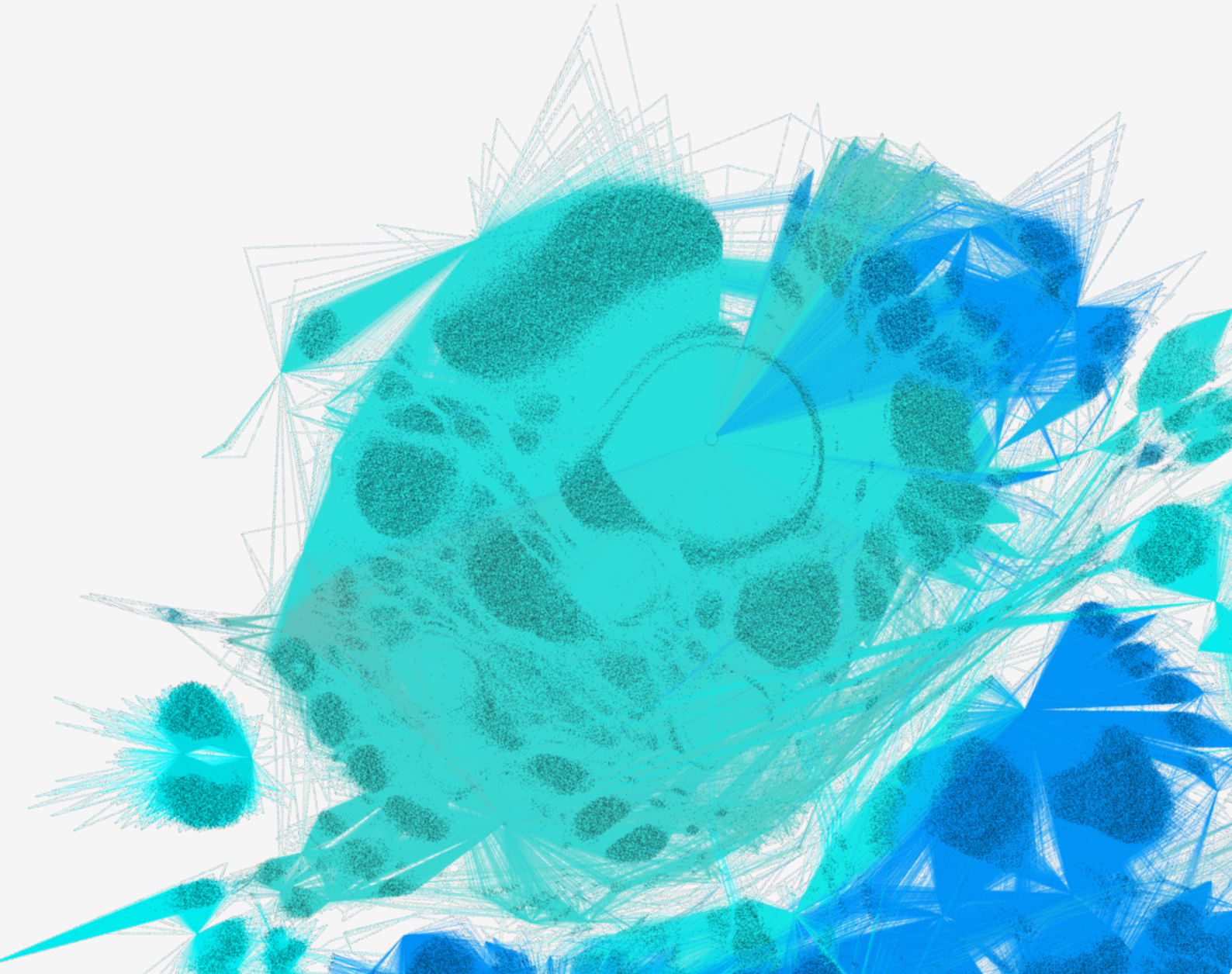
PERSONA REPORT

Head in the Clouds:

A study into User Behaviour to Better Understand Insider Threats



Introduction

These are remarkable times. Organisations across the globe have been forced to come to terms with radically new ways of working, whilst in some cases battling an invisible enemy that represents an existential threat to their business. Against this backdrop, IT and cybersecurity leaders have been working to support the rapidly evolving needs of their users whilst tackling a surge in threats.

Cyber-criminals have responded with predictable agility to the unfolding crisis. As Trend Micro and others have documented, they're using localised COVID-19 lures to trick users into giving away their log-ins, unwittingly downloading malware, even wiring corporate funds to fraudsters. Google alone claims to be blocking over 240 million COVID-themed spam messages each day.

The majority of these threats target what is often described as the weakest link in the enterprise security chain: its users. This was true before the pandemic, and it will still be the case long after.

As flexible working becomes more widespread and digital transformation broadens the corporate attack surface, organisations are increasingly exposed to attacks targeting their users. The use of AI by cyber-criminals also represents a coming storm. Trend Micro predicts deepfakes will be the next frontier of enterprise fraud.

In many cases, users also expose their employer to threats unprompted, through negligence and risky behaviour. Verizon claims 22% of all breaches last year were down to human error such as misdelivery of emails and misconfiguration of cloud systems.

13,200
employees

27
countries

Profiling employees

To help IT leaders better understand the cyber risk to corporate systems and data from their employees, Trend Micro commissioned new research to answer three key questions:

- What are employees doing in the cloud?
- Why are they behaving in this way?
- How do you motivate them to stop negative behaviours?

Alongside interviews with 13,200 employees in 27 countries on their attitudes to corporate cybersecurity and IT policies, we enlisted the help of Dr Linda K. Kaye, Cyberpsychology Academic at Edge Hill University. She worked to profile four key employee personas based on their cybersecurity behaviours.

Kaye explained "Our research on personality profiles has been really helpful for this work, to help us better understand the way individual differences impact on cybersecurity behaviours". In this study we explain each in turn, and make recommendations for IT managers on how to negate bad cloud security habits.

Introducing four cloud security personas

No two employees are the same, or act the same. That's why one-size-fits-all policies and training aren't always successful. Creating relevant personas helps to tackle this challenge. We have identified four key character types: fearful, conscientious, ignorant and daredevil.

Fearful

Fearful employees are anxious about doing something wrong that might expose themselves or their organisation to risk. They are highly accountable for their own behaviour, even if they don't know precisely what cyber risks are out there and how to manage them. As such, they may deploy risk avoidance strategies such as declining tasks or waiting for advice and guidance from others first.

Conscientious

Conscientious workers are well versed in understanding cybersecurity risks and take heed of advice accordingly. They don't just avoid risk but proactively take steps to manage it, such as using VPNs for accessing external sites. They are also highly accountable for their own behaviour and mindful of their role in protecting the organisation.

Ignorant

Ignorant users are a key risk for organisations due to their lack of cyber awareness and absence of accountability for their own behaviour. They are careless and take risks such as using public Wi-Fi on work devices, although their limited awareness of risk means they may not understand the significance of these actions.

Daredevil

Daredevil employees display a similar carelessness and lack of diligence as ignorant users, although in their case it is not driven by ignorance but recklessness and perceived superiority. They have no regard or accountability for their own behaviour and instead attribute this externally to others.

Advice for IT leaders

Consider the following steps to help minimise cloud security risks stemming from employee error or negligence:

Fearful employees will benefit from training in how certain behaviours lead to specific risks, and demonstrations of proactive behaviours that can make them more cyber-secure employees. Simulation environments can be useful here, allowing fearful users to try things they wouldn't normally do. Tools installed onto user machines that test files/URLs and provide real-time feedback are also beneficial for learning, as is actionable threat information. These personas would benefit from a buddy or mentor from the conscientious group, alongside a "blame-free" culture in the organisation.

Conscientious employees are ideal individuals to team up with others as security champions. Good practices should be recognised, rewarded and used as an example for others to follow.

Ignorant users need basic training to begin with, followed by practical advice on how to mitigate risk. Keeping instructions simple is key, perhaps using gamification techniques and simulation exercises can be useful to engage the individual. Additional interventions may be required to help them truly understand the consequences of risky behaviour.

Daredevil users will need to be handled in a similar way to ignorant personas. However, they may be less persuaded by authority and so other tactics are required to change behaviour, such as award schemes for compliance. In extreme cases, managers may need to restrict access to sites and applications and use additional controls like DLP to mitigate risk in the meantime.

There is no right or wrong way to do this as each organisation will have their own unique challenges. Security teams must be enablers of positive change by demonstrating, encouraging, motivating and challenging in fun, positive ways about the risks. We recommend IT teams treat obstacles as an opportunity to learn and, most importantly, don't make end-user security awareness training a punishment for doing something wrong.

TREND MICRO™