HIMSS Cybersecurity Community Sponsor

FairWarning helps healthcare organizations establish a culture of security, privacy, and compliance to expand trust with their patients. Our patented cloud-based platform simplifies the full lifecycle of privacy and insider security incident management and helps those in the highly regulated healthcare industry more easily detect, investigate, mitigate, and remediate improper user access or behavior. FairWarning helps satisfy key regulatory requirements across multiple industries and localities, including HIPAA, GDPR, PCI, and SOX.

HIMSS
transforming health through information and technology™

The Converging Paths of Cyber Risks and Patient Safety

Richard Staynings
HIMSS Cybersecurity Committee

HIMSS
transforming health through information and technology™

HEALTHCARE CYBERSECURITY COMMUNITY

Agenda

1. What is Patient Safety?
2. What is Cyber Risk?
3. Why is Cyber Risk So important in Healthcare?
4. How to Assess and Manage Risk

What does Patient Safety mean to CEOs?

Healthcare CEOs know all about patient safety – at least that's what they'll tell you. Joint Commission and others have been all over the subject for years. Ask them what patient safety really means and most will probably start talking about how health care organizations protect their patients from errors, injuries, accidents, and infections. It's a big issue. As many as 440,000 people die every year from preventable errors in hospitals alone.

HIMSS
transforming health through information and technology

Patient Safety

Patient safety means more than protecting patients from medical malpractice and hospital-borne infections.

If medicine is about keeping the whole body healthy then patient safety should follow a similar approach.

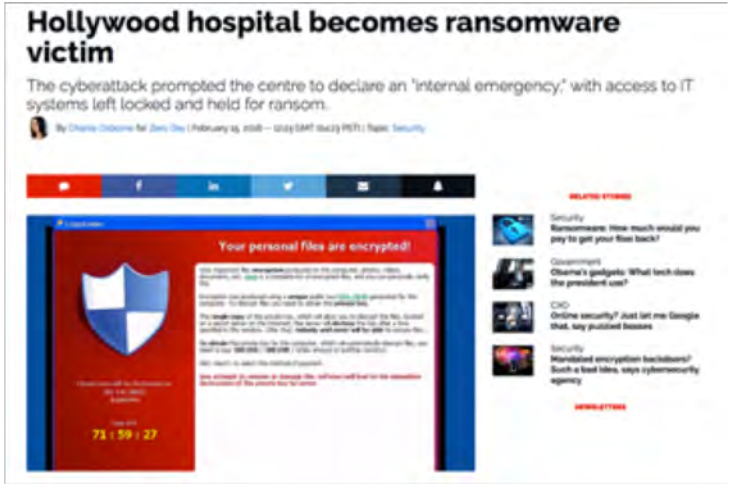
And that includes…..

Healthcare is Under Attack

It has become a major target for theft of PHI, ransomware and DDoS

Healthcare is also poorly protected compared to other industry sectors and therefore is considered an easy target with rich pickings

Hospitals have been disproportionally hit with ransomware since 2014



WannaCry Global Attack

HIMSS
transforming health through information and technology

Not Petya / Nyetya cost $1.2 Billion

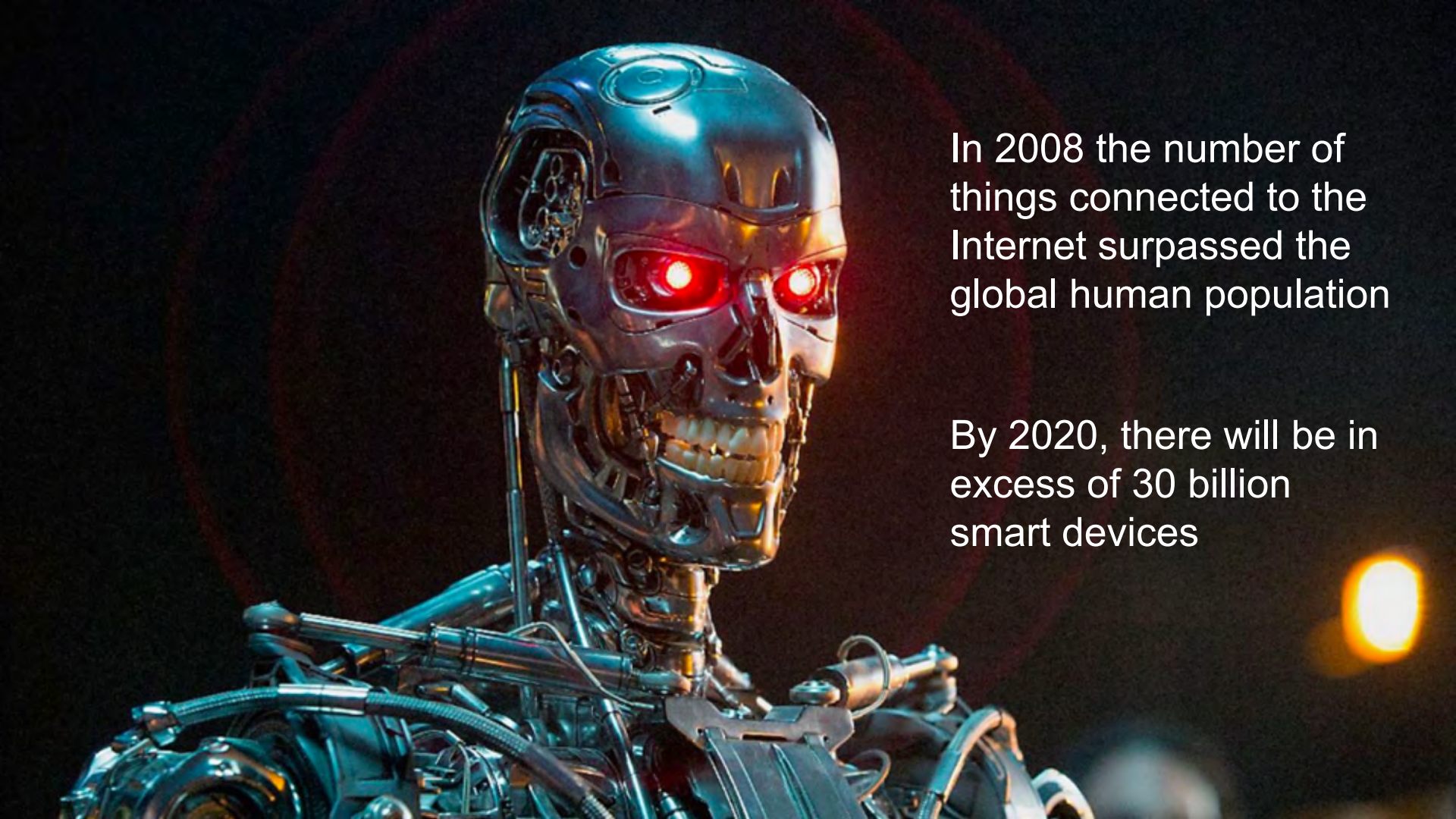
	Lost Revenue Only
FedEx TNT	$300,000,000
Nuance Communications	$ 15,400,000
Mondelez International	$150,000,000
Reckitt Benckiser	$129,000,000
Maersk	$275,000,000
Merck & Co. Pharmaceuticals	$135,000,000

NonPetya forced Maersk to reinstall 4,000 servers, 45,000 PCs & 2,500 applications

Security and Risk Management Due Diligence

DDoS being used against critical infrastructure

Rising use of IoT BotNets – CCTV Cameras



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

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”**


Why is Healthcare Under Attack?

Lack of Understanding of Cyber Risks

20 years of under-investment in Healthcare Security

….and healthcare is an increasingly value-laden target

Healthcare uses a LOT of Vendors


Third-Party Due Diligence

Third Party Vendor Risk Management

- Rank your vendors
- Perform Risk Analysis to SP800-30 standards
- On all of them over time
- But …with 3,000+ vendors, partners, suppliers and Business Associates how can you possibly assess and report risk for each of them?
- Good News: New Are Tools Coming

HIMSS
transforming health through information and technology

Target Breach caused by insecure HVAC Vendor


INTERNET OF THINGS

Hospital IoT

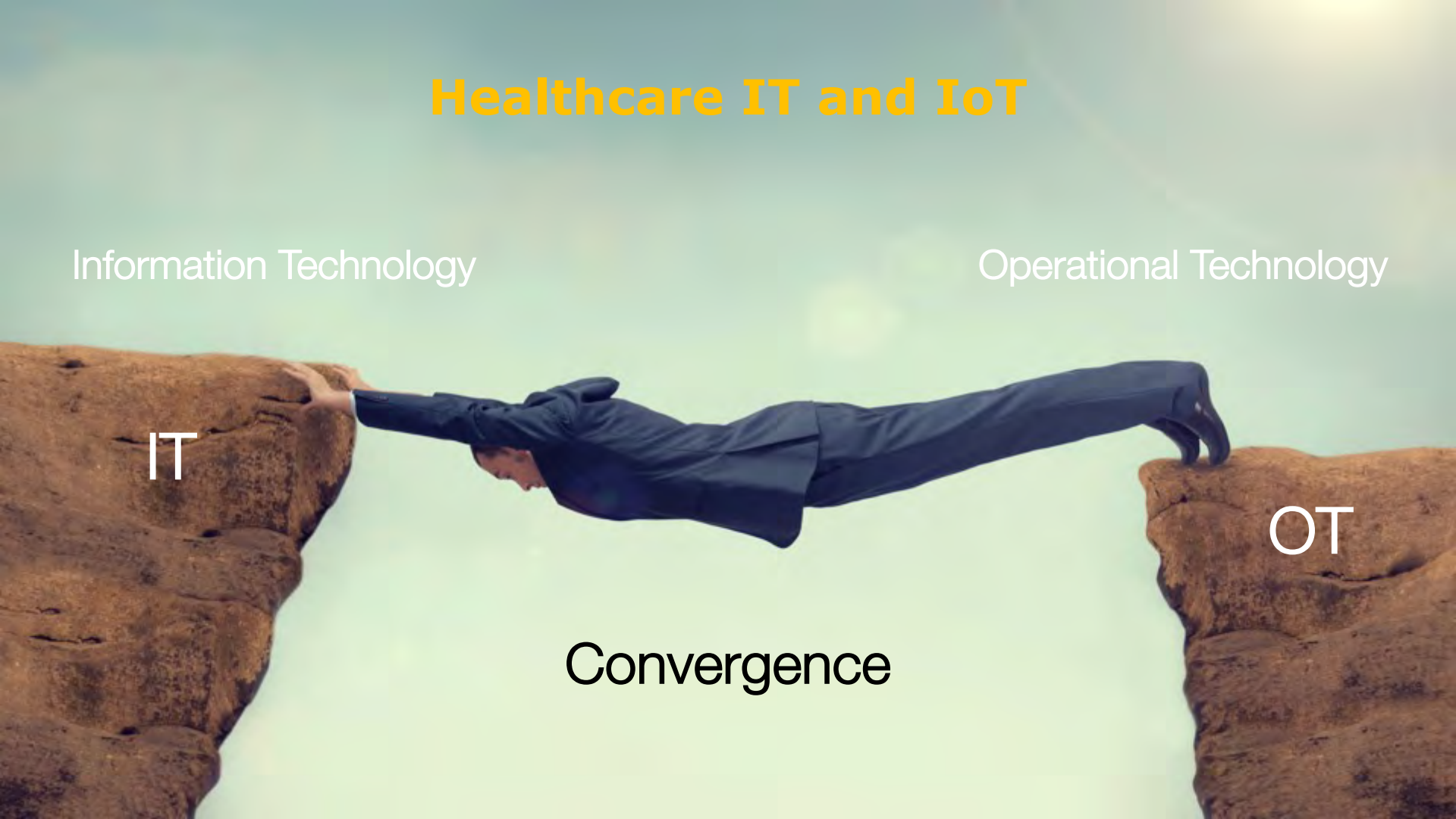
Hospital Building Management Systems

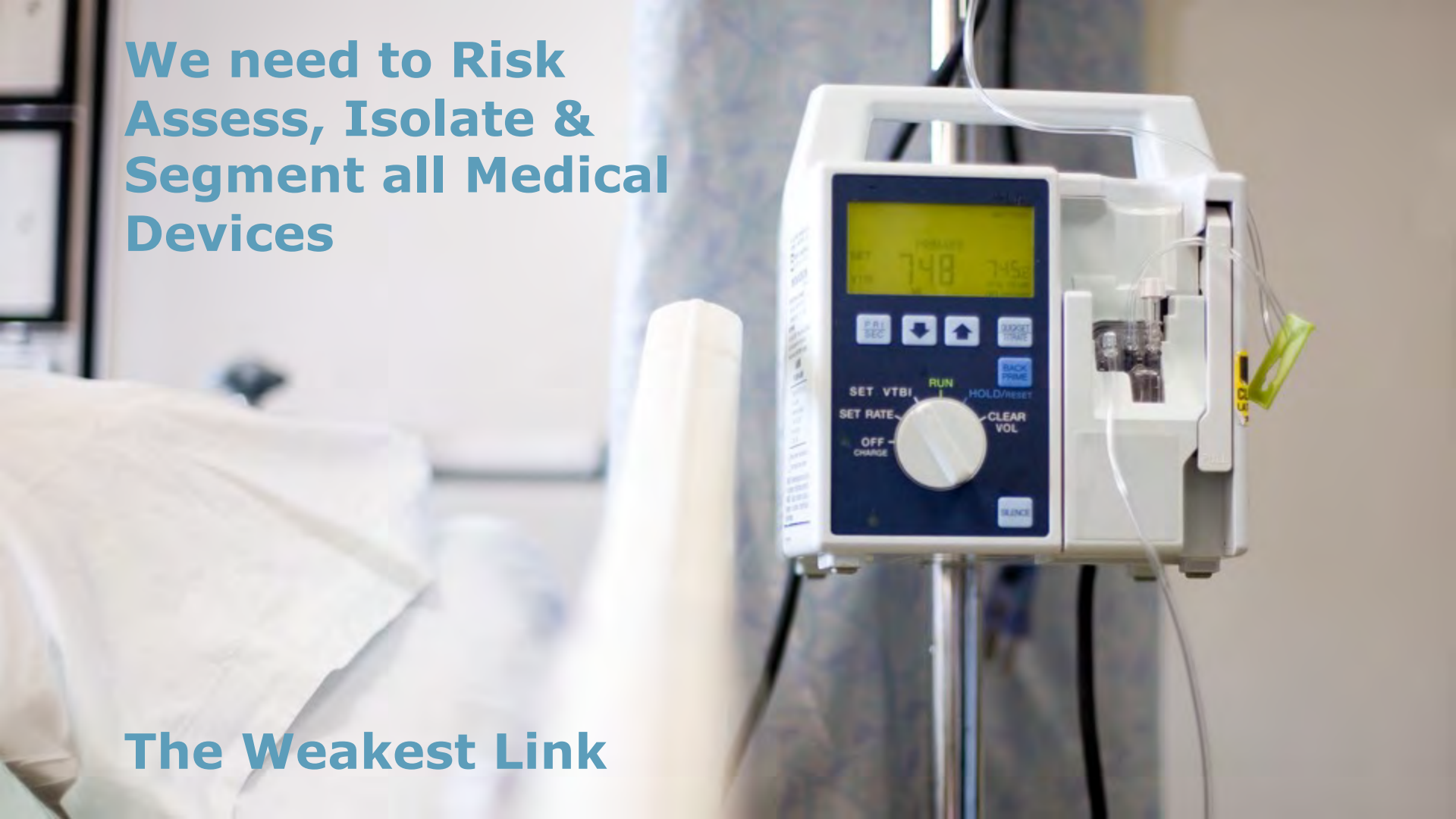

Massive Growth in Medical Devices

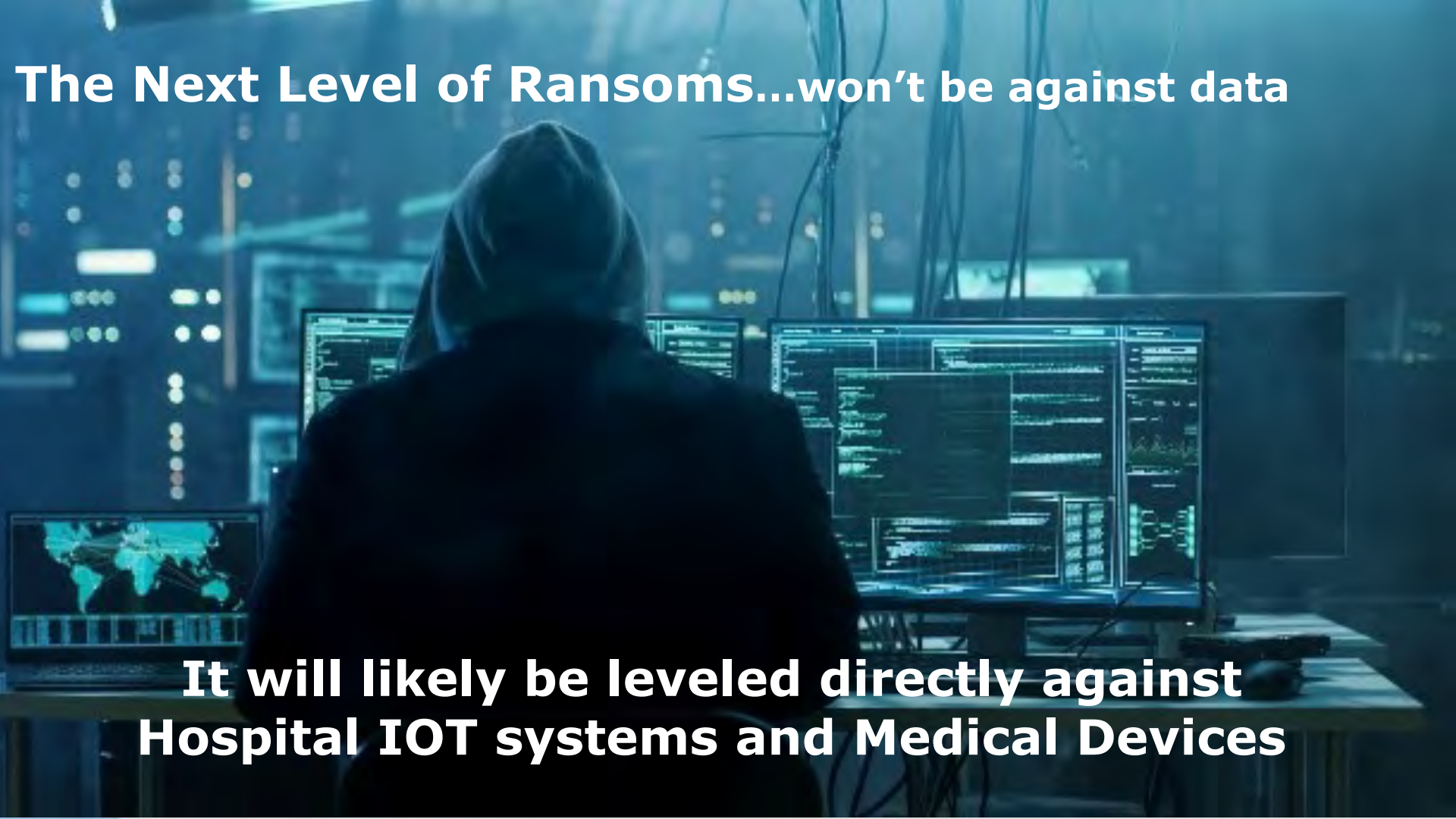
All Connected to the Hospital Network

Medical Devices

Healthcare IT and IoT




We need to Risk Assess, Isolate & Segment all Medical Devices
The Weakest Link
SET VTBI
RUN
HOLD/RESET
SET RATE
CLEAR VOL
OFF
CHARGE


The Next Level of Ransoms…won't be against data
It will likely be leveled directly against
Hospital IOT systems and Medical Devices

IOT services we can't do without:

- HVAC
- Elevators / Lifts
- Water Management
- Electrical supply

Many Hospital Deaths Result of the Failure of Critical Building Management IoT Systems

HIPAA Security Rule

Requires: Administrative, Technical and Physical security controls to protect the Confidentiality, Integrity and Availability of Health IT Systems and Data

The Big Concern However is AVAILABILTY

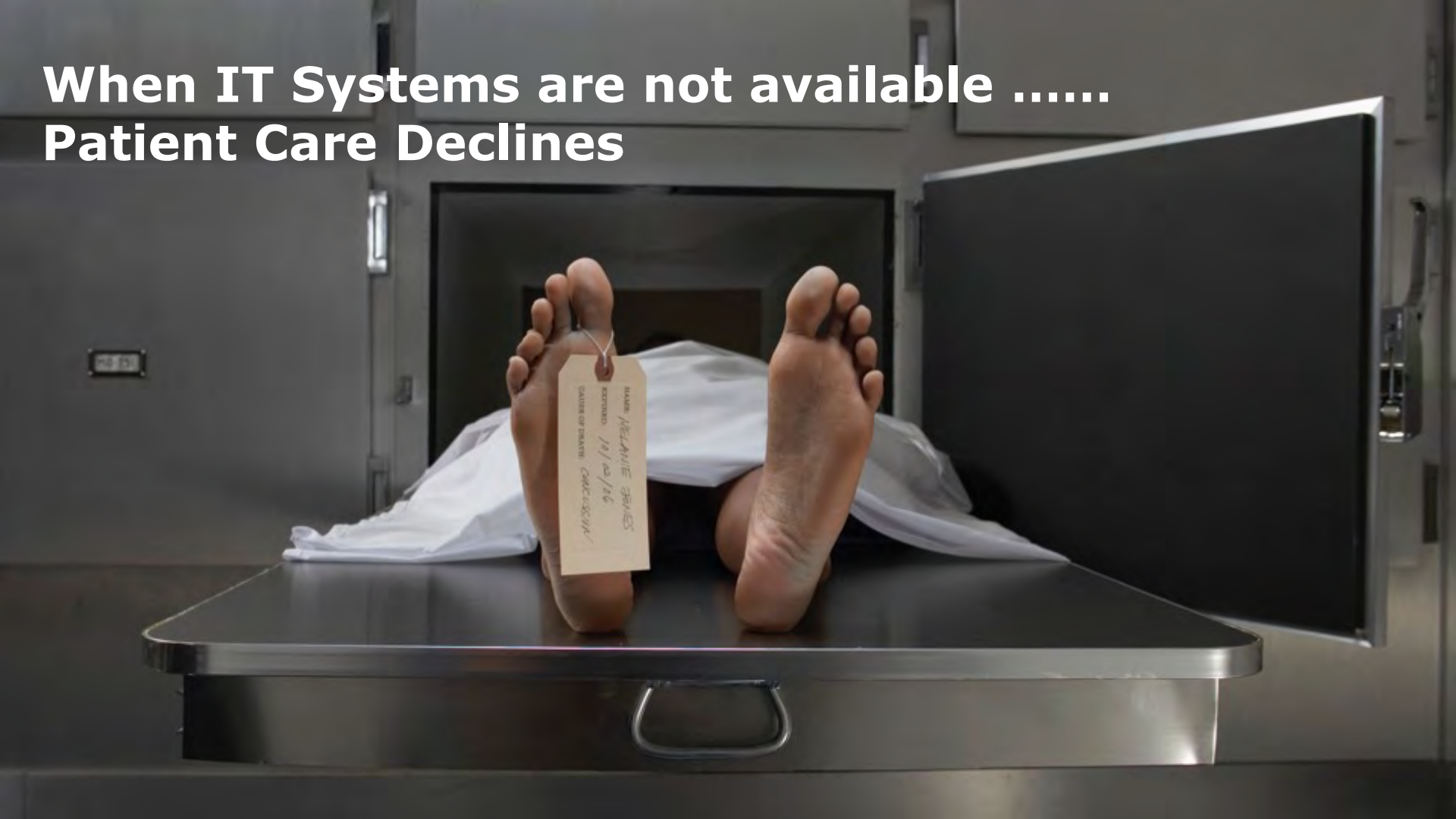

Your personal files are encrypted!
Your important files encryptive produced on this computer: photos, videos, documents etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt 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 100 USD / 100 EUR / similar amount in another currency.
Click <Next> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.
Private key will be destroyed on
9/24/2013
6:21 PM
Time left
54 : 15 : 15
MacBook Pro

Availability of Health IT Systems

No matter where you live, healthcare today is highly dependent upon electronic systems

Patient Safety and IT System Availability Are Now Inextricably Linked

When IT Systems are not available ……
Patient Care Declines



Reasonably Anticipated Threats

OCR is beginning to change its focus and is asking for evidence of security analysis of all **Reasonably Anticipated Threats** rather than just devices that create, contain or transmit PHI.

Reasonably Anticipated Threat includes anything that connects to a healthcare network – including IoT and medical devices.

The threat is that one of these devices could be turned into a botnet or used as a foothold or as an ingress / egress gateway for the exfiltration of non-public 'Protected' information.

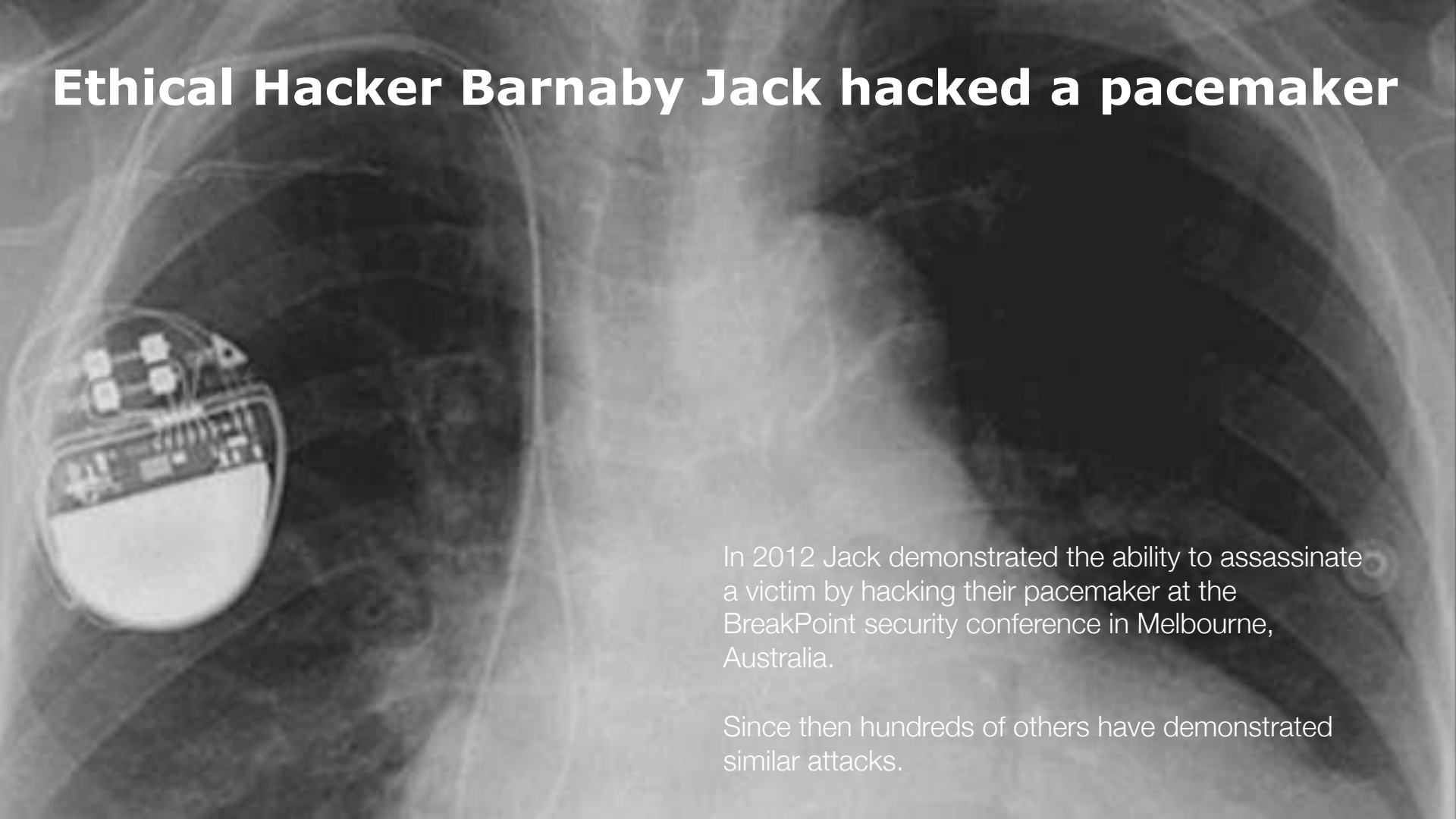
Integrity is Also a Growing Concern

Can You Trust the Integrity of your EMR, Lab Equipment & other systems?

Is my medical data correct?

HIMSS
transforming health through information and technology

Ethical Hacker Barnaby Jack hacked a pacemaker



In 2012 Jack demonstrated the ability to assassinate a victim by hacking their pacemaker at the BreakPoint security conference in Melbourne, Australia.

Since then hundreds of others have demonstrated similar attacks.

Can you Trust Your Medical Devices?

If Your Patients Were Held to Cyber Ransom….


Would you take the risk of Not Paying?
password
Without Good Information its tough to make the Right Call

First - Conduct an Enterprise Risk Assessment

(Including Medical Devices)

HIMSS
transforming health through information and technology

- Frame
- Assess
- Respond
- Monitor

Your Risk Analysis needs to conform to HHS OCR Guidance or it will be rejected

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Risk Assessment

Is NOT:

- Technical Vulnerability Assessment
- Penetration Test
- Compliance Gap Assessment

HIPAA and other regulations require you to conduct an Annual Risk Assessment

But how can you do that if you don't know what assets you have attached to your network?

Or understand what threats exist against them?

(That Includes Medical Devices)

Is Your Current Risk Assessment Process…..?

- ~~Controls Based~~
- Asset Based

You will need to evaluate the effectiveness of your security controls but before you can do that you need to understand what information assets you have

Don’t put the cart before the horse!

HIMSS
transforming health through information and technology

Determine the Level of Risk at Granular Level

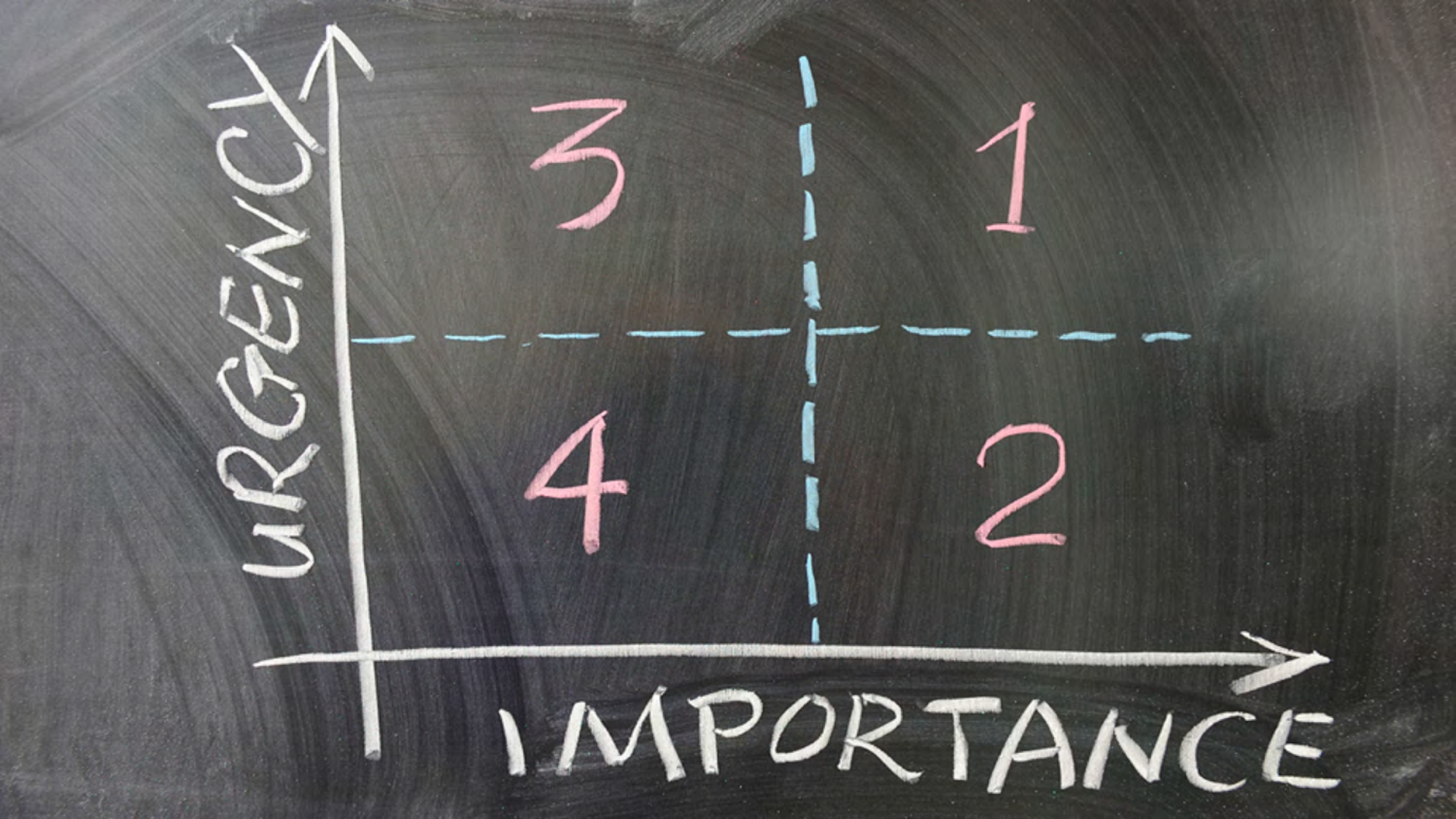
Asset	Threat Source / Action	Vulnerability	Likelihood	Impact	Risk Rating
Laptop	Burglar steals laptop	No encryption	High (5)	High (5)	25
Laptop	Burglar steals laptop	Weak passwords	High (5)	High (5)	25
Laptop	Burglar steals laptop	No tracking	High (5)	High (5)	25
Laptop	Careless User Drops	No data backup	Medium (3)	High (5)	15
Laptop	Shoulder Surfer views	No privacy screen	Low (1)	Medium (3)	3
Laptop	Lightning Strike	No surge protection	Low (1)	High (5)	5

So You Can..

CRITICAL and HIGH RISK findings should be addressed immediately to minimize the likelihood and impact of a potential attack.

Given scarce resources we need to prioritize.

Remediation of MEDIUM and LOW risk findings may need to be budgeted for next year.


URGENCY
3
1
4
2
IMPORTANCE

Questions?

HIMSS
transforming health through information and technology


Thank You
Richard Staynings
@rstaynings
Web: Richard.Staynings.Com
Blog: Cyberthoughts.Org
LinkedIn: richardstaynings
HIMSS tv