

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: MASH-F03

Cybersecurity and Hospital Infection Control: Overlaps and Opportunities

Howard Poston

Cyber R&D
The Cybermaniacs

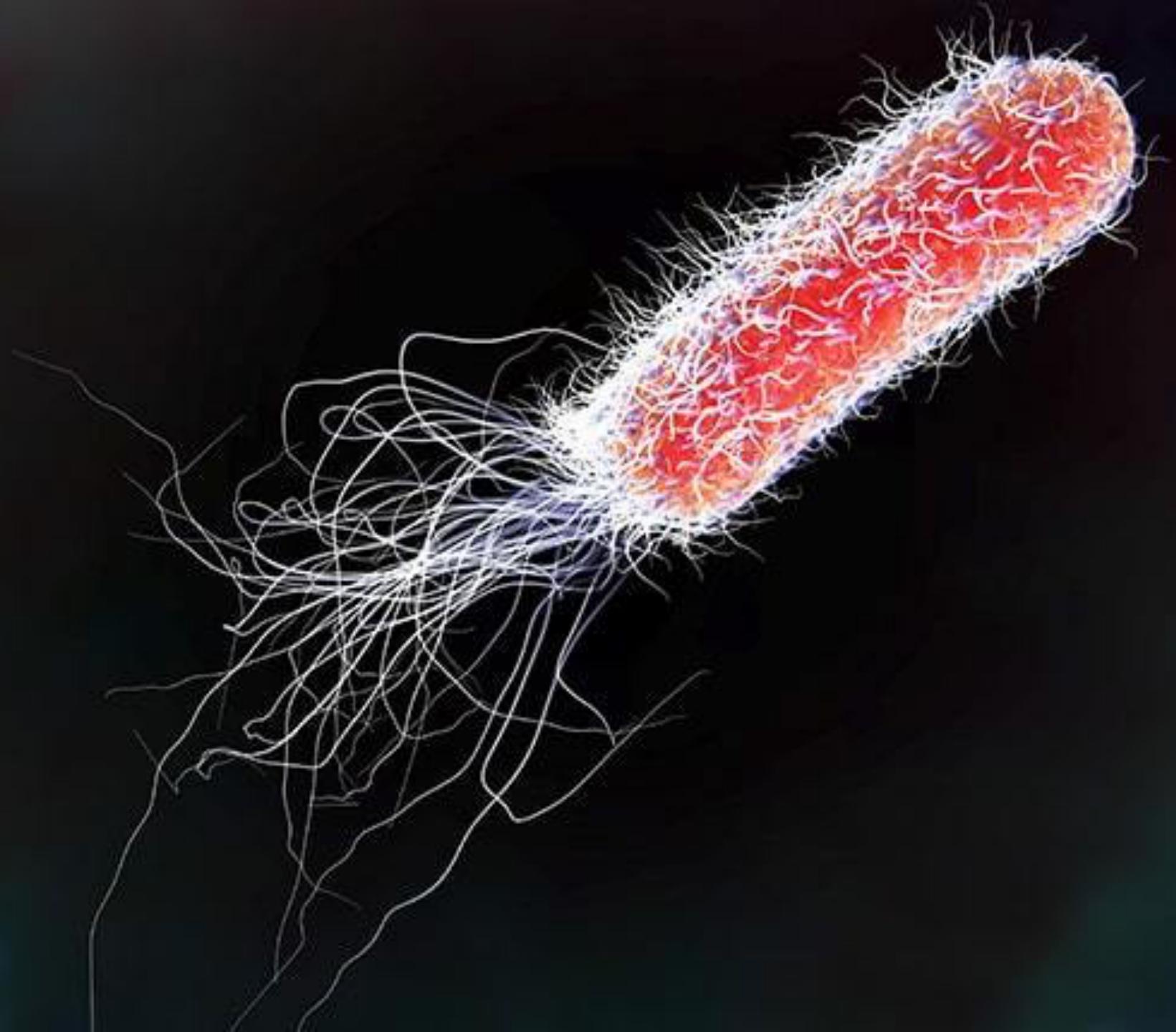
Mariam Salas, MD

Assistant Professor, Infectious Diseases
University of New Mexico

#RSAC

RSA®Conference2019

Cybersecurity and Hospital Infection Control



Hospital Infection Control

- **Infection prevention and control (IPC)**
 - is a scientific approach and practical solution designed to prevent harm caused by **infection to patients and health workers**. It is grounded in **infectious** diseases, epidemiology, social science and health system strengthening.



Hospital Infection Control

- **Infection Control Specialists**

- work to prevent disease outbreaks from becoming **epidemics**
- focus on **preventative actions** (encouraging good hygiene, preparing for an outbreak, etc.)
- and **respond** to outbreaks in progress



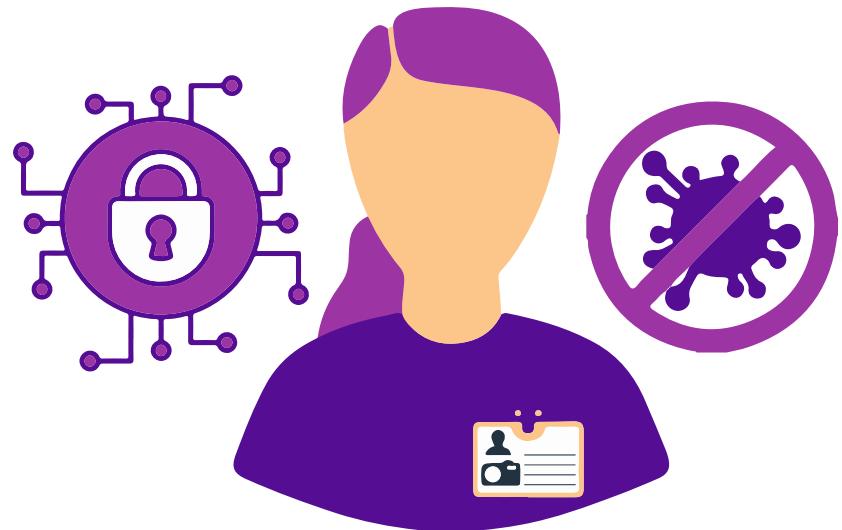
The Overlap

*Cyber security professionals and hospital infection control practitioners perform **similar roles** in very different environments...*



The Overlap

*Cyber security professionals and hospital infection control practitioners perform **similar roles:***



- **Phases:** Prevention, Detection, Response
- **Penalties:** regulatory, financial, public perception/reputation
- **Surveillance system design**
- Infrastructure to aid **prevention**
- **Behaviors** of individuals/end-users
- **Agility** needed to keep atop threats
- **Global scale**

The Big Differences

- **Expected Impact:**
 - **Healthcare:** Loss of life/health is possible or probable
 - **Cybersecurity:** Financial/reputational damage is most probable
- **Types of Threats:**
 - **Healthcare:** All threats are self-spreading, infectious diseases
 - **Cybersecurity:** Only a subset of computer viruses are “worms”



A Brief History of Infection Control

- Wait and see
- Witch burning/folk remedies
- Quarantine
- Individual treatment
- Immunization
- Preventative treatment
- Individualized/genetics-based treatment

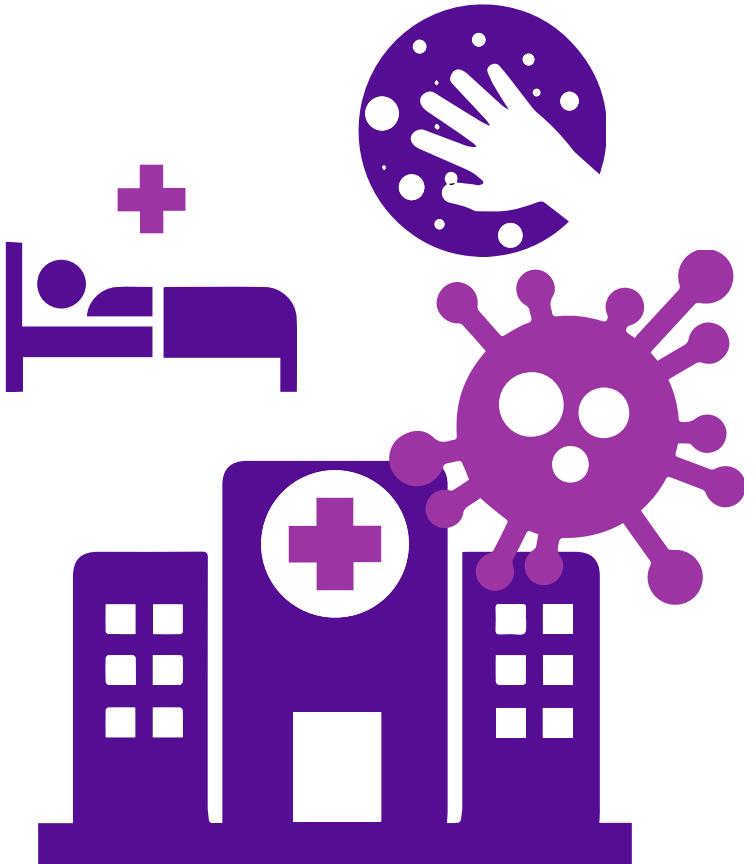


RSA® Conference 2019

What's the
Problem?



- Anyone admitted to a hospital has a **5%** chance of contracting an HAI.
- The hospital length of stay increases by **17.6 days** when patients get an HAI.
- Nearly **99,000 people** die in the United States annually from HAIs; this is more than breast cancer and prostate cancer combined.
- Around **9.4%** of inpatient costs are HAI-related.
- HAIs cost the healthcare system around **\$35 billion** per year.
- HAIs account for **\$1,100** per patient admission.



The Scope of the Cyber Threat

- Today, **1 in 13 web requests** lead to malware (Up 3% from 2016). ([Symantec](#))
- Malware and web-based attacks are the two most costly attack types — companies spent an average of US **\$2.4 million** in defense. ([Accenture](#))



The Scope of the Cyber Threat

- **69%** of organizations don't believe the threats they're seeing can be blocked by their anti-virus software. ([Ponemon Institute's 2017 Cost of Data Breach Study](#))
- By **2020**, we expect IT analysts covering cybersecurity will be predicting five-year spending forecasts (to 2025) at well over **\$1 trillion**. ([Cybersecurity Ventures](#))

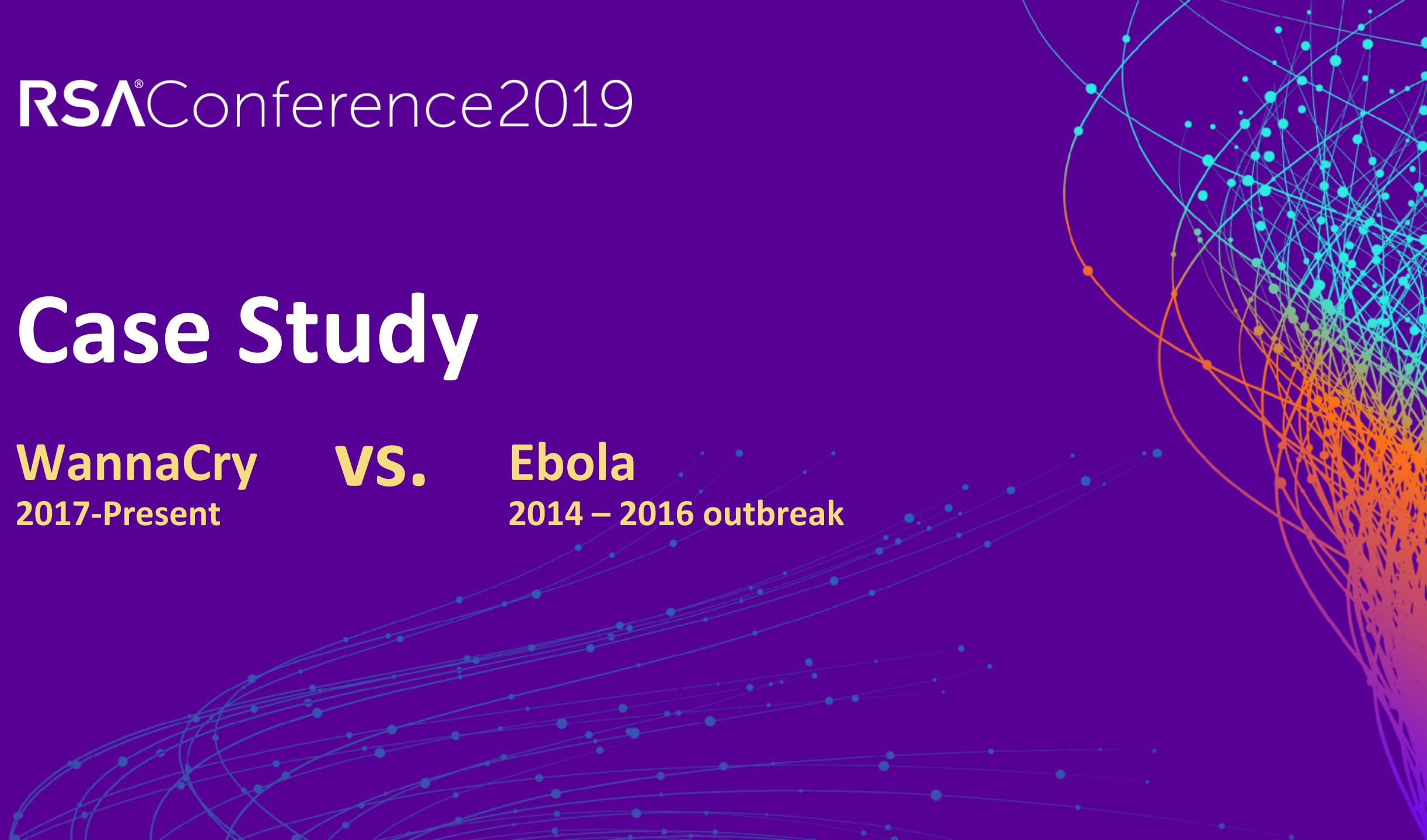


Case Study

WannaCry
2017-Present

VS.

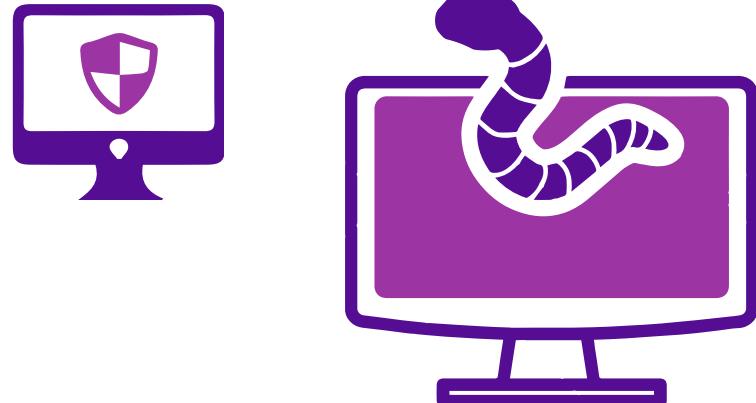
Ebola
2014 – 2016 outbreak



Case Study: WannaCry vs. Ebola

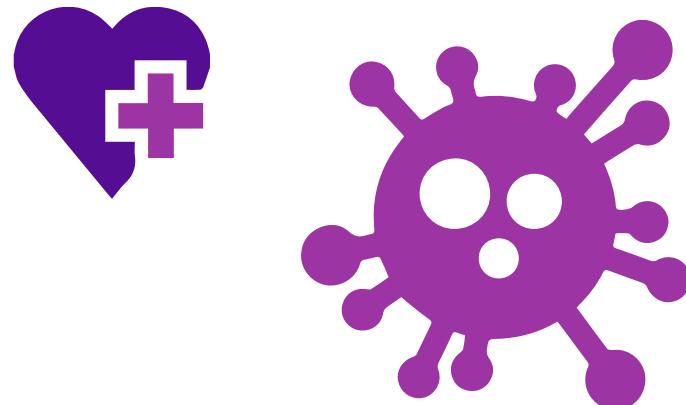
WannaCry 2017-Present

- Organizations poorly prepared to deal with worm using NSA exploits
- Discovery of a “kill switch” enabled propagation to be controlled



Ebola, 2014 – 2016 outbreak

- Long period to identify Ebola in an unexpected location
- Poor public health infrastructure and resources to control propagation



Case Study: WannaCry vs. Ebola

WannaCry 2017-Present

- Traditional cybersecurity policies and procedures harmful to managing the outbreak
- Use of outdated technology helped enable the worm to propagate
- Current device patching methodologies need a redesign



Ebola, 2014 – 2016 outbreak

- US Healthcare system inadequately trained/prepared (e.g., Dallas)
- CDC with delayed and perpetually updated guidance
- Personal protective equipment challenging and needs redesign

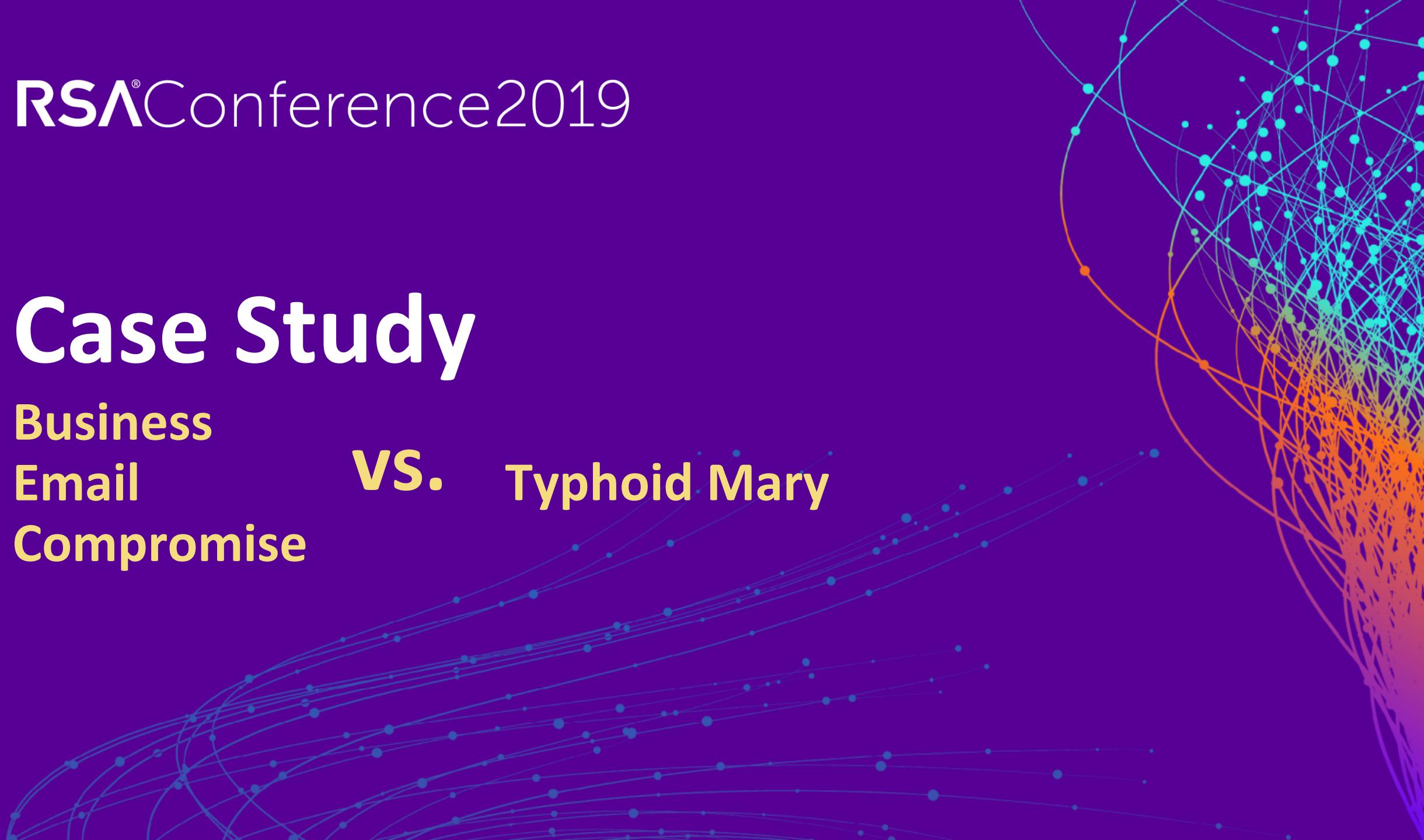


RSA®Conference2019

Case Study

**Business
Email
Compromise**

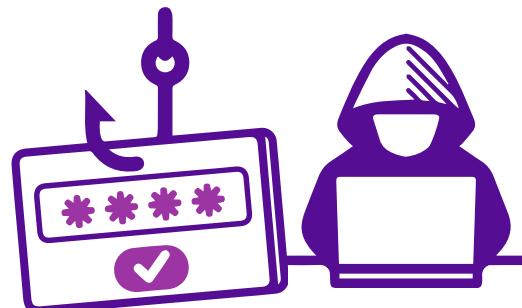
VS. **Typhoid Mary**



Case Study: BEC vs. Typhoid Mary

Business Email Compromise

- Targets employees in positions of power or influence
- Victims commonly believe that it couldn't/didn't happen to them
- Often, BEC attacks are aimed at compromising other targets using the victim's trusted account



Typhoid Mary

- Worked as a chef, which enabled spread of the virus
- Mary Mallon never believed that she was a typhoid carrier
- Mary Mallon was an asymptomatic carrier and exhibited no symptoms



Case Study: BEC vs. Typhoid Mary

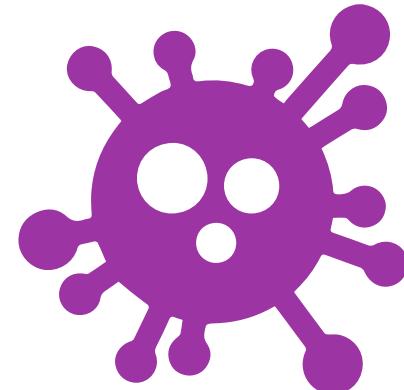
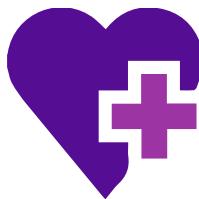
Business Email Compromise

- User's poor email security habits lead to compromise
- Users often return to old habits after a breach



Typhoid Mary

- Failure to wash hands increases the probability of typhoid infection
- Mallon took a position as a cook under a false name after promising not to





AMERICANS' HAND HYGIENE HABITS

A majority of Americans are getting caught dirty-handed when it comes to their handwashing habits. A survey by SCA, a global hygiene company, uncovered that consumers understand the importance of hand hygiene but their practices may be grossly exaggerated.

71%

say they practice good hand hygiene and wash their hands regularly

58%

have witnessed others leaving a public restroom without washing their hands

20%

witnessed restaurant employees

35%

witnessed co-workers

33%

witnessed friends

MORE THAN HALF

do not wash their hands after riding public transportation, after using shared exercise equipment, or handling money

39%

do not wash their hands after sneezing, coughing or after blowing their nose

On average, you come in contact with 300 surfaces every 30 minutes, exposing you to 840,000 germs*

*According to 2011 Tork® Report

On behalf of SCA, KRC Research conducted 1,000 online interviews among a nationally representative sample of adults in the U.S. from October 4 to October 7, 2012.

The State of Cyber Hygiene



- **90%** of cyber breach claims were caused by human error¹
- **91%** of successful cyberattacks start with a spear phishing email²

¹ Decode the Human Threat Willis Towers Watson

² 2016 Enterprise Phishing Susceptibility and Resiliency Report PhishMe

The State of Cyber Hygiene

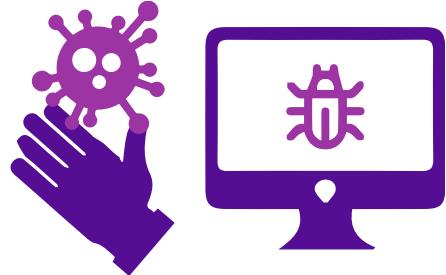


- In 2017, spear-phishing emails were the most widely used infection vector, employed by **71%** of those groups that staged cyber attacks. ([Symantec](#))



- **65%** of companies have over **500 users** who never are prompted to change their **passwords**. ([Varonis](#))

Takeaways



- Both the medical and cybersecurity fields have issues arising from poor user hygiene



- The lack of global epidemics means they're doing something right



- What can we apply from hospital infection control to our field?

RSA® Conference 2019

How Do We
Solve It?



How is Physical Hygiene Promoted?



- Gentle reminders (signs, etc.)
- Proactive gestures (providing hand sanitizer, wipes, etc.)
- Regular checkups
- Incentives for preventions (health awareness programs, etc.)



How Can We Improve Cyber Hygiene?



- Gentle reminders (signs, etc.)



- Proactive gestures (providing free USB drives, AV subscriptions, etc.)

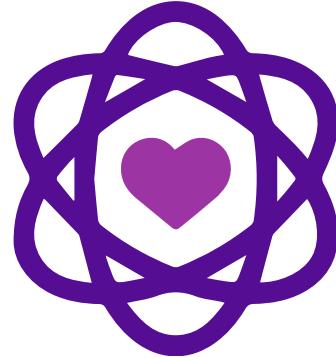


- Regular checkups



- Incentives for preventions (cyber health awareness programs, etc.)

Effective Cybersecurity Training



Has to be
relatable



Has to account for
culture



Has to be **human**
centric not policy
centric

Apply What You Have Learned Today

Next week you should:

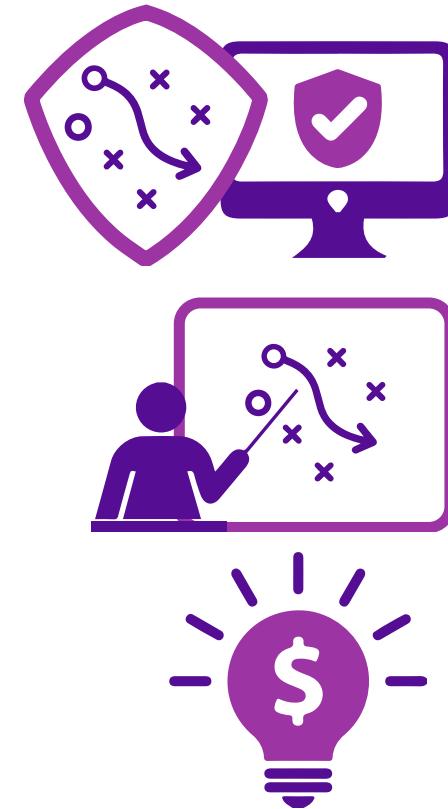
- Evaluate how your organization is promoting good cyber hygiene
- Identify aspects of your organization's cybersecurity strategy where behavior change is necessary but difficult



Apply What You Have Learned Today

In the **first three months** following this presentation you should:

- Create user stories mapping good cybersecurity hygiene to good personal hygiene
- Develop a strategy for building training focused on behavioral change
- Identify and produce low-cost, high-impact cyber hygiene aids



Apply What You Have Learned Today

Within **six months** you should:

- Build cyber-awareness training modules designed to drive behavior change through making risks and best practices relatable to users



RSA® Conference 2019

Questions?