# Are people the problem?

{ The human aspects of information security

- What factors are influencing people to not comply with information security/data protection best practice?
- How can we promote positive behavioural change?
- How can technological solutions best support change?

- Esquire - March 2020:

  *"**Whether the coronavirus pandemic lasts for two months or two years, the way that we live and work will be altered irrevocably**"*

- However, has the pandemic fundamentally altered this issue?

# The elephant in the room

1) **$1.8 million** lost every minute to cybercrime
2) Security breaches cost companies approx. **£20 every minute**
3) Approx. **£1 million** is lost every hour to phishing attacks
4) **More than half** of businesses admit that employees are their biggest risk to their information security
5) 65% of data security incidents reported to ICO in 2018 resulted from 'incorrect disclosure of data', as opposed to 13% caused by malware, ransomware, phishing and brute force attacks
6) Two-thirds of all data breaches reported to ICO in 2019 resulted from 'human error'

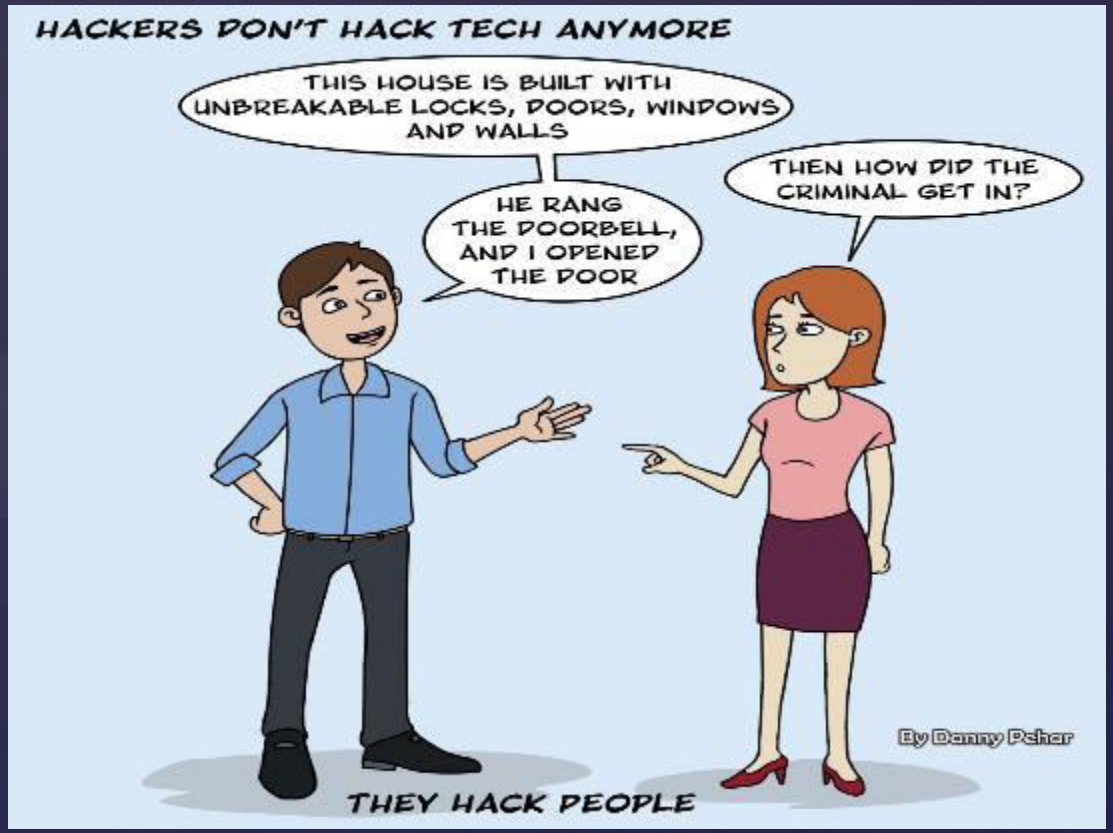
# Some numbers…

- Cyber threats are very costly
- Majority of threats come from human error
- These problems cannot be tackled with more technology alone

# What do those numbers tell us?

- The changes to the world of work have increased the cyber attack surface exponentially for most organisations
- The pandemic brought specific threats to the fore, and increased them
- The speed and frequency of attacks is accelerating constantly

# The problem is growing


HACKERS DON'T HACK TECH ANYMORE
THIS HOUSE IS BUILT WITH UNBREAKABLE LOCKS, DOORS, WINDOWS AND WALLS
HE RANG THE DOORBELL, AND I OPENED THE DOOR
THEN HOW DID THE CRIMINAL GET IN?
By Danny Pehar
THEY HACK PEOPLE

1) May 25th 2018 was the “finish line”
2) It’s an additional – and unwanted – burden
3) Over-reliance on tech solutions
4) Lack of understanding
5) “It’s not my job”
6) Lack of training / poor training

# So why don’t people comply?

**People are the problem**

**BUT**

**They are also the solution**

# So where does this leave us?


# How do we promote change?

1) Research has shown that making training personally relevant enhances its efficacy
2) Raise awareness and understanding
3) Understand the business needs

# 1) Make it personal

1) Cyber security threats are constantly evolving – policies need to adapt accordingly
2) One size does not necessarily fit all
3) No more “ivory towers”
4) Make it intelligible and applicable

# 2) Update policies and procedures

1) Only 11% of companies continuously train employees to recognise cyber threats. 52% of companies only train once per year
2) Training should be ongoing and evolving
3) Understand and employ approaches from behavioural science – “nudging”

# 3) Continuous training

1) Identify the key factors influencing your strategy
2) Learn from other organisations and disciplines
3) Iterate your approach – “fail fast” and adapt
4) Make it relevant and intelligible

# 4) A clear strategy is key

1) At a very fundamental level, you can make more progress towards long-term cyber security solutions if you take the time to understand the problems and their causes, rather than simply trying to solve them
2) Be flexible – it's not all about you
3) Try to say "Yes, if…" rather than "No"

# 5) Start with "Why?"

# How can tech help us?

1) Horizon scan
2) Have a clearly articulated business need
3) Use tools that support behavioural change
4) “Data protection by design”

# Focus on what tech is for

# In conclusion

- Staff can be the single most significant cyber security risk factor but also the key ally in achieving compliance
- The solution is a “whole organisation” approach – not solely the remit of information security/data protection

# Thank you

Jonathan Craven
Privacy and Compliance Lead (UK), iRhythm Technologies Ltd