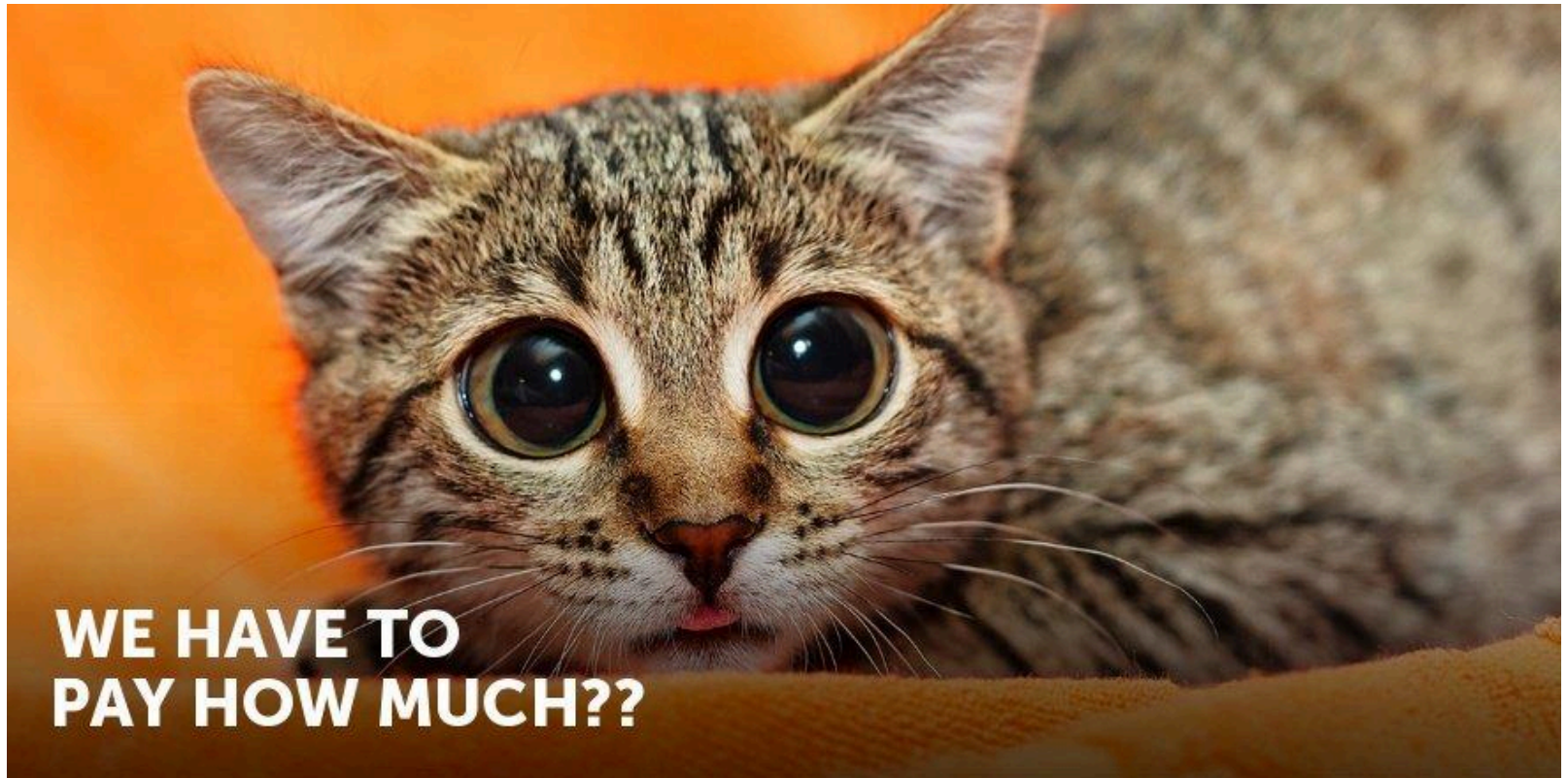
The Case of the Kidnapped Computer



Cybercrime: Drivers



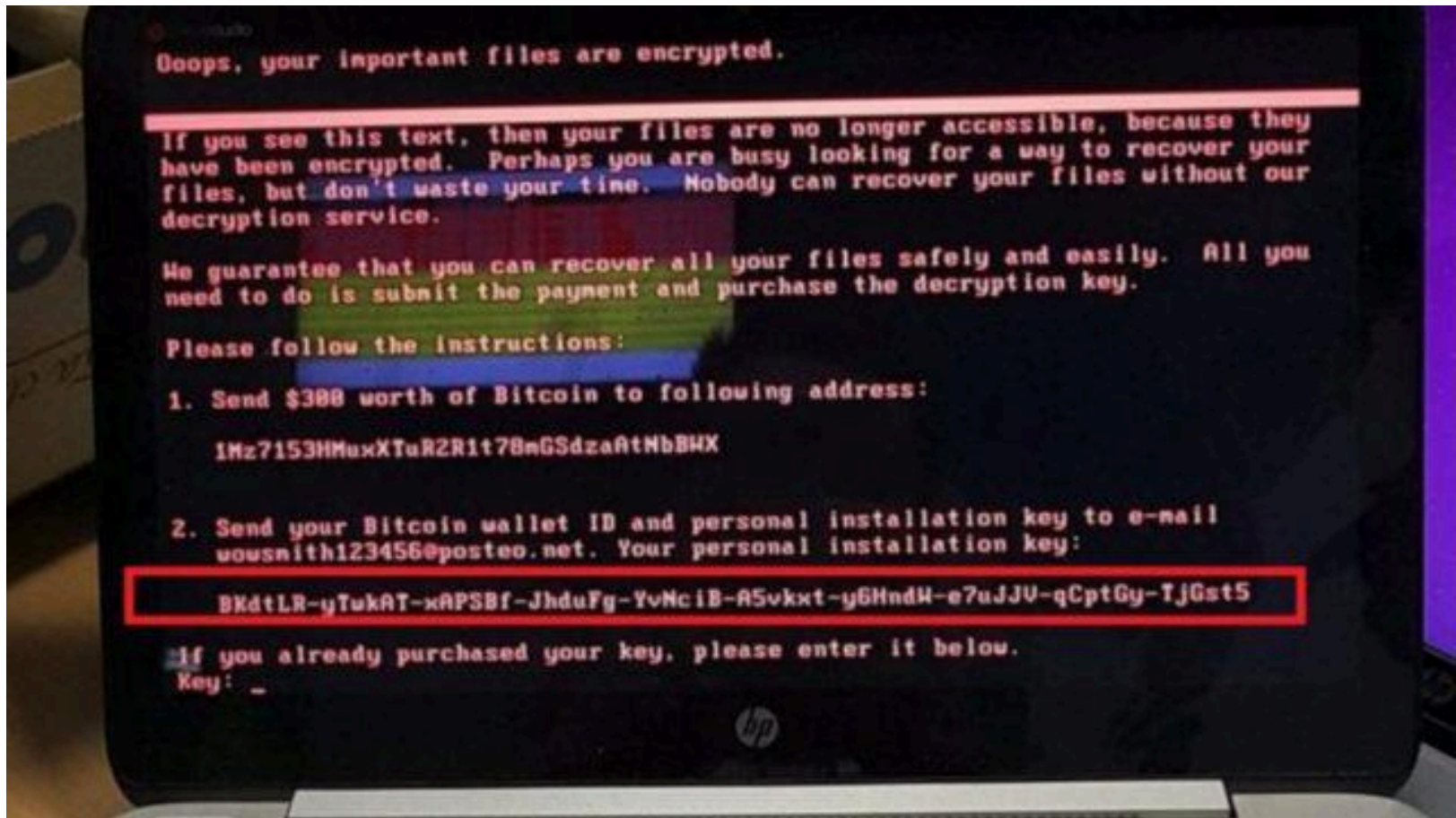
The Case of the Kidnapped Computer



**WE HAVE TO
PAY HOW MUCH??**

Cybercrime: Drivers

The Case of the Kidnapped Computer



Cybercrime: Drivers



The Case of the Short Seller





cyber security

Anatomy of an Attack

Reconnaissance



Weaponization



Delivery/Infiltration



Exploitation

```
root@Chocolate-Crispy:~/DET# python det.py -c ./config.json -p icmp -L
[2016-03-08.16:07:27] CTRL+C to kill DET
[2016-03-08.16:07:27] [icmp] Listening for ICMP packets..
[2016-03-08.16:07:28] [icmp] Received ICMP packet from: 10.0.1.10 to 192.168.0.1
[2016-03-08.16:07:32] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:32] Received 67 bytes
[2016-03-08.16:07:32] Register packet for file /etc/passwd with checksum a7b8bda
05119f81ea199100df01bbfcb
[2016-03-08.16:07:35] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:35] Received 840 bytes
[2016-03-08.16:07:36] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:36] Received 994 bytes
[2016-03-08.16:07:37] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:37] Received 872 bytes
[2016-03-08.16:07:40] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:40] Received 820 bytes
[2016-03-08.16:07:43] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:43] Received 914 bytes
```

A close-up, high-angle view of a computer keyboard. The keys are primarily blue and white, with some keys having yellow or orange characters. A prominent red key is in the foreground, featuring the words "cyber security" in white, lowercase letters. The text "Who is Worse...." is overlaid in black, bold font across the red key and the surrounding blue keys. The background is a soft, out-of-focus blue and white, suggesting a digital or technological environment.

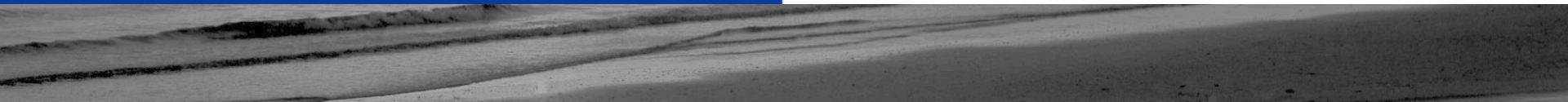
Who is Worse....

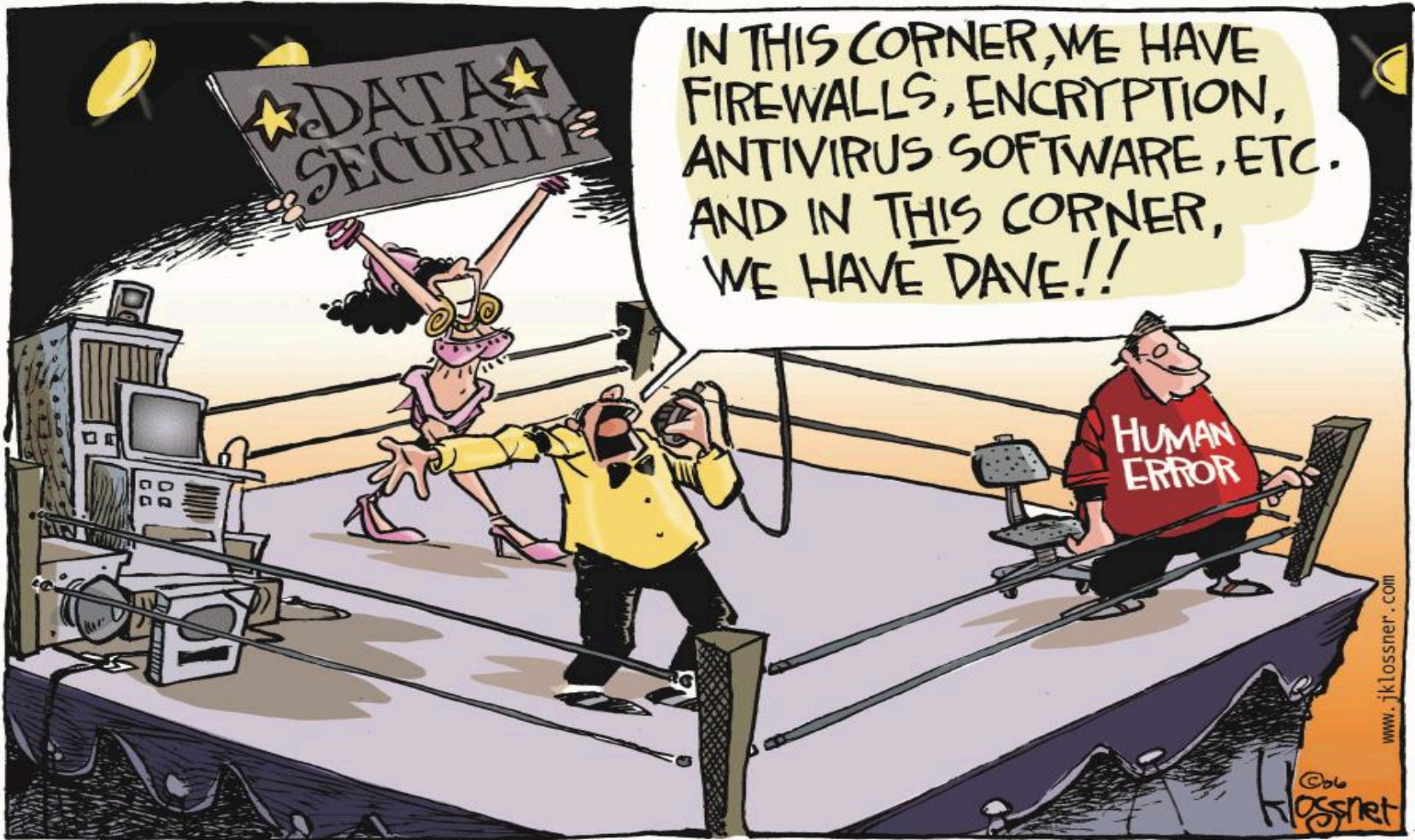
cyber
security

INTERNAL

V

EXTERNAL





www.jklossner.com

copyright 2006 john klossner, www.jklossner.com

The Weakest Link...

- **"A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted" – Kevin Mitnick**

This is the Gmail Phishing Scam website. Notice the URL or Web Address in the Address Bar of the web browser is incorrect.



Welcome to Gmail

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Fast search

Use Google search to **find the exact message** you want, no matter when it was sent or received.

Lots of space

Over 2757.272164 megabytes (and counting) of free storage so you'll never need to delete another message.



Chat right inside Gmail

It's just one click to chat with the people you already email. You can even save your chats in your Gmail account. [Learn more](#)



Mobile access

Read Gmail on your mobile phone by pointing your phone's web browser to <http://gmail.com/app>. [Learn more](#)

Get Gmail for your business, school, or organization with [Google Apps](#).

Sign in to Gmail with your
Google Account

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)







[About Gmail](#) [New features!](#)


©2007 Google - [Privacy Policy](#) - [Program Policies](#) - [Terms of Use](#)

Hosted by [T35 Free Web Hosting](#). [Free Domains](#) - [One Way Backlink](#) - [Hosting](#) - [Paid Proxy](#)


Business Email Compromise









 New ▾ |  ▾ |  ▾ |  |  ▾ |  | Reply Forward


 **Request from Supplier**
Subject: New Account Number

To: Company C Accounts Payable


 *High Importance*

Our account number and account information has been changed. Please update your records for future invoice payments to our new Account information below...

 New ▾ |  ▾ |  ▾ |  |  ▾ |  | Reply Forward

 **Request from CEO**
Subject: Immediate Wire Transfer

To: Chief Financial Officer

 *High Importance*

Please process a wire transfer payment in the amount of \$250,000 and code to "admin expenses" by COB today. Wiring instructions below...

Social Engineering




Microsoft Edge

Microsoft Edge

The server meetatsite.com is asking for your user name and password. The server reports that it is from II Cyber Security Warning II The Computer Is Locked To Stop Your Illegal Activity. Please Call +1-844-307-1766 Immediately. All Suspicious Files From Your Computer Were Transmitted To A Special Server And Shall Be Used As Evidences. You must call the support at +1-844-307-1766 To Get Your Computer Unlocked II Your PC May Be Infected By Malware, Thus You Are Voilating The Law Of Neglectful Use of Personal Computer. To Unlock The Computer Please Call Support At +1-844-307-1766.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.



User name

Password



Incident Response

■ ■ ■ Before the Incident

Establish Cybersecurity as a Core Strategic Objective with Board-Level Attention



Before the Incident



- The First Thing You Do Is...Conduct A Risk Assessment!
 - To Protect It, You Have To Know:
 - What You Have (the Asset)
 - Where It Is (the Environment)
 - What Is At Risk (the Vulnerability)
 - What Might Go After It (the Threat)
 - How Likely That Will Happen (the Risk)
 - What You Can Do About It (the Plan)

What Needs to be Protected?

- Protected Health Information – HIPAA
- Consumer Information – FTC
- Payment Card Information – PCI DSS
- Other Sensitive Information – State Law
 - Drivers License
 - Email Addresses
 - Employment Information
- Corporate Information
- Contractually Protected Information

Before the Incident

- The Next Thing You Do Is...Develop an Incident Response Plan
 - The best incident response starts well before the incident!
 - A security incident is a high-stress event. Planning helps.
 - The question is not whether there will be a security incident and possible data breach; the question is when.
 - Team members need to know their role.
 - Develop policies so users know what to do.
 - Engage Senior Management
 - Develop a First-Responder Toolkit

Before the Incident

- Pre-incident activities include:
 - Encryption!
 - Strong (but reasonable) passwords
 - Obtain/configure software that watches the system and tracks access
 - Risk Assessments – and not just one
 - Have a workable data back-up and test it (DR/COOP)
 - Audit trails – application level and system level
 - Intrusion Detection/Prevention
 - Drills and exercises
 - Align all data security policies and procedures
 - HIPAA
 - PCI DSS

Before the Incident



- Identify and Document Computer Assets
 - Hardware
 - Software
 - Storage
 - Mobile Devices
- Save only what must be saved; delete when you can
- Test back-ups (System and Data)
- Policies and Procedures
 - Security
 - Confidentiality
 - Breach and Security Incidents

Cybersecurity Information

Sharing Act

- Directed the creation of a “single, voluntary, national health-specific cybersecurity framework...” between DHS, NIST and industry stakeholders
 - Common set of voluntary, consensus-based and industry-led standards, security practices, guidelines, methodologies, procedures, and processes as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations
 - Support voluntary adoption and implementation efforts to improve safeguards
 - Consistent with HIPAA security and privacy regulations
 - Updated on a regular basis
- Provides protection to support information sharing
- Liability protection for monitoring and defensive measures on your own system

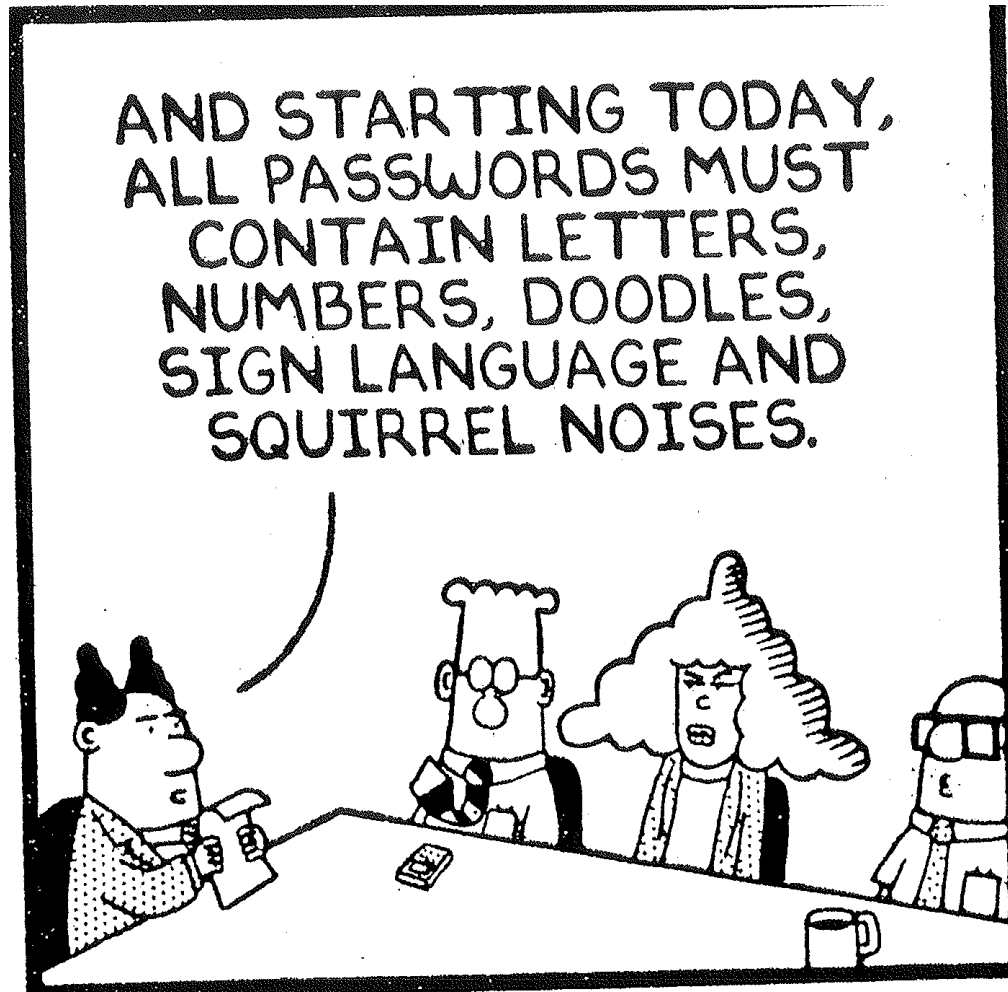
Information Sharing under CISA

- Consider whether to participate in information sharing of Cyberthreat Indicators and defensive measures
- Personal information must be scrubbed and only relevant data submitted
- Consider participation in National Healthcare Information Sharing and Analysis Center (NH-ISAC)

Incident Response

- Enforce the rules
 - Sharing passwords
 - Proper use and disclosure of PHI
 - What information is maintained where
 - Use of personal email...
- Publicize that you enforce the rules
 - Even if the miscreant is an important doctor
 - Even if it is the CEO

Before the Incident



Incident Response

- Evaluate the scope of the incident.
 - What was exposed?
 - Who is impacted?
 - Evaluate both users and potential victims
 - Where did the incident reach? What was touched?
 - Where and how was access gained?
 - Where was the actor?
 - When did the incident start?
 - How was the incident/attack accomplished?

Incident Response

- Activate Incident Response
 - Who is responsible
 - For making decisions
 - For technical activities
 - For communications
 - What needs to be done
 - Isolate the attack!
 - Forensic investigation?
 - Correct corrupted data?
 - When must tasks be completed?
 - Notice to law enforcement
 - Notice to affected individuals?

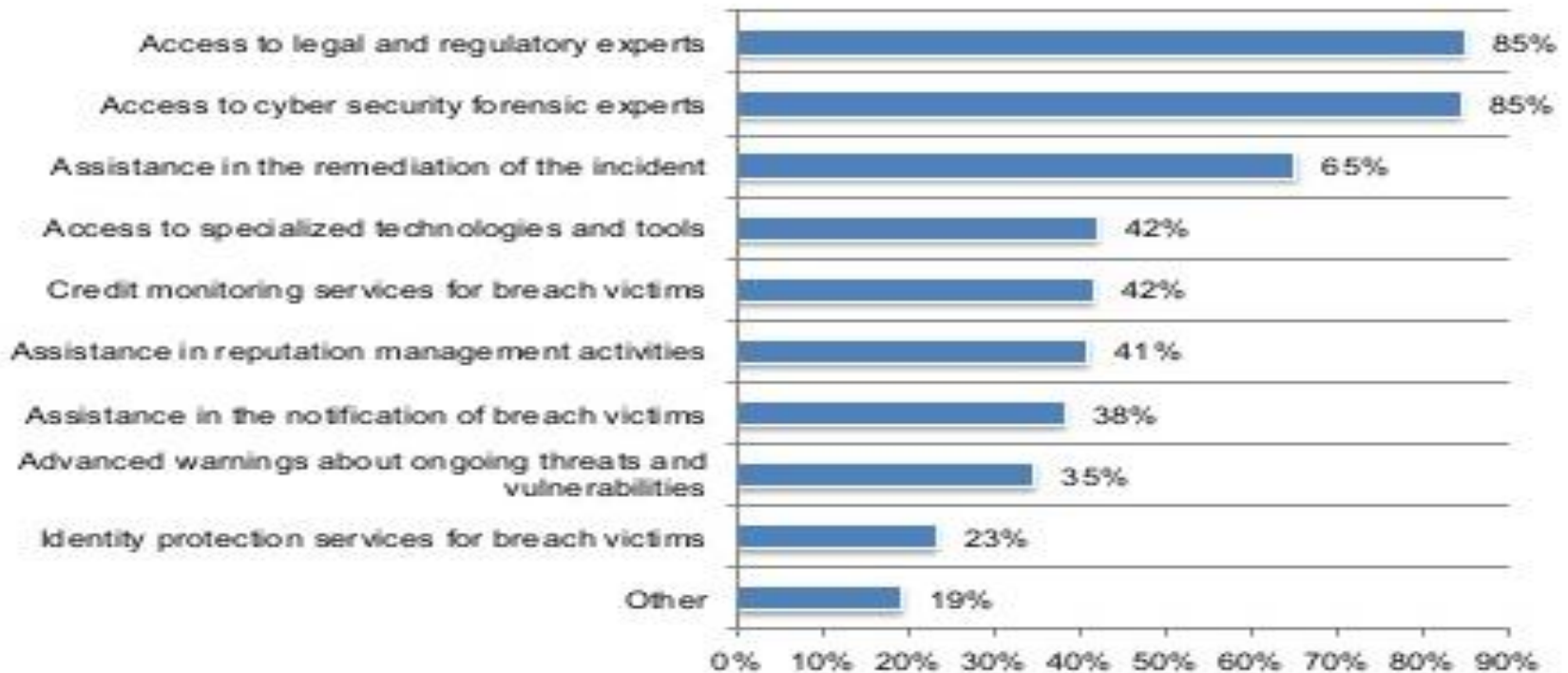


Cyber-Insurance



Figure 17. Other services provided by the cyber insurer

More than one response permitted



Incident Response

- Conduct the Investigation
 - Stop the bleeding
 - Isolate the computer
 - Wipe mobile devices
 - Activate keystroke monitoring
 - Suspend automatic processes that could destroy evidence
 - Preserve relevant logs, audit trails



Incident Response



- Conduct the Investigation
 - Preferably NOT an internal data investigation
 - Evaluate data reliability
 - As necessary, transfer to back-up machines/data
 - Preserve audit trails, metadata, etc.
 - Forensic copy of email, hard drive, portable devices
 - Write-block device



Forensic Computer Experts

- If you anticipate litigation
 - Need an expert who can testify
 - Independent, neutral third party usually more persuasive
 - Attorney-client privilege and work product protection is important!
- Address issues in agreement
 - Best to have an arrangement in place before it is needed
 - Address authority, roles, expectations, costs

Incident Response



- Prepare for Notification: HIPAA HITECH and State law; SEC and other requirements
 - Affected Individuals
 - HHS
 - Law Enforcement
 - Attorney General/Cybercrime Squads
 - Insurer?
 - Credit Monitoring Services?
 - Credit card companies?



Incident Response

- Prepare for Notification

- May be subject to multiple laws
- Some laws may be inconsistent
- Consider contractual obligations

- When/How/Who

- What if notification arguably not required?



Incident/Breach Response



- Set up a dedicated call-in center
 - Be prepared!
 - Be honest
 - Be open
 - Have sufficient lines
 - Have trained, informed, compassionate staff



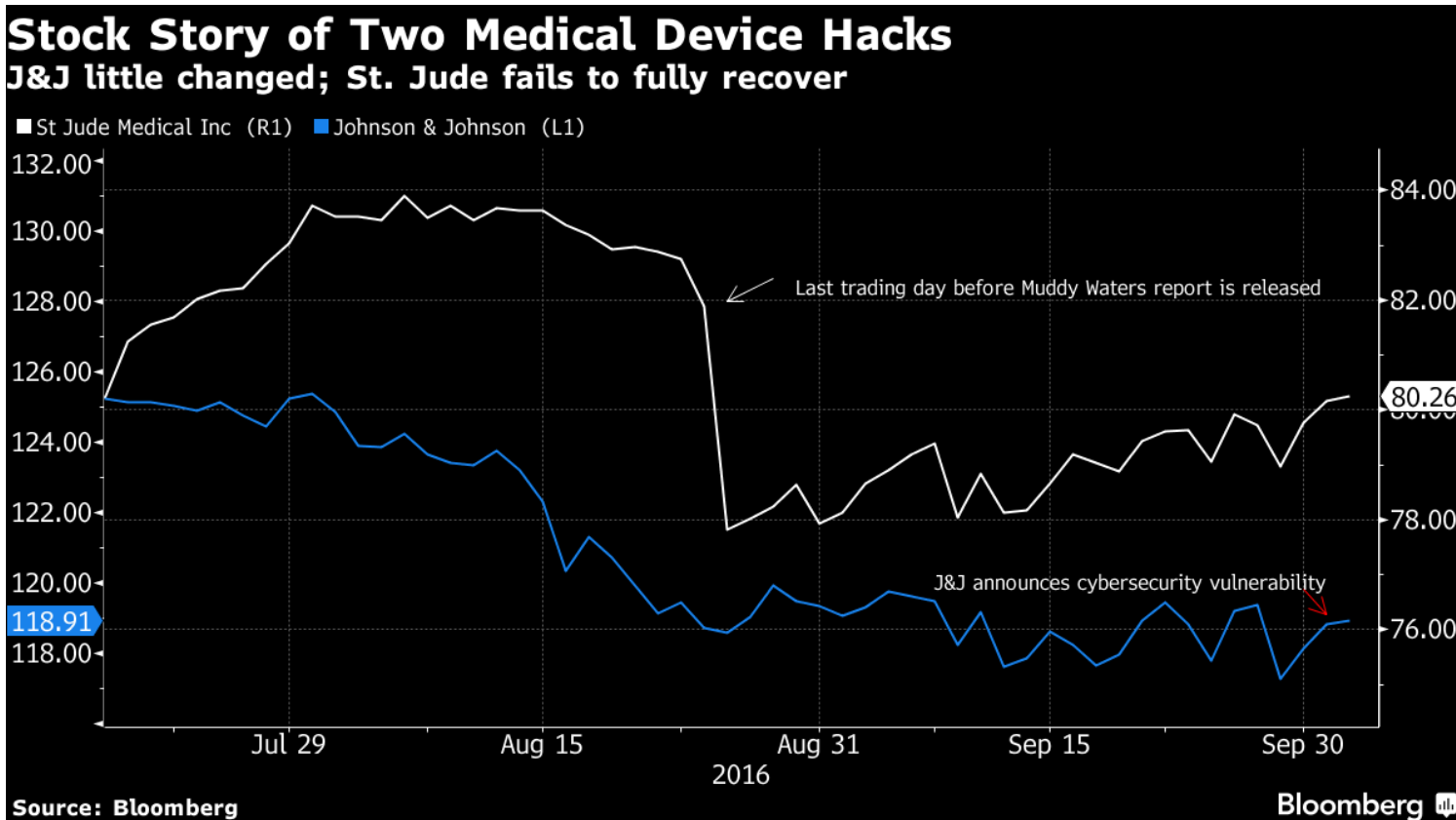
Incident Response

- Get control over the information
 - Work with law enforcement to avoid compromising the investigation
 - Open, clear, effective and timely!
 - To your Board
 - To affected individuals
 - To employees, stakeholders
 - One person should talk to the media
 - Provide accurate, consistent information
 - Publicize the call-in number

J & J Ping Insulin Pump Hack



A Tale of 2 Stories...



Incident Response

- Prepare for possible probable litigation
 - By affected individuals
 - Regulatory actions
 - If DSS were violated
 - Civil case against hacker
 - Criminal case against hacker





Incident Response

- Post-Investigation Actions
 - Evaluate the Incident
 - Was the risk that was exploited covered in the initial risk assessment?
 - What changed to make this vulnerability higher risk than anticipated?
 - What policies/procedures worked, and what didn't, to protect against this incident?
 - Evaluate the Response
 - After Action Reports are critical
 - Invite LEO to participate



Incident Response

- Post-Investigation Actions
 - Prevent Future Recurrence
 - Additional Training
 - Modify or Add Policies/Procedures
 - Add technical safeguards
 - Audit
 - Terminate/Modify Vendor Agreements

Incident Response



- Do the Right Thing
 - It may not be cheap
 - It may not be safe
 - But it respects the trust that patients place in healthcare providers

Working with Law Enforcement



Access to computer assets:

HIPAA

- Victim may disclose PHI to law enforcement
 - 'Disclosure by victim' talks about workforce members who are victims
- Covered entity may disclosure PHI:
 - as required by law; or
 - in compliance with a court order, warrant, subpoena, summons, or an administrative request (including a civil or authorized investigative demand)
- Covered entity may disclose PHI for a crime that occurred on the premises
 - But, did a hack that originated in Estonia "occur on the premises"?

Issues to Consider

- Exposure of Confidential Information
 - HIPAA
 - Provider-Patient Privilege
 - Part 2 Drug and Alcohol Abuse Records
 - State Law Confidentiality
 - Mental Health
 - STDs
 - Other
- Other Uses of “Plain View” Information
- Work with LEO counsel to resolve concerns

Issues to Consider

- Operational Impact
 - Access to live environment?
 - Access to imaged environment?
 - Inventory all items accessed/removed
 - At the file level
 - Chain of Custody
 - Access Records
 - Protocols on Access, Copying, Destruction of Records
- Any Ongoing Obligation
 - Publicity?



Laws! I Need Laws!



Some Major Computer Laws

- Computer Fraud and Abuse Act
 - Prohibits access to computers without or in excess of authorization; transmission of harmful code
 - Multiple different infractions; multiple different penalties
 - Protects computers engaged in interstate or foreign commerce; federal computers; financial computers; medical computers
 - Criminal and Civil penalties
 - Secret Service has jurisdiction

Some Computer Laws

- Electronic Communications Privacy Act
 - Protects wire, oral, and electronic communications while being made, in transit, and in computer storage
 - Title I: Wiretap Act – prohibits intentional or attempted interception, use or disclosure of any wire, oral or electronic communication.
 - Exceptions for ISPs and operators while providing service, and permitted surveillance
 - Title II: Stored Communications Act – protects files stored by ISPs and records of ISPs
 - Title III: Pen Register and Trap and Trace Act

Still More Computer Laws

- CAN-SPAM Act
 - Prohibits false or misleading header information
- Gramm-Leach-Bliley Act, Title V
- Sarbanes-Oxley Act §404 (SOX)
- HSPD 7
- Homeland Security Act of 2002
- USA Patriot Act
- Consumer Protection Acts
- Children's Online Privacy Protection Act
- Fair Credit Reporting Act

Still More Computer Laws

- Federal Trade Commission Act Section 5
- Electronic Funds Transfer Act (Reg E)
- Free and Secure Trade Program (FAST) (voluntary)
- Customs-Trade Partnership Against Terrorism (C-TPAT) (voluntary)
- Fair and Accurate Credit Transaction Act (FACTA), Red Flags Rules
- 21 CFR Part 11
- Federal Information Security Management Act (FISMA)

Other Legal Resources

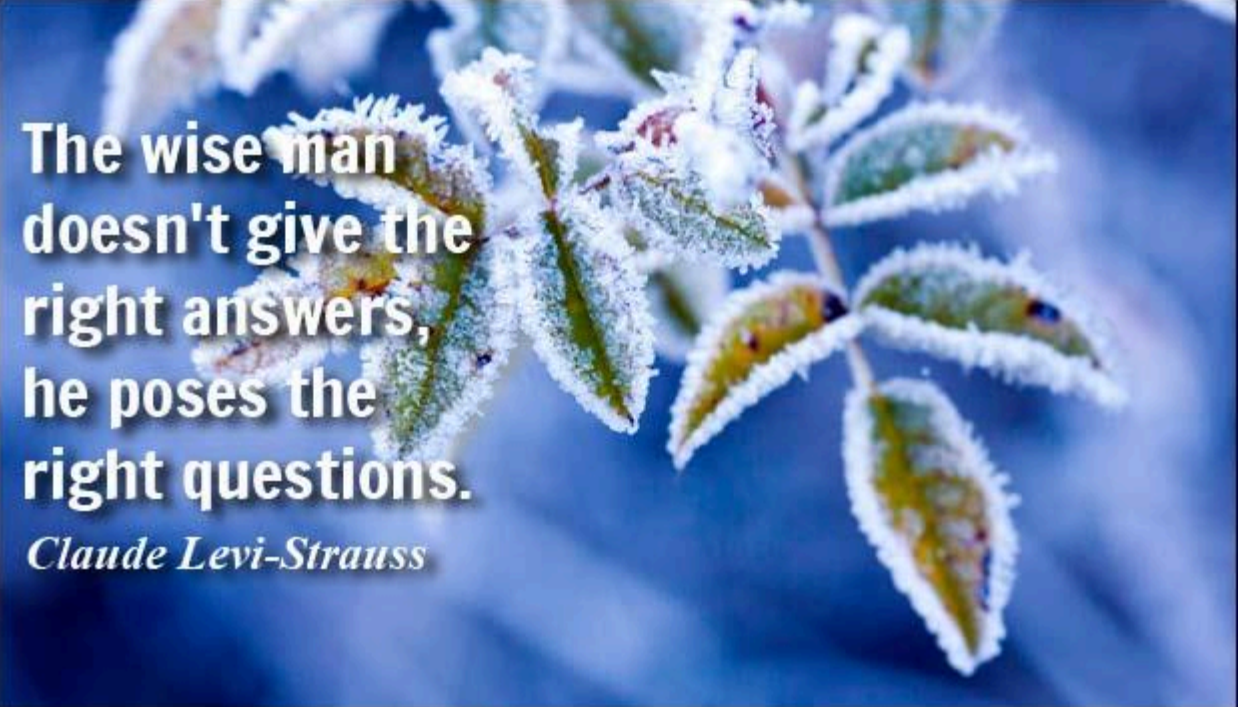
- State laws
 - Computer-specific
 - Identity Theft Acts
 - Breach Notification Laws
 - Consumer Protection Laws

- PCI DSS

- Some Interesting Possibilities
 - Trespass
 - Fraud
 - Economic Espionage

Cybercrime: Harmonizing laws

- European Convention on Cybercrimes
 - Treaty that provides a common international framework for dealing with cybercrimes
 - Adopted in November 2001 by the EU Committee of Ministers of the Council of Europe
 - Covers topics ranging from illegal access to misuse of devices to child pornography
 - 46 countries have signed the treaty
 - But only 24 have ratified it
 - In force in the US as of Jan. 1, 2007
 - ** China and Russia have not signed it

A close-up photograph of green leaves covered in a layer of white frost. The background is a soft, out-of-focus blue.

**The wise man
doesn't give the
right answers,
he poses the
right questions.**

Claude Levi-Strauss