Insight Space

cyber insights programme

nccgroup

Technical Viewpoint

# The insider threat: understanding the human behaviours that impact cyber resilience

Ollie Whitehouse

# Introduction

**When a cyber attack happens, it can be easy to point the finger at users who may have been the trigger or inadvertently involved in a breach, but playing the blame game is both toxic and often counterproductive. Instead, it's important to dig into the human factors and behaviours that lead to a cyber security incident.**

Often, the underlying cause can actually be a combination of human, business process and technical factors. Research into human factors and the insider threat continues to be an emerging and evolving field of study in cyber science. Within this research, it is recognised that despite the often-held misconception that systems would be far more secure without users, people can indeed be the strongest link, especially when you educate them about their role in keeping the organisation secure.

# Taking into account the behaviours of people

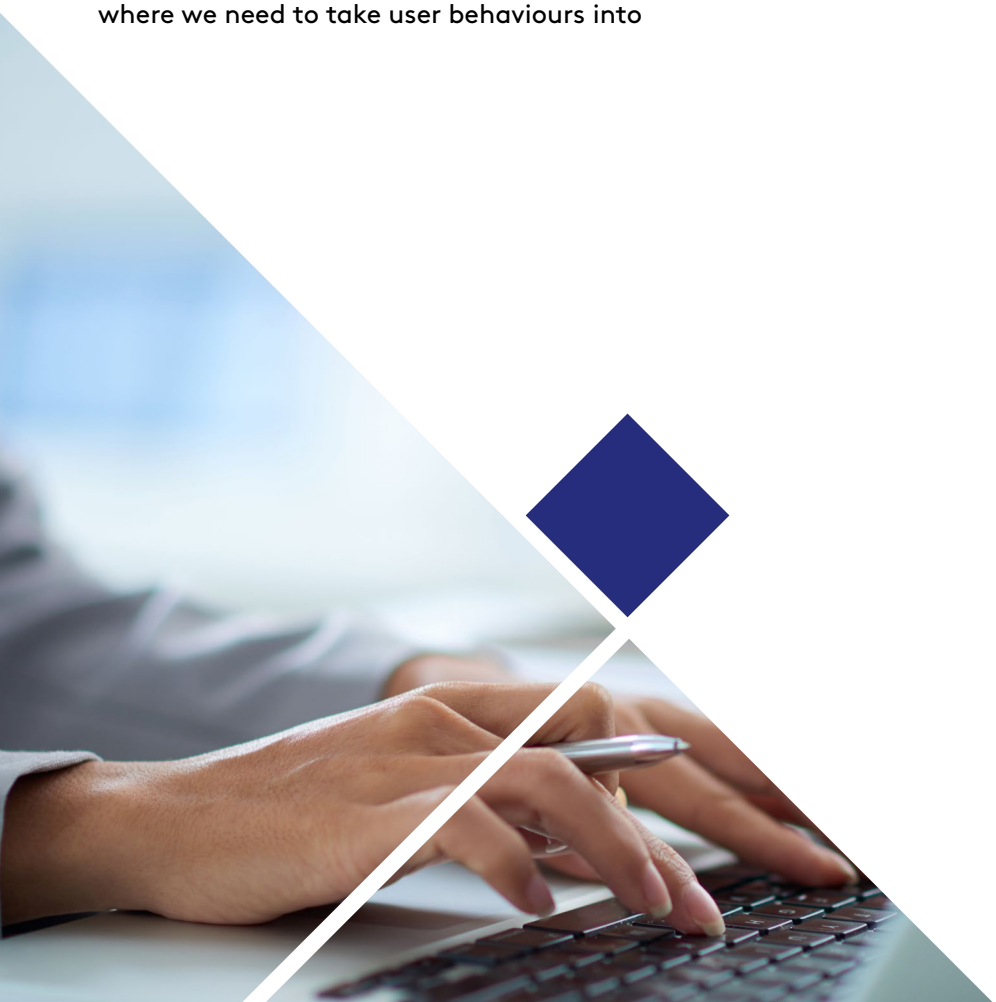
## With the proliferation and evolution of phishing emails, it's becoming harder for users to spot a malicious link or attachment, especially when they come from a convincing contact or colleague.

Read any serious phishing research and the statistics will show that with any user population of any reasonable size, the chances are that more than 10% will fall victim to phishing attacks.

This is one example where user behaviours need to be taken into account. If your security strategy relies on the fact that people won't click on links or open attachments, despite this being crucial in roles such as recruitment – then you quickly see how critical it is to have a viable resilience strategy. This strategy should be airtight and ensure that if and when a user becomes a security weakness, you can prevent, detect or otherwise mitigate malicious activity.

Similarly, various research shows that if you put too much temptation in front of someone, the risk that they will take advantage for personal, ideological or other gain increases. This is another example where we need to take user behaviours into account. If your security strategy solely relies on the integrity and stability of your staff, you can see how this might quickly unravel in the real world, and the possibility of a truly malicious insider compromising your organisation.

Finally, when thinking about cyber security and information technology professionals, it's important to understand our own biases for solutions. The University of Bristol's Decisions and Disruptions game, which was developed to analyse the decision-making behaviours of various stakeholders across a business, proves that a technology-focused bias exists. Results from the game showed that cyber personnel and leadership are technology-driven, whereas those in IT were the only group to materially consider human factors and intelligence gathering, both of which are just as crucial as technology when it comes to formulating robust security strategies.



# User-centric security design

## Users are not cyber security experts for the most part and asking them to make decisions which oscillate between everything is fine and everything is on fire by simply clicking one of two choices next to each other is going to raise the table stakes accordingly.

This is where a user-centric security design can prove effective. Put simply, this is where the flow of the process, user experience, tools and day-to-day operations are considered.

**While there are various considerations, the key ones to prioritise include:**

- How onerous are security controls on the practices and processes of various business functions? If too onerous, they will be worked around and undermine security no matter how secure.
  - The Royal Holloway University of London's Information Security Group delves into this more in their paper 'Inclusive Security: Digital Security Meets Web Science'.
- How fit for purpose are the business processes? Overly complex processes during periods of high cognitive load can often fail.
- How intuitive or easy is it to make mistakes which result in security consequences? For many, this could be the user experience, which has been explored in more depth in the following publications:
  - The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home
  - Usability Research in Support of Cyber-Security

**Practical examples of user-centric security design vary, but a couple of examples include:**

- Virtual desktop infrastructure (VDI) – cloud or on premise – which can be used for various discrete use cases, such as web browsing, email or privileged user function. This approach has a number of benefits:
  - The user experience is familiar and can be akin to native applications
  - Allows compartmentalisation which provides resilience and detection opportunities
  - Provides the organisation the ability to apply variable policies and controls
  - Can be ephemeral precluding persistence by threat actors
- Privileged access management (PAM) provides real-time and auditable access to systems and applications in an automated manner:
  - Easy-to-use from a user perspective
  - Prevents a build-up of long-term high privileged access on particular users
  - Provides an audit tail which provides detection opportunities

With more employees working from home than ever, this approach will be even more helpful in bringing the user's machine into an environment where maximum resilience benefits can be provided without impacting functionality or the user experience.

# Monitor host, application and user behaviours

## Managing the risk from the insider threat has its basis in strong identity and access management (IAM), coupled with behavioural monitoring to identify suspicious or outright malicious behaviour.

However, this root of identity and access management and monitoring shouldn't solely be about the people of a system. With many more machine-to-machine interactions and thus application-to-application interactions, it is equally critical to consider these as part of the overall solution.

This widening of the scope is why we have seen the original acronym of user behaviour analytics (UBA) expanded to user and entity behaviour analytics (UEBA). Or more simply put, the application of statistical modelling on a set of properties to detect those activities that might be suspicious or malicious – often described as analytics or machine learning.

**For this type of strategy to be effective, there are several factors to keep in mind:**

- Telemetry coverage and context: this is our eyes on the problem. If we can't see it happening and don't have context, it's near impossible to detect systematically.
- Analytics with various horizons: this is our brain for deciding what is abnormal. For this to be effective, we need various time horizons on the models. Some will be minutes, while others are months. This approach ensures that we can detect both the long and slow attacks, as well as the smash and grab breaches.
- Alerting and context: this is what drives our response to allow us to quickly contain and remediate issues.

**This monitoring then occurs across the full stack:**

- Hosts: examining which hosts are communicating to which, on what protocols and by how much.
- Applications: looking at which applications are communicating to which, what other processes are they spawning, how much data are they sending and receiving over the network and where to.
- People: assessing which people access which applications or data sets at what times of day, in what quantities and what they are doing.

**This visibility allows organisations to detect what is anomalous and what should be classed as abnormal behaviour. This is the crux of UBA and UEBA – that is:**

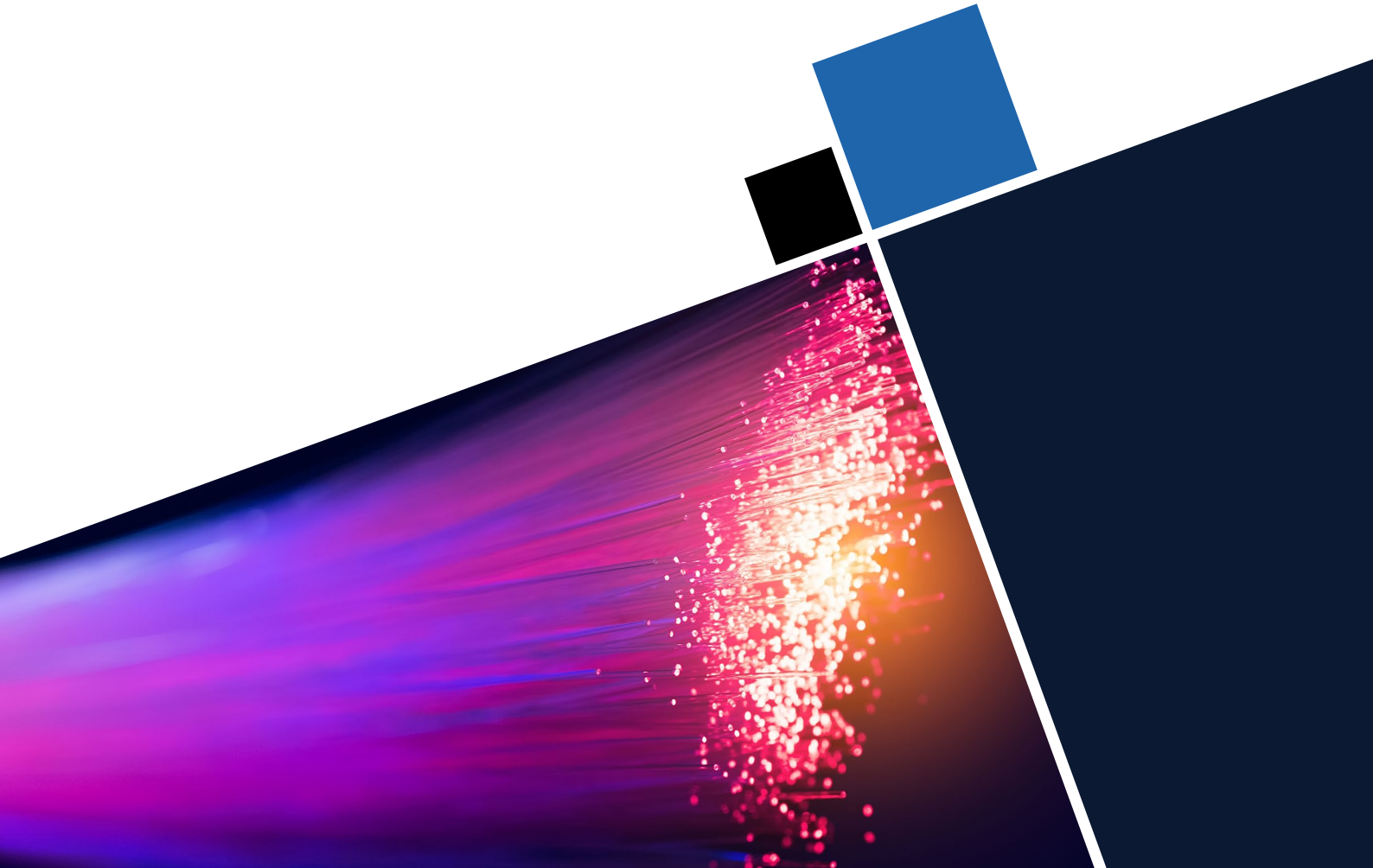
- Strong identity of host and user
- Comprehensive telemetry coverage across network, host, application and user behaviour
- Analytics working various time spans and horizons using technologies (depending on use case and coverage), such as Apache Kafka, Microsoft Sentinel or Splunk

However, the complexity involved in building, maintaining and responding is still beyond the sustainable ability of many organisations in reality. This is why managed detection and response (MDR) services are such a valuable offering in the cyber resilience space.

# Conclusions

## The insider threat takes many forms – from the truly malicious to the otherwise honest yet complicit through no fault of their own. As the world moves to a post-pandemic model of working, organisations should consider how they think about the insider threat across their people, processes and technology.

Most importantly though, organisations should ensure that the burden is not put on the user. Creating a culture of openness and awareness as opposed to one of blame is crucial. Getting the balance right between this and technology can be difficult, but it is how one can achieve true resilience.



# Insight Space

cyber insights programme

nccgroup

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss managing your people risk, speak to our team today.

**+44 (0)161 209 5111**
**response@nccgroup.com**
**www.nccgroup.com**