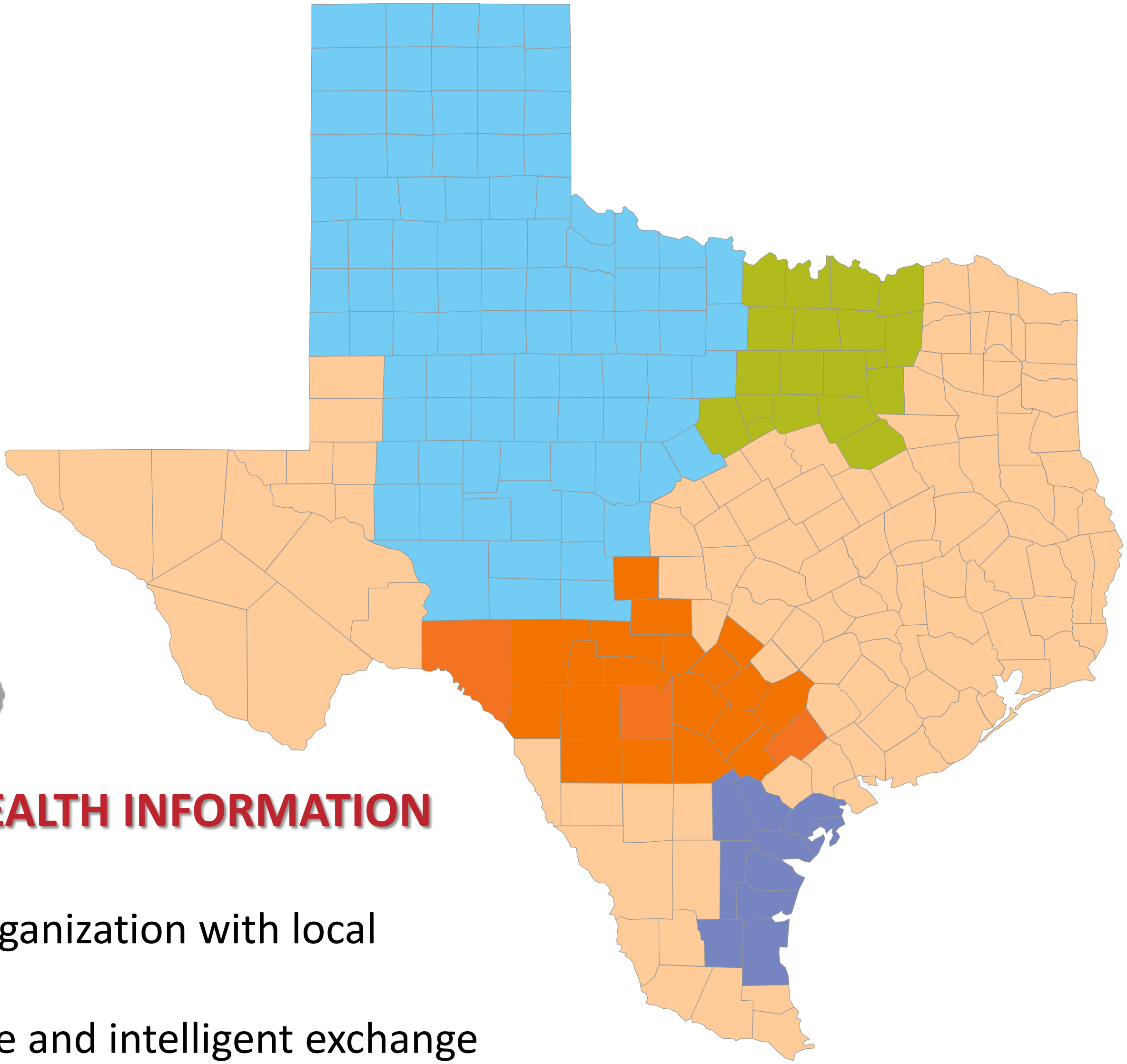
Cybersecurity Health

Phil Beckett, PhD

HASA, CIO and Security Officer

How to stop the bleeding!



HASA

Health Information Organization

COMMUNITY-BASED HEALTH INFORMATION EXCHANGE

- Neutral not for profit organization with local oversight
- Agile platform for secure and intelligent exchange
- In Texas, for Texans, connected today

WHAT IS HASA?

Centralized model

- Single community record
- Customized views
- Population management

Agile platform

- Multiple connection models
- Workflow integration
- Access and usability
- API and system integration

Community Partner

- Integrate with existing initiatives
- Local governance
- Complementary offering

Value Driven

- Focus on local stakeholder business needs
- Manage utilization and ROI metrics
- One connection, all the data

WHO IS HASA?

Gijs van Oort
CEO

Phil Beckett
CIO

Kim Harris
Marketing

Andrea Espinosa
Analytics

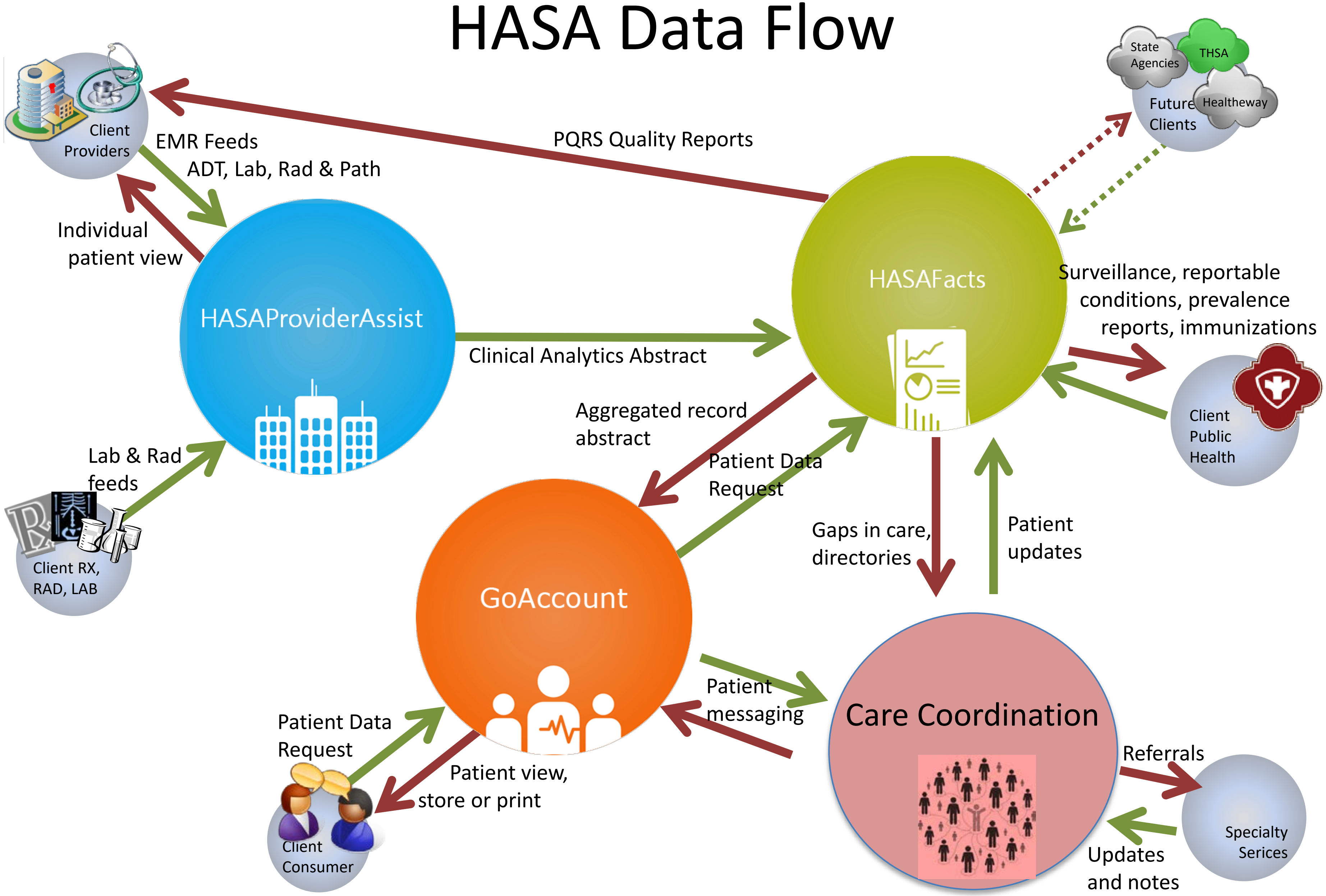
Rob Harris
Implementation

Carol Herrera
Administration

Jim Hoag
North Texas Lead

Storey Sherriff
Marketing

HASA Data Flow



Client Providers

EMR Feeds
ADT, Lab, Rad & Path

PQRS Quality Reports

State Agencies

THSA

Healtheway

Future Clients

Individual patient view

HASAProviderAssist

Clinical Analytics Abstract

HASAFacts

Surveillance, reportable conditions, prevalence reports, immunizations

Client Public Health

Lab & Rad feeds

Client RX, RAD, LAB

Aggregated record abstract

Patient Data Request

Gaps in care, directories

Patient updates

GoAccount

Patient messaging

Care Coordination

Referrals

Specialty Serices

Updates and notes

Patient Data Request

Patient view, store or print

Client Consumer

FOURTH ANNUAL 2017

DATA BREACH INDUSTRY FORECAST

Experian®

By Experian® Data Breach Resolution

Based on Experian, the top data breach trends for 2017 are:

- Aftershock password breaches
- Nation-State cyber-attacks move from espionage to war
- Healthcare organizations will be the most targeted sector
- Criminals will focus on payment-based attacks
- International data breaches will cause big headaches for multinational companies
- Virtual reality

What is the Incentive

- 10 Medicare numbers – 22 bitcoin, $15,550
- Why $1500 per Medicare number?
  - Includes SSN, names, dob, policy #s and billing information
  - Can
    - Open credit lines
    - Generate fake IDs
    - Purchase and resell medications and durable medical equipment
  - Longevity

Why the easy target

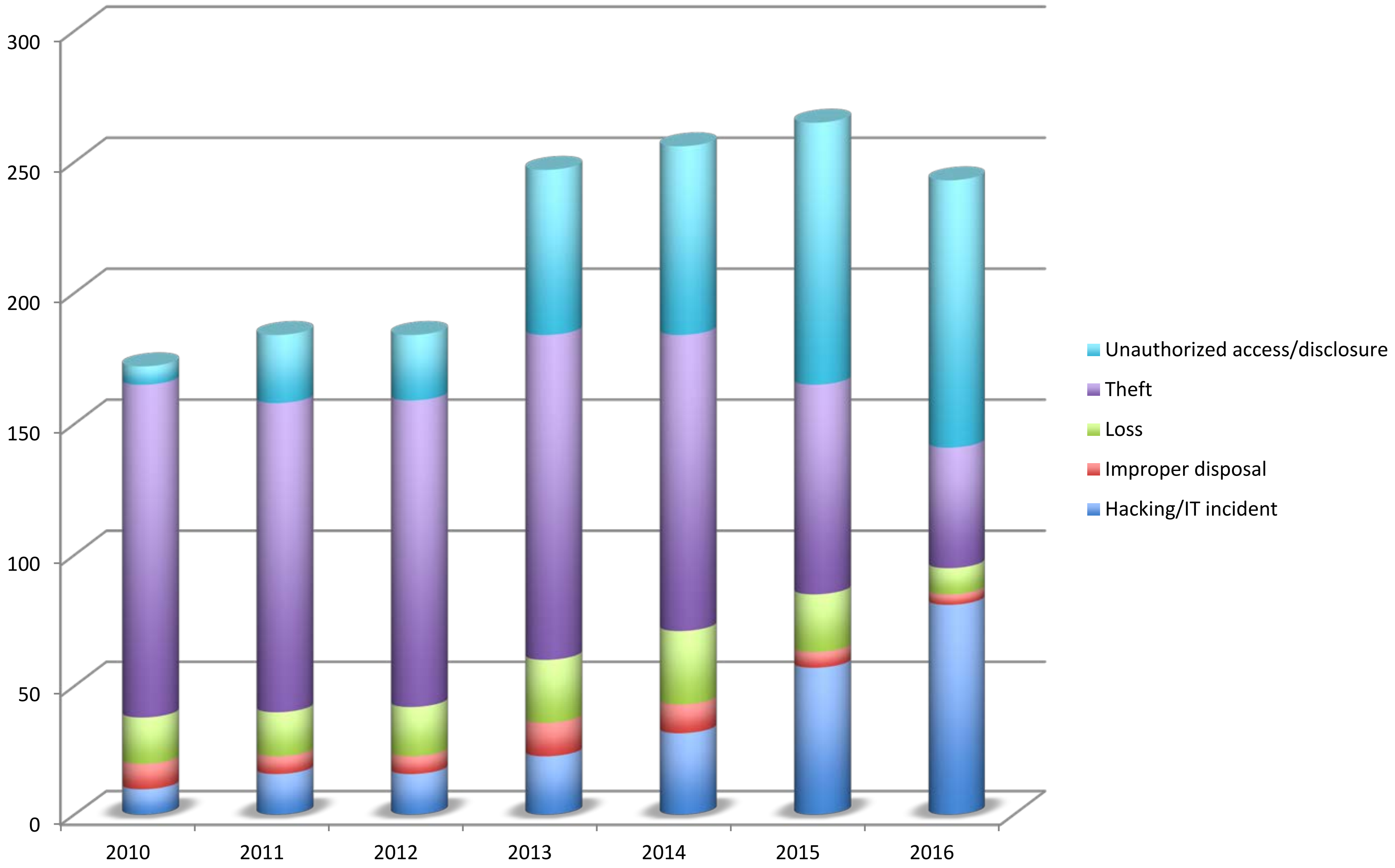
- Independent workforce, many in small practices
- A focus on healthcare
- Thin margins/investment priorities
- Damaged party and controlling party different/consumer demands
- Need to share/many Business Associates
- Software systems requiring old OS

How

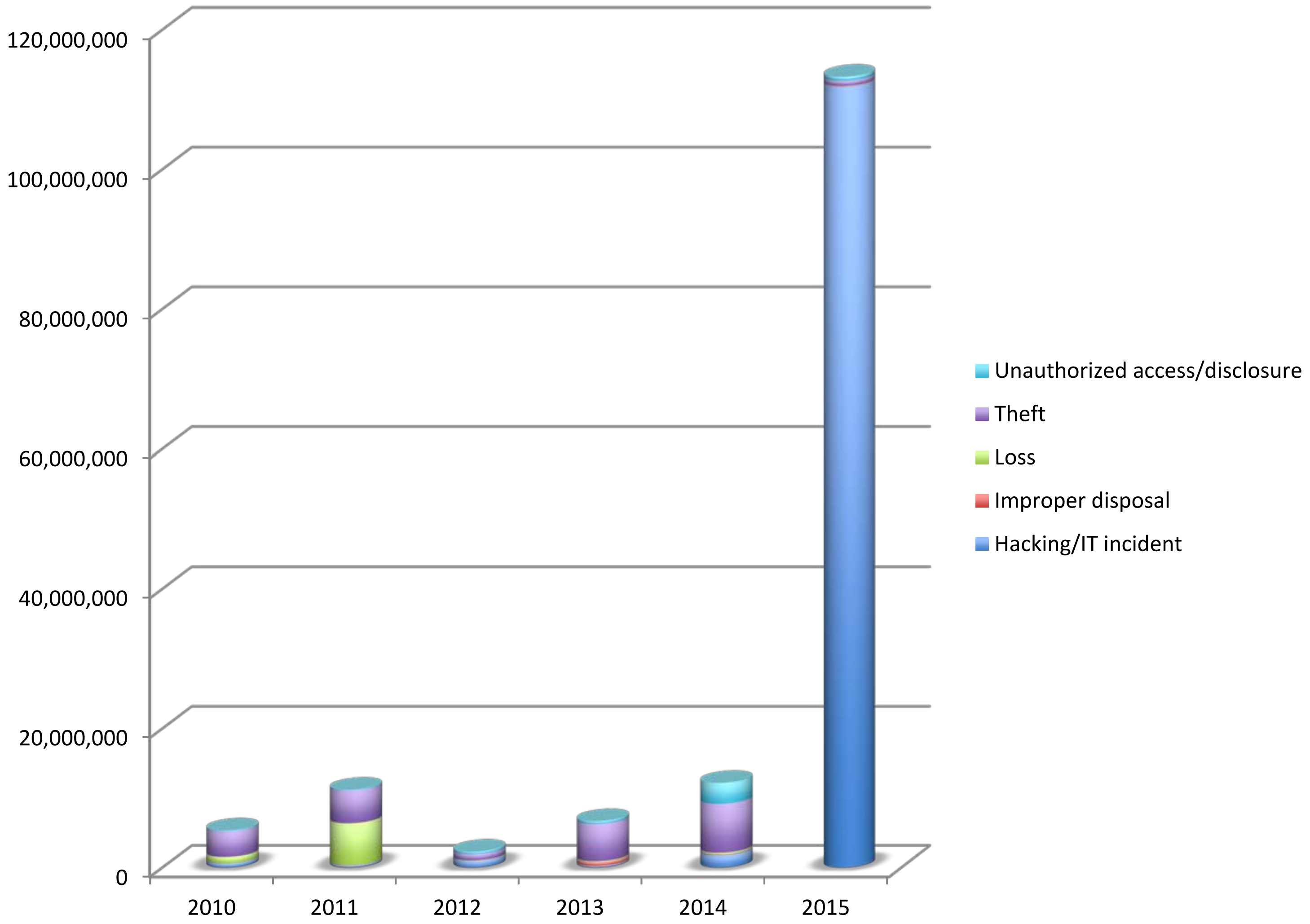
- Social exploitation/engineering
  - Ransomware
  - Phishing

- Theft, loss, improper disposal, data on laptops
- Unauthorized disclosure
- Internal malfeance

How much/many?

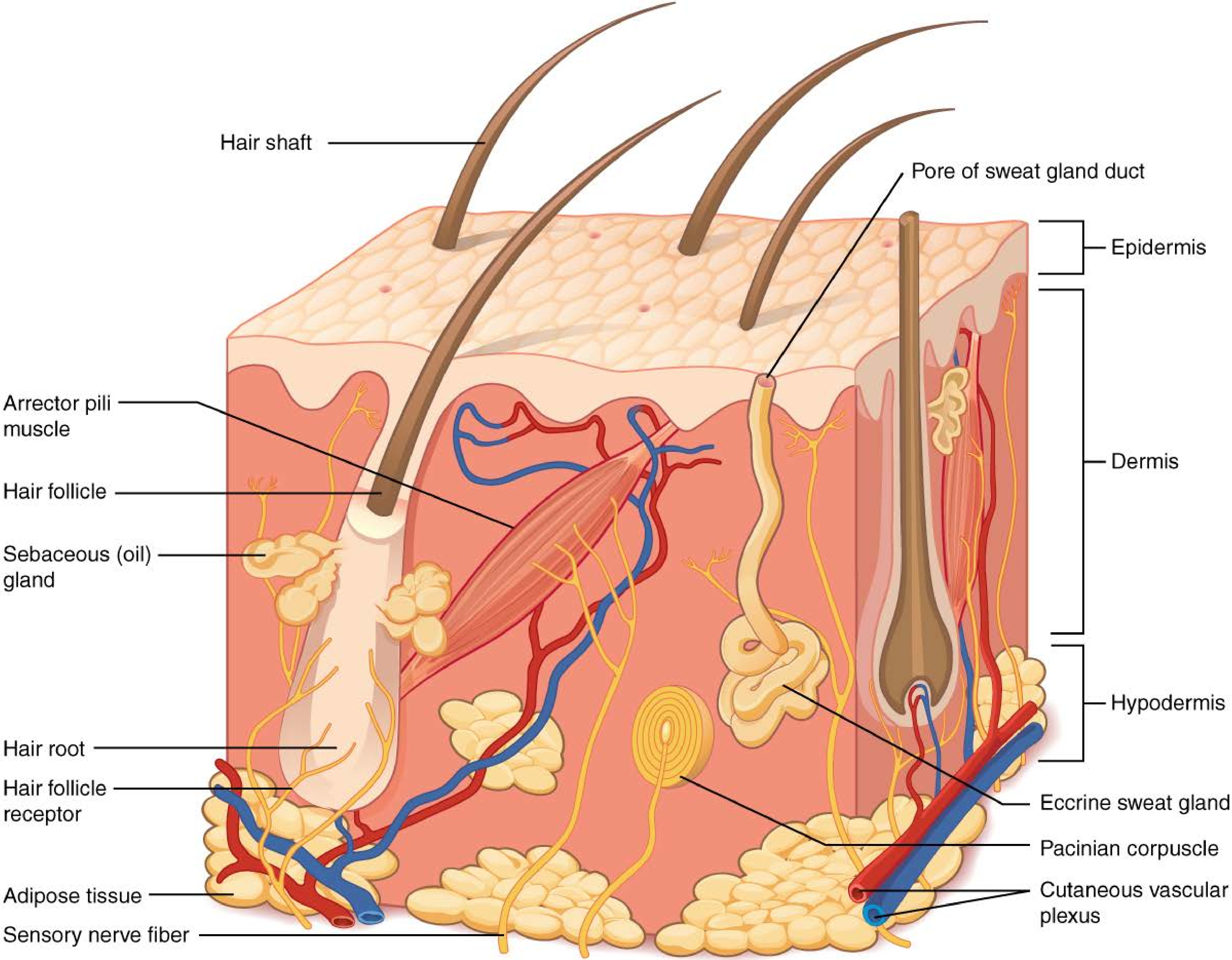


Records disclosed

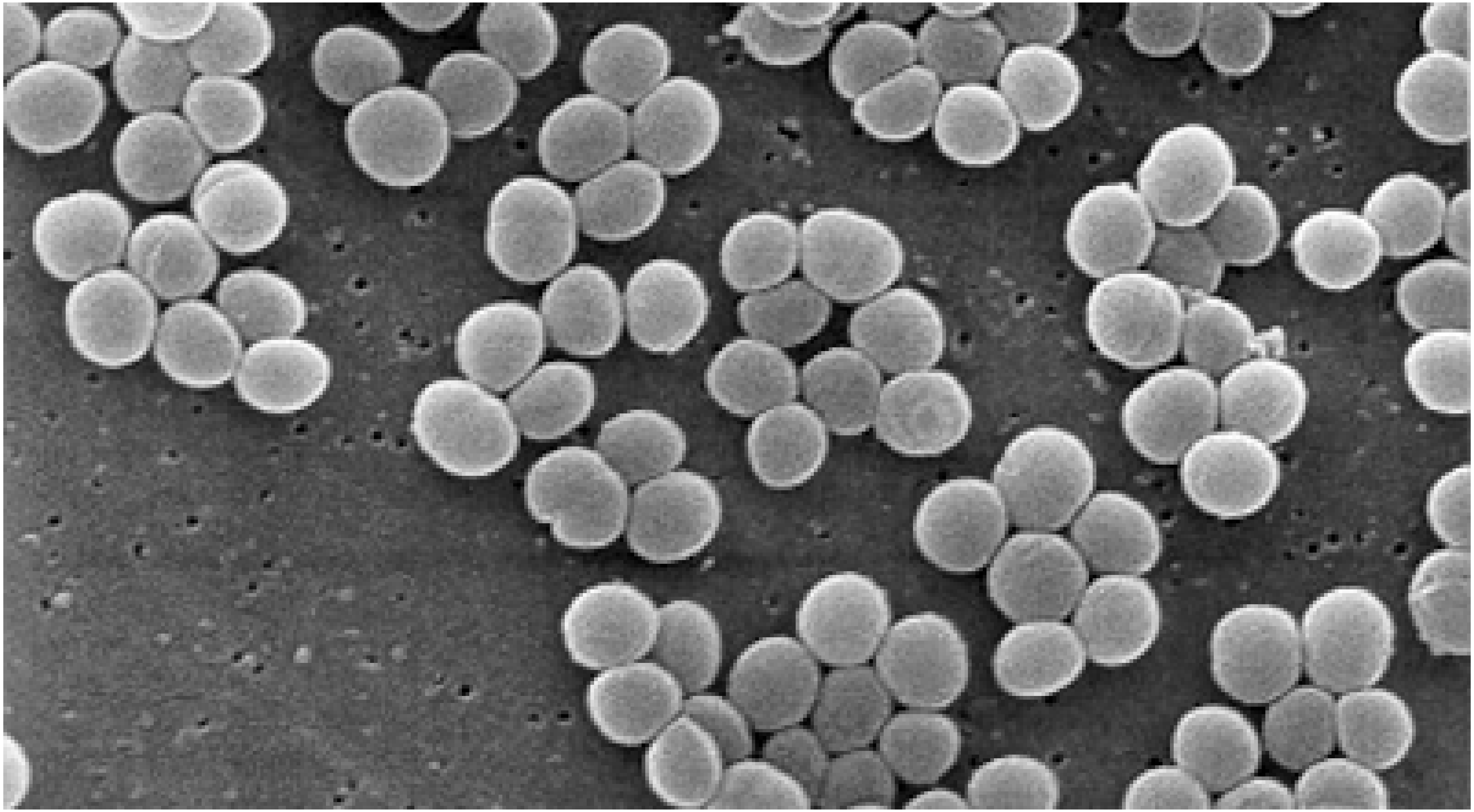


Incidents by:

- External Hackers – 40%
- Internal negligence – 30%
- Internal bad players – 30%



Hair shaft
Pore of sweat gland duct
Epidermis
Arrector pili
muscle
Dermis
Hair follicle
Sebaceous (oil)
gland
Hypodermis
Hair root
Hair follicle
receptor
Eccrine sweat gland
Pacinian corpuscle
Adipose tissue
Cutaneous vascular
plexus
Sensory nerve fiber



Multi factor defense

1. Barrier – epidermis replaces itself every 4 weeks
2. Covering of good microbes
3. Blood clot – prevents systemic distribution
4. Lymphocytes – grab germs and isolate them in lymphocytes
5. Nerve cells – signal to the body of a problem, activate immune system
6. Pattern matching to know self from pathogen

Sepsis – 0.072%, 35% mortality

2015 - 100 million healthcare records hacked

External Hackers

HACK LIKE A PRO

Linux Basics for the Aspiring Hacker, Part 1 (Getting Started)

Multi Factor Authentication

Username	pbeckett
Password	********************************

Sign in

Verify

Remember – hackers can call your cell phone service provider, change your SIM and redirect your SMS to another phone. Put two factor on your phone account. Use email recovery with two factor

Block Chain

- Encrypted catalog
  - Hash – to know if corrupted
  - Access control/permissions
  - Link to source

Internal negligence

- Encrypt
- Multi factor authentication
- Don’t copy, use Block chain

Internal bad players

- Culture of security
- Make secure methods the path of least resistance
- Incentivize good habits, penalize bad habits
- Leverage the crowd
- Monitor, track, question and respond

Summary

- Encrypt
- Multifactor authentication
- Make catalogs not copies
- Make security your company culture

Thank You

Questions?