

The Guide Book to Data Security

Rich Miller

President & CEO, Virtua

September 8, 2017

Optima Healthcare &

California Healthcare Insurance

Owners Retreat

September 8, 2017

Leadership & Cybersecurity

What's ahead:

- About Virtua
- Healthcare Phishing Attacks: Impacting Awareness and Behavioral Change
- Rich's 10 Leadership Tips



MISSION:

Virtua helps you *Be Well, Get Well, Stay Well*

VISION:

Virtua will be the premiere choice in
health and wellness

VALUES:

- Integrity
- Respect
- Caring
- Commitment
- Teamwork
- Excellence

■ Ambulatory

- Access and Navigation
- Virtua Medical Group
- Virtua Express Urgent Care
- CVS MinuteClinics
- Health & Wellness Centers
- Ambulatory Surgery Centers
- Home Health Agencies serving Burlington, Camden and Gloucester counties
- Virtua Home Caregivers
- Hospital Based Ambulatory Programs
- Teladoc



■ Population Management

- Virtua Care-Accountable Care Organization
- Virtua Physician Partners—Clinically Integrated Network

■ Acute Care

- Three acute care facilities in excess of 950 beds
 - Marlton
 - Mount Holly – Relocation to Westampton (Projected 2022-23)
 - Voorhees

■ Post Acute

- Two skilled nursing facilities in excess of 300 beds



■ Other

- Virtua Foundation
- Virtua Assurance – Captive



■ Quality and Safety

- Best Regional Hospitals – US News & World Report
- Patient Safety Excellence Award – Healthgrades
- “A” Rating – The Leapfrog Group

■ Financial

- AA- credit rating with Standard & Poor’s and Fitch Ratings
- Total revenues of \$1.3 billion

Something Smells
PHISHY 

Impacting Awareness
and Behavioral Change





The

PLAYBOOK

on Cybersecurity

If you don't have one already,
create an IT Committee to the Board

Make data security

part of your strategic plan

Employ a Chief Information Security Officer
(CISO)

Invest in the necessary technology

(Not an option not to be compliant)

Work with **GREAT partners**

(makes sure goals are aligned on security)

Engage in **constant employee education**

on best practices around data security

Develop **policies and procedures**

on how to protect data, *but also what to do should a breach occur*

Centralize IT purchases,

and have every vendor complete an in depth questionnaire

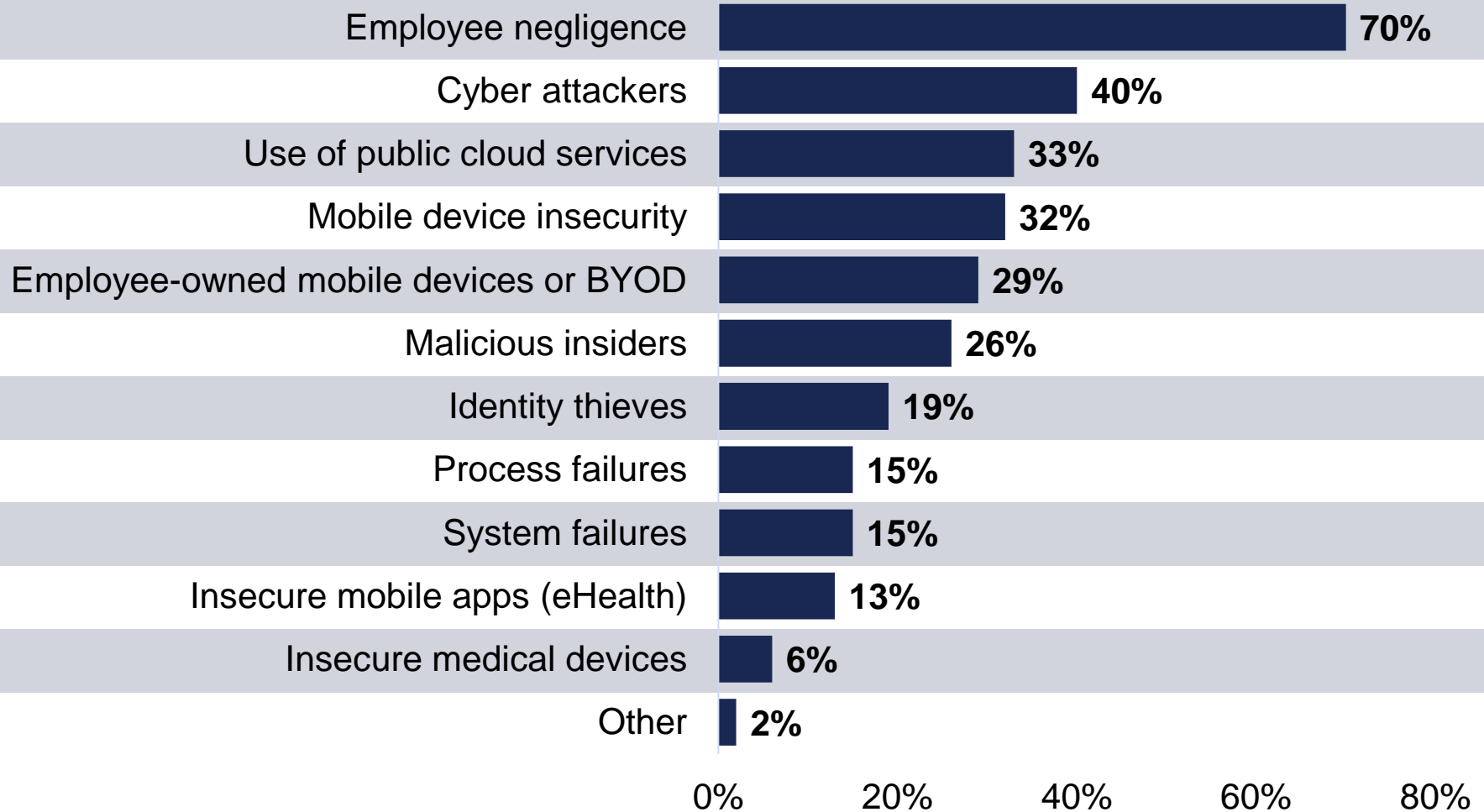
Ensure all vendors have **cybersecurity insurance and BAA**

(Business Associate Agreement)

Governance, Communication, Risk Management Program's are **required**

no matter the size of the organization

Security Threats Healthcare Organizations



2016

HIGH PROFILE EXAMPLES



**HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER**

- Ground to a halt after hackers breached the system
- Relied on pen and paper records for over a week
- **Paid the 40 bitcoin (\$17,000) ransom to regain control of its network**

MedStar Health and a hospital in Kentucky were hit with similar attacks



is a
TARGET!

Why are Phishing attacks so dangerous?

Often the email **appears to come from a legitimate company** and looks very official.

In some cases, **the email actually comes from a known legitimate email address** that has been compromised.

Easy to be fooled into providing credit card numbers, social security numbers and account information

The sense of urgency and impending doom created coaxes recipients into taking immediate action or face dire consequences.

Double clicking on unknown Word, Excel, or PDF attachments **can lead to serious virus infections** such as Ransomware.

Why is

SPEARPHISHING

so successful?

Highly Targeted & Thrives on Familiarity

The attacker knows your name, your email address, and at least a little about you.

The salutation on the email message is likely to be personalized:
"Hi Bob"
instead of
"Dear Sir."

The email may make
reference to a "mutual friend."
Or to a
recent online purchase
you've made.

Because the email seems to come from someone you know,
you may be less vigilant
and give them the information they ask for.

Vulnerabilities

Not just EHRs – devices (monitors, pumps, etc.)

**Industry push
for connectivity
adds risk —**
HIEs, and
community
physicians

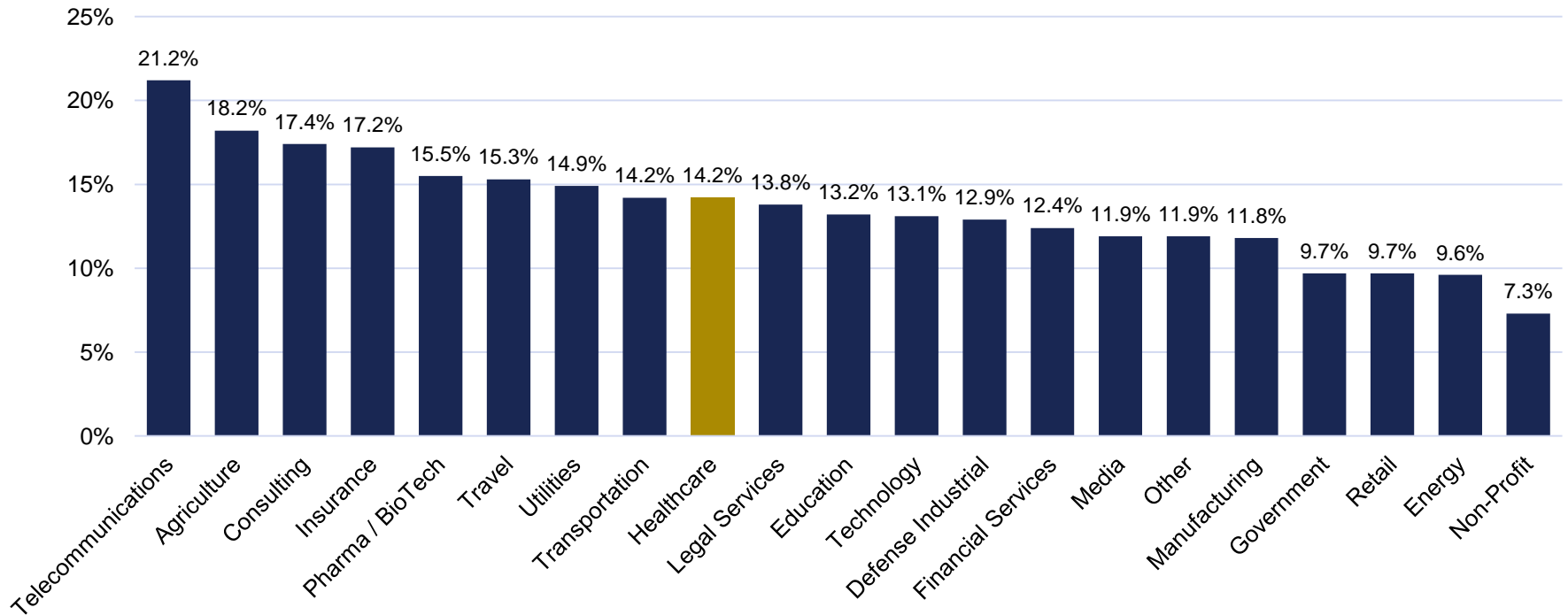
**Common
deficiency —**
lack of
effective risk
assessments

**Vulnerabilities
through
vendor
relationships**

**It's not just
IT/technical
security –
PEOPLE**

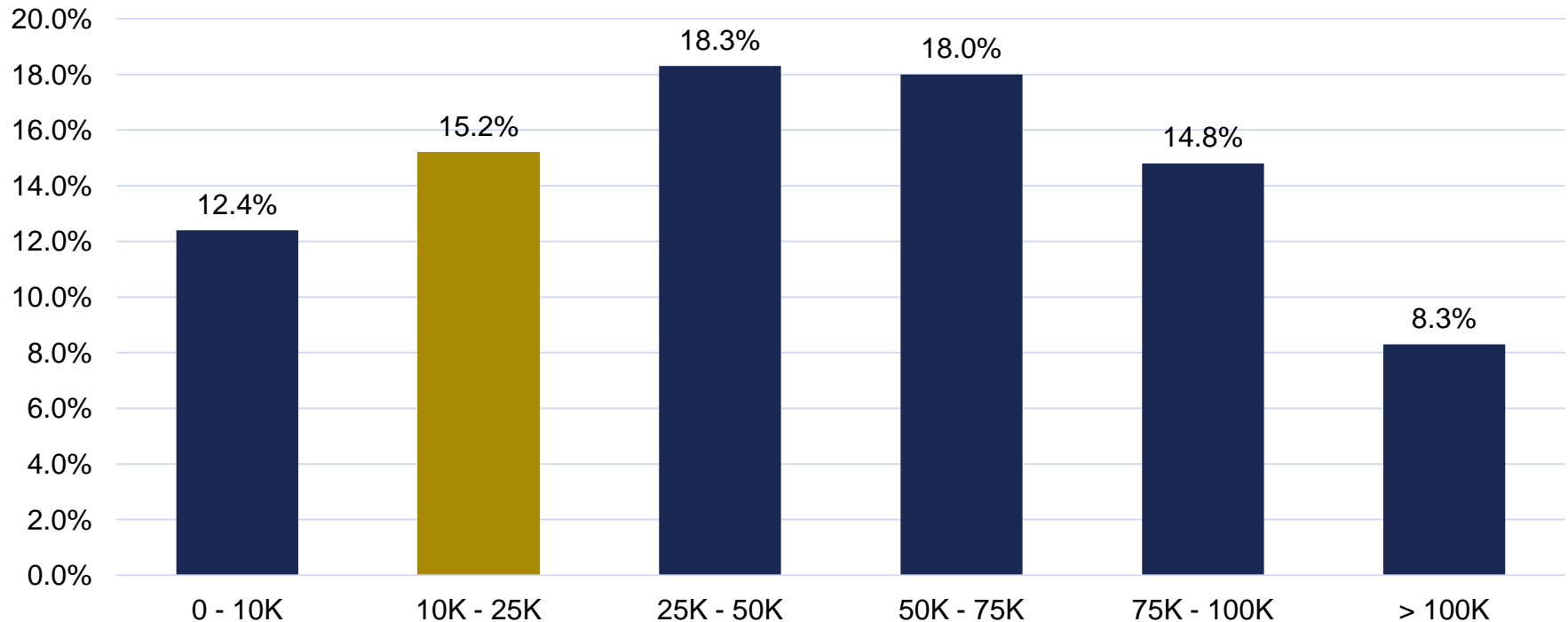


Average Susceptibility Rate of Each Industry 2016



- The healthcare industry had an average susceptibility rate of **14.2%**.
- This number represents the average susceptibility rate of 100 healthcare companies and over 1,000 scenarios launched.

Healthcare Industry Average Susceptibility Rate by User Group Size
2016

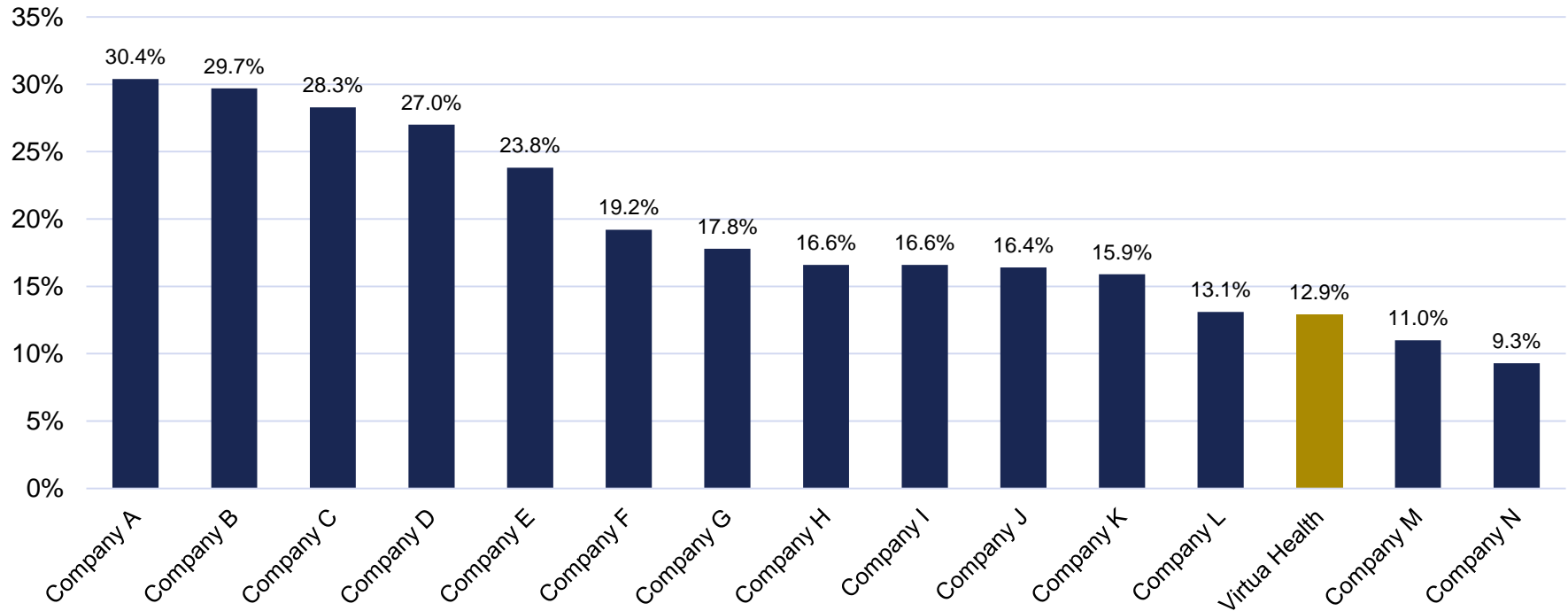


- Healthcare companies with 10K to 25K users had an average susceptibility rate of **15.2%**.
- Similar size as Virtua


2016 Virtua vs. Other Healthcare Company Susceptibility Rates



Virtua Health vs. Other Healthcare Companies' Average Susceptibility Rates



- The average susceptibility rate of 14 healthcare companies similar to Virtua that ran scenarios in 2016.
- Compared to these companies, Virtua Health had an average susceptibility rate of **12.9%** for all scenarios completed in 2016.

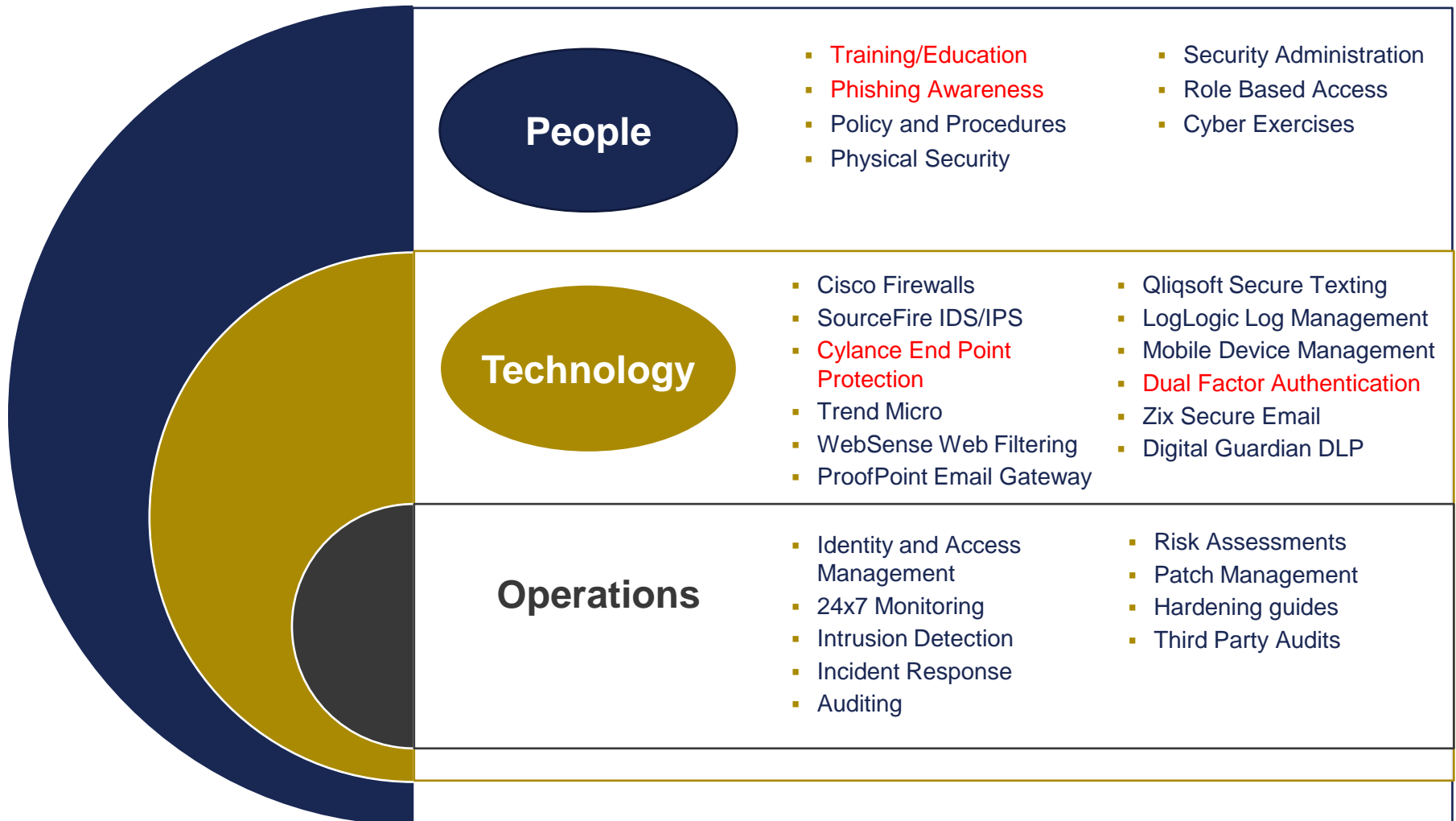


Firewalls,
gateways,
filtering, and
other **perimeter**
defenses

Inside the
perimeter
– **soft**
& **gooey**

*Need
education,
awareness,
communication,
and tools*

Virtua Defense In-Depth Strategy



Governance

Security starts at the top – cyber risk should be part of the Risk Management (RM) program

Build in accountability for information security across the organization from frontline to executive staff

Ensure the **information security function is visible** (Senior management accountability and board engagement)

Educate, communicate!



PHISHING with Rich Miller & Lou Dignam

ReportPhish@virtua.org



PhishMe

helps enterprises proactively combat the serious threat of Phishing by **cultivating their most overlooked security asset: their users.**

Prepares employees to be more **resilient and vigilant** against targeted cyber attacks.

Empowers employees to **easily report suspicious emails** to the internal security team and help desk in a timely manner.

Provides incident responders with the ability to effectively prioritize, analyze, and act on suspect email reports detected by users, **producing actionable intelligence** that can be integrated with and employed by an organization's existing security infrastructure and analytics capabilities.

OUR Goals



Reduce employee susceptibility to email-based social engineering



Minimize/eliminate repeat victims



Minimize/eliminate employee backlash to this process

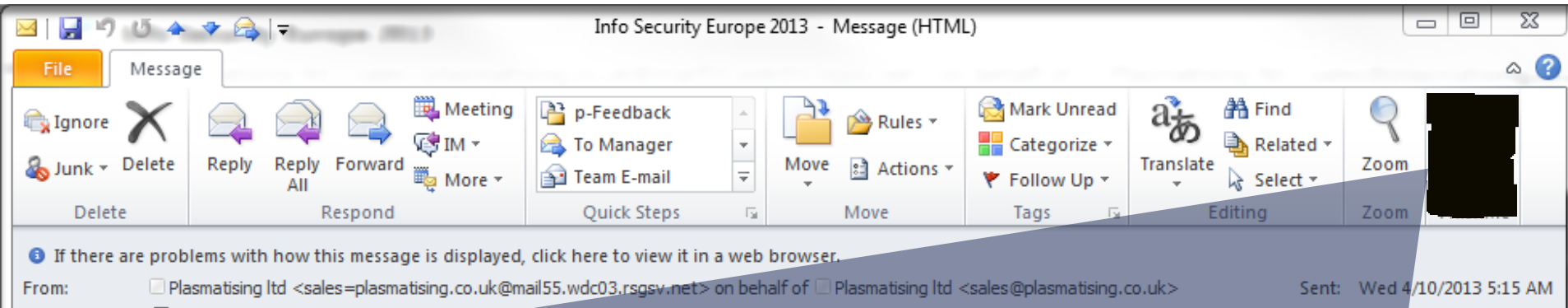


Encourage employees to report suspicious emails in a timely manner



Rapid detection and response to phishing/malware attacks

PhishMe Reporter



- Simplified single-click reporting for users
- Standardized submission format to security and the help desk
- Reported PhishMe scenarios reflected in reporting
- Fully customizable
- Enterprise-wide deployment

Protect Yourself and Your Company

Be very cautious when looking through email.

Examine it closely before opening or clicking on any links or attachments.



Hover over all links in an email without clicking on them.

This tells you exactly where the URL is going to take you.

If you don't recognize the link, **don't click!**
REPORT IT!

- Be the same person at work, as you are at home. In other words, be genuine all the time – bring your values with you everywhere you go!
- It's all about people, people who you surround yourself with and how you hire.
- There will be great days and there will be bad days – stay even keel – do something for someone every day.
- Use your intuition in decision making.
- Listen well.
- Cultural change is enormous and takes time.
- Get a life coach as you move up – someone you can talk intimately to. (different perspective)
- Life balance is crucial.
- Have fun – enjoy the small stuff.
- Quiet time – time to think.

Questions & Answers

