Q&A

Why leaders must prioritise mitigating human risk in the age of AI

The risk of artificial intelligence in the field of cybersecurity is an increasingly pressing concern. Mimecast's senior manager of product management, **Dr Kiri Addison**, explains how firms can better manage human-risk in the age of AI

The human element of cyber risk is emerging as the biggest cybersecurity strategy gap in the age of AI. A Forrester report predicts that 90% of data breaches in 2024 will have a human element, up from 74% in 2023. Yet, Mimecast's 2024 ***State of Email & Collaboration Security*** report found that employees' ability to recognise cyber threats was a notable concern for organisations. Businesses must take a proactive approach to mitigating human risk and invest in employee training to ensure their defences are strong against cyber attacks. Dr Kiri Addison explains why it's important to remember humans remain the most likely victims of, and tool against, AI-powered cyber attacks.

Q Where does the issue of AI and cybersecurity currently sit?

A AI in cybersecurity is something that we've spoken about for a long time, but in the last couple of years, the explosion of generative AI (GenAI) and ChatGPT has really brought it back to the forefront. You've got the positive side of it, which is that it's going to have a beneficial impact on cybersecurity, but there's also the negative side.

There's a lot of talk about the negatives and what may happen in the future. But we're not necessarily seeing everything people seem to be talking about, like the vast amounts of phishing emails generated by AI or a surge of malware developed by AI.

Q What are the real and present risks?

A There was a takedown recently of a group in the UK that was reportedly using GenAI to create a vast library of phishing web page templates. Security has always been a bit of a cat and mouse game, but GenAI can assist criminals in terms of scaling up their operations, helping them evolve even more quickly.

The other trend on the rise is the use of deep fakes in cyber attacks. The technology hasn't been quite good enough to launch a serious financial attack – but now it is. There was a recent incident in Hong Kong in which criminals utilised deep fake technology via a Microsoft Teams call to persuade an employee into making a huge wire transfer using fake footage of their CFO.

We're seeing an explosion of ransomware attacks, extortion, phishing, deep fakes, all increasing alongside each other. It's all part of the same threat landscape, which was already getting more complex.

Q It's a tricky time to be a CISO. What are they looking for?

A I think it's all about risk. People don't have endless budgets, especially at the moment. So, it's making the most of the budget that you do have. A priority is understanding why your organisation would be attacked. What is that attack going to look like? How would that play out? And how likely is it to happen? You need to have a good understanding of your own organisation, but also the threat landscape as well. That's where the threat intelligence element comes into it.

Then, you need to understand your defences. What do you already have in place to address some of these risks and mitigate them? Where are the gaps that exist? And what would the impact on your organisation actually be if one of these attacks were to succeed? Once you have that information, you can prioritise and focus on the areas you've identified. This requires reliable data and information to help you take a risk-based approach.

> **Businesses must take a proactive approach to mitigating human risk and invest in employee training to ensure their defences are strong against cyber attacks**

Q Where are those risks most commonly seen?

A The human element is a significant one. Whether that's opening a malicious file or a link you've just been sent in a new collaboration tool, these actions may ultimately end up leading to a ransomware attack on the system. Or maybe you've been sent a compromised email spoofing your boss and it's asking you to respond with some sensitive data. There's a whole range of different attacks that could happen, but a lot of them require a human to be tricked into taking a certain action.

For a long time, humans have been blamed for making mistakes, but actually I think we need to look at them as a very critical part of a strong defence strategy. You can see them as a risk, but you can also see them as a control. With ongoing comprehensive training, they can recognise and be suspicious of the increasingly sophisticated attacks they will encounter. Then, you can rest assured your human firewall is all set and working. But like any tool, if it's misconfigured or not switched on properly, then it isn't going to do as good of a job. The approach that we're encouraging is to identify which individuals need the most support and tailoring your training towards that.

Q How can organisations form a comprehensive cybersecurity strategy to protect both employees and businesses?

A Mimecast offers customers an awareness training product that interacts with end users, testing their ability to recognise and avoid risks. Mimecast can help companies send out test phishing campaigns to employees to see who will interact with them positively and negatively. This identifies which employees are in need of further support to avoid falling victim to real attacks.

Being proactive, rather than reactive, is the necessary response to human risk in the age of AI. This plays into the risk-based approach: identifying your areas of weakness upfront and thinking about how you're going to prevent and also recover from this. Nothing is 100% certain, so you still have to think of the element of recovery. In the uncertainty of the AI-driven cyber threat landscape, human risk is one factor businesses can take a combative approach towards, by addressing weaknesses ahead of time and investing in regular training to help employees remain vigilant, should they encounter a threat.

Learn more at mimecast.com

Visit Mimecast at InfoSecurity Europe 2024 at Stand E55

mimecast