

ACRP 2019

APRIL 12-15, 2019 • NASHVILLE

Cybersecurity and Clinical Research

Paul Connelly
Vice President and Chief Information Security Officer
HCA Healthcare

ACRP 

The presenter for today's educational program is:

Paul Connelly

I have no relevant
financial relationship(s) in
connection with this
educational activity.

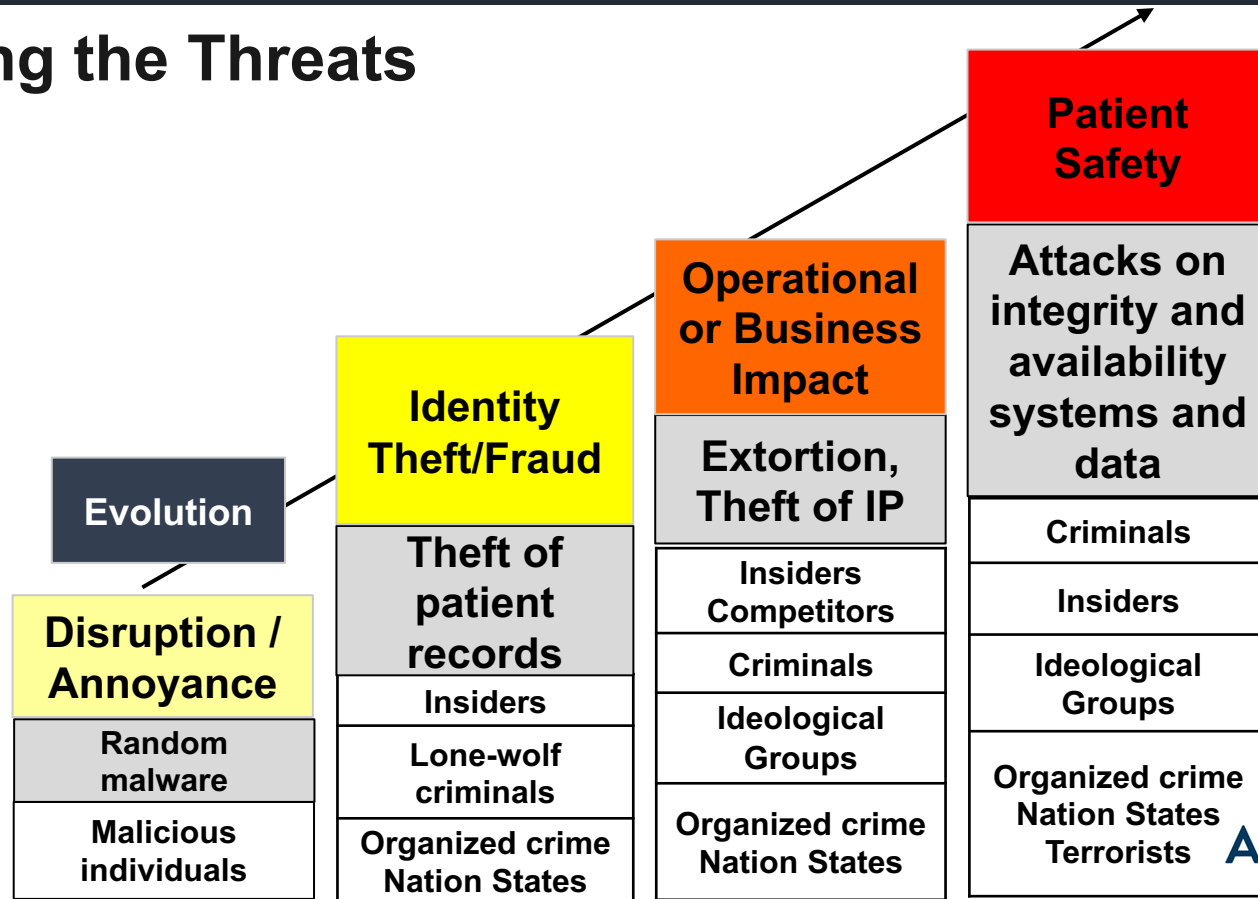
Our Perfect Storm

- Large amounts of high value data
- Growing uses of technology and data
- Dependence on third parties and data sharing
- Patient-centric focus
- Necessity for research



- Legacy of low priority given to security
- Substantial installed base of non-secure devices
- Opportunity to exploit for financial gain, leverage
- Sophistication and availability of malicious tools
- Low risk of being caught or punished

Understanding the Threats



The Potential Impacts

>40,000 Devices Disabled in
90 Seconds by Cyber Attack

CareFirst

Advocate
Health Care

CHS

Anthem

Health data breaches up 97 percent

February 01, 2012 | Diana Manos, Senior Editor

UCLA

Health System

Excelus

\$1B suit filed against Sutter Health over data breach

November 23, 2011 | [Name], Editor

PREMERA
BLUE CROSS

84 Million Health Records
Reported Breached Last year

UNCLASSIFIED
FIRE LINE
INTELLIGENCE FOR FIRE, RESCUE, AND EMS
8 February 2017

Medical Device
Hijack Attack
Discovered

Boston Children's
Hospital Comes Under
Repeated Denial of
Service Attacks

Ransomware causes 52 UK
Hospitals to Divert Patients

Nuance knocked offline by
ransomware attacking Europe

"THEDARKOVERLORD" to Post 9.3 Million
Patient Records if Ransom is Not Paid

What They Are After – “Crown Jewels”

Patient Data

- Personal data
- Insurance and payment
- Prescriptions
- Medical condition and treatment

Business Insider Information

- Market-influencing insider information
- Business email accounts
- Employee names, roles
- Business process information

Intellectual Property

- Clinical trial data
- Research data
- Clinical results
- Tools and techniques
- Trade secrets

Business Operations

- Critical systems
- Leverage for extortion

Why am I telling you this scary stuff?

The risks have changed

- Our data and role makes us a target
- We have to step up our game
- “Every member of the team has to do their part”
- It won't happen to me – famous last words

Why Cybersecurity is Critical to Clinical Research

1. Protects patients

Cybersecurity programs protect the confidentiality, integrity, and availability of data and systems used to care for patients. It is not a stretch to say it protects lives!

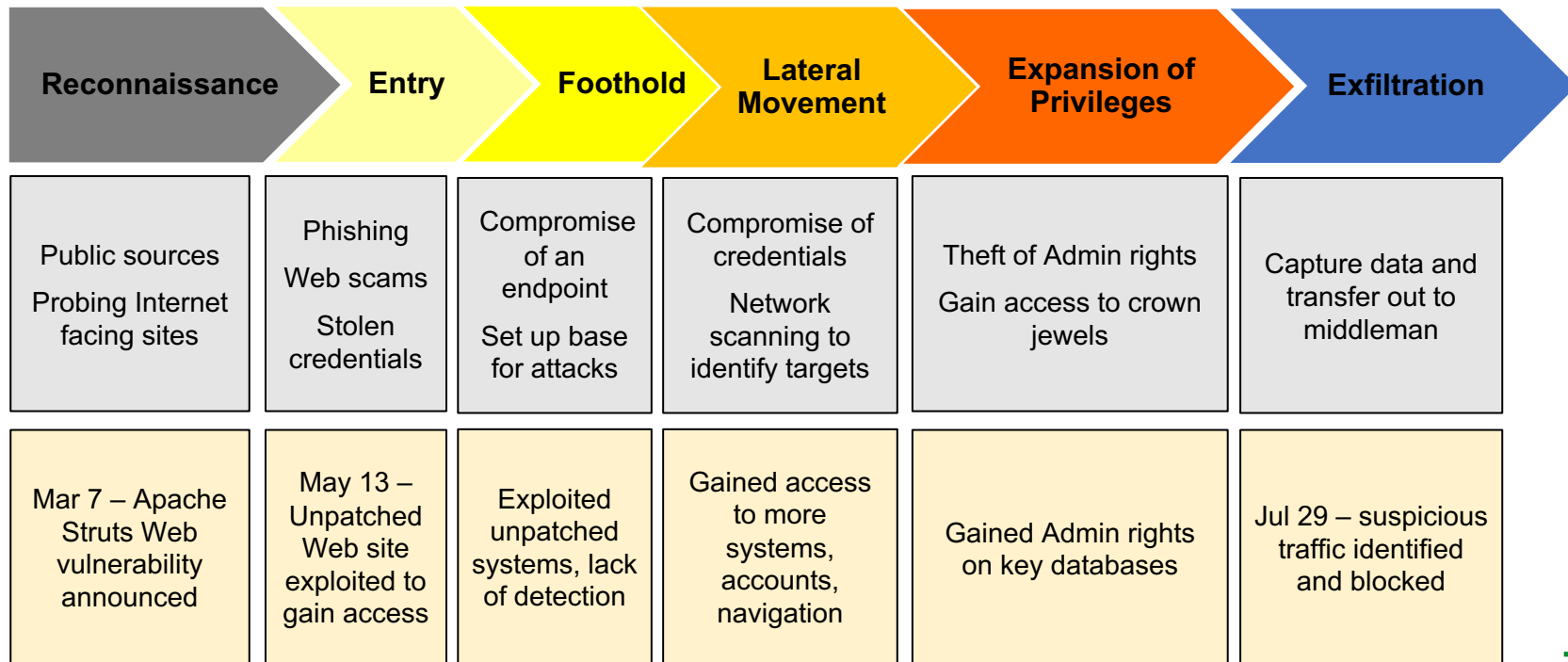
2. Protects intellectual property

Data gathered in clinical trials may determine the competitive potential of the drug, device, diagnostic tool, or vaccine. A break-through could be worth billions of dollars. Cybersecurity in clinical research is more than an ethical imperative – it's an economic requirement.

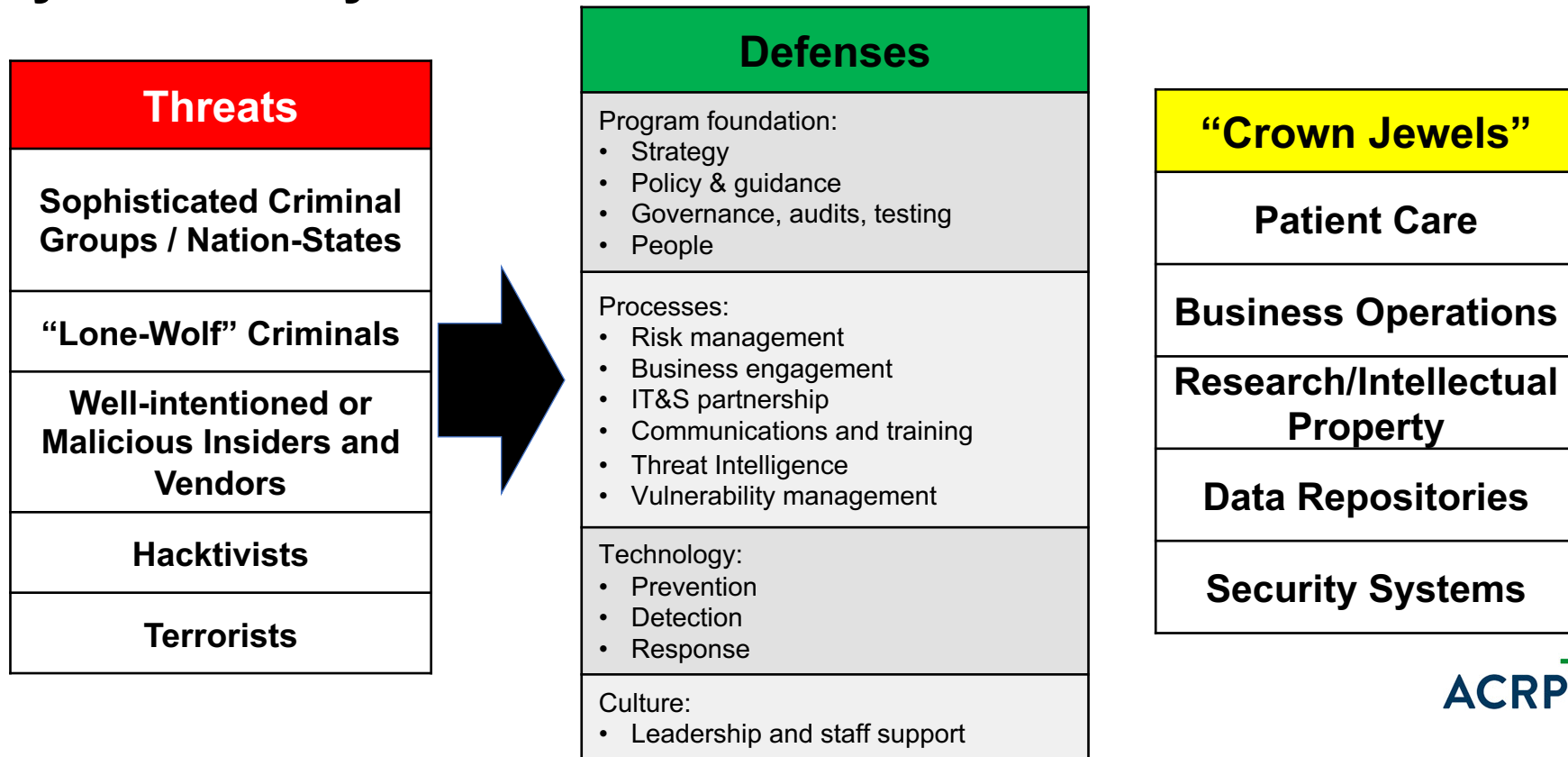
3. Protects reputation and credibility

Hacks make a lot of noise, and headlines can drastically alter a company's reputation. A breach of research/trial data can lead to challenges to the integrity and validity of conclusions and destroy or render a study worthless.

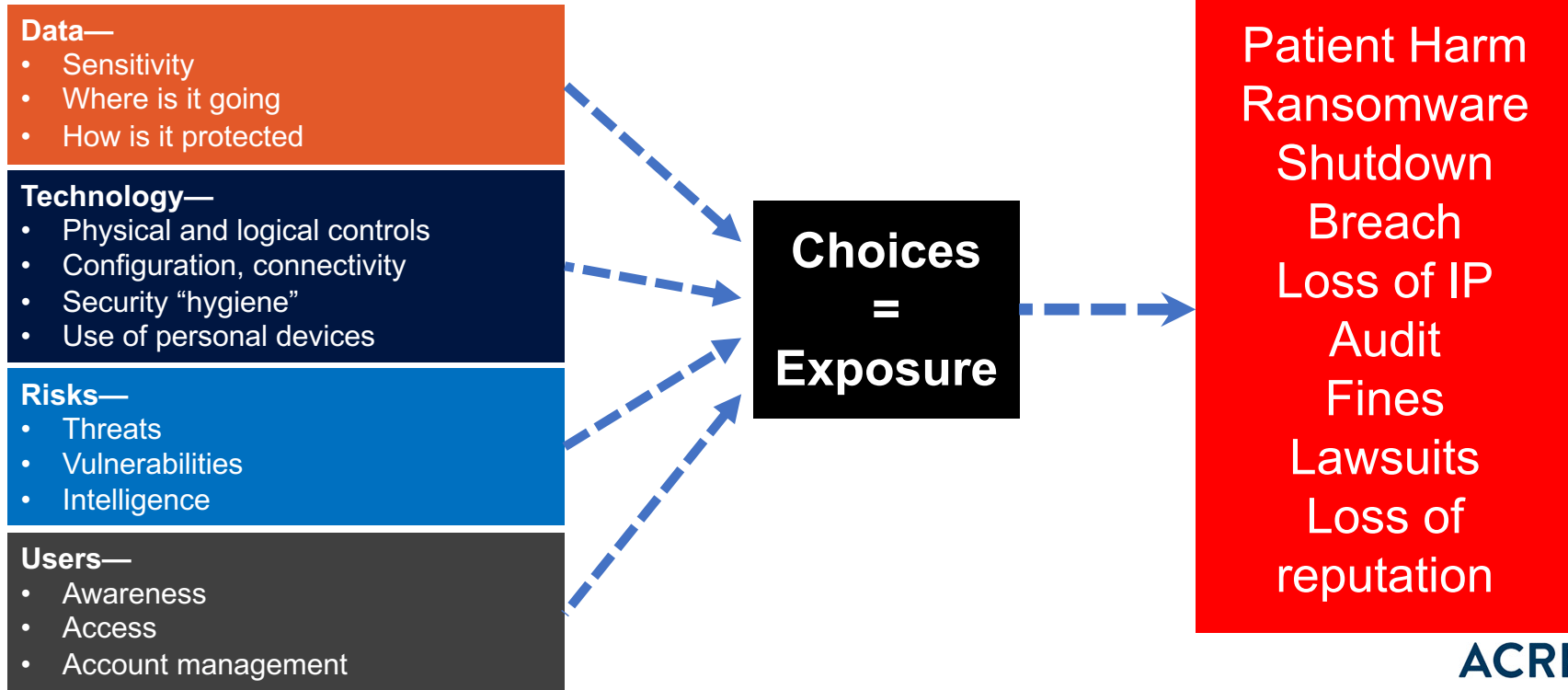
How it Happens – The Hacking “Kill Chain”



Cybersecurity Focus: Break the chain



How You Help - Connect the Dots to Your Role



Do Your Part – Know Thyself

- Know your security partners
- Know your Crown Jewels
- Think like the bad guys –
 - What do they want?
 - How could they get to it?
 - Think globally
- Work together on a plan for protection
- Keep an ongoing engagement – the risk is not static!

Do Your Part – Tools for Protecting Your Data

Need to Know: Access, use, or disclosure of information is for a legitimate patient care or business support purpose

Limited Data Set: Eliminate key elements across the data set to reduce the impact of a breach, while maintaining the validity of the data for operational or research purposes

Minimum Necessary: Share the least amount of sensitive or confidential information needed to get the job done

De-Identification: Elimination of specific personal identifiers in records to anonymize the data and reduce personal impact

Do Your Part – Catch a Phish

>90% of malicious activity starts with email

- Don't open attachments or click links in suspicious emails
- Watch for:
 - **Unexpected** notification, even from senders you know
 - **Convincing** but out of the ordinary scenarios
 - Sense of **Urgency**
 - Directing you to **hyperlinks or attachments**
 - *Sometimes--* inaccurate information or grammar
- Verify or report/delete
- Apply the same caution to social media and websites

Top Scams:

- Amazon order issue
- FedEx/UPS/USPS delivery
- Help Desk tech support
- IRS tax issue
- Credit fraud investigation
- “Unusual activity” notice from bank
- Wire transfer request
- Account lock-out
- Missed court appearance
- Refund due

Do Your Part – Take It Home

- Protect your online accounts using:
 - Strong and UNIQUE passwords
 - Two-factor authentication where available
 - Access through VPN
 - *Need-to-know* and *minimum necessary* when it comes to social media
- Reduce your exposure to tax fraud and identity theft:
 - File your taxes early
 - Consider a security freeze on your credit reports with Equifax, Experian, and TransUnion
 - Review your financial statements carefully
- Have a plan – talk with your family and friends about all types of emergency situations and actually practice your plan.
- See something, say something no matter where you are.

Pop Quiz!

From: Michael.Jones@BigPharma.com [[mailto: sender30@gmail.com](mailto:sender30@gmail.com)]

Sent: Tuesday, March 12, 2018 3:09 AM

To: Smith Beth <Elizabeth.Smith@HCAHealthcare.com>

Subject: {EXTERNAL} Updated Documents

Hi Elizabeth,

Attached are some documents for your to complete and return.

You can upload them directly to our new portal (click [here](#) to log in).

I need you to get this done ASAP!

Regards

Michael

Questions?

Paul Connelly
paul.connelly@hcahealthcare.com