Q&A

Awareness is not action

Employees broadly understand the implications of cybersecurity and how their behaviour could impact their company's safety and yet still take actions that could put it at risk. Mimecast EMEA field CTO, **Johan Dreyer**, explains how employees need better support to maximise their cyber hygiene and how businesses can provide it

Q Why do so many organisations struggle to have a culture of cybersecurity?

A It's quite simple. Business leaders do understand the potential risks associated with lax cybersecurity. Quite apart from their regulatory commitments, there are significant costs incurred as the result of an attack, from systems recovery to business downtime. Business owners are acutely aware of the need to make their organisations as cyber secure as possible.

Findings from our *State of Email Security 2023* report have shown that almost every business (99%) offers some form of cybersecurity awareness training to its staff. And yet, in the past 12 months, three out of four have seen an increase in email-based threats, two-thirds have been harmed by a ransomware attack and 80% believe their company is directly at risk as a result of careless or negligent employees.

This negligence is not down to laziness, a devil-may-care attitude or even malice. On the whole, employees are as keen as their bosses to be safety conscious when it comes to cybersecurity. The problem is that cybersecurity training as it stands is rarely tailored to the needs of the employee. Our *Collaboration Security: Risks & Realities of the Modern Work Surface* research found that one in five employees skip all the cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment, for example.

1 in 5

employees skip all the cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment

Mimecast, 2023

Q How do we bring employees' understanding of cyber risk closer to that of the business?

A The same logic that you might apply to clicking on a dodgy ecommerce or social media link needs to apply to the corporate culture. As a consumer, you know you can find yourself in a position where your personal life is severely impacted if you're not thinking about what you're clicking on. The more we can bring that consumer understanding into a work context, the more we'll have the empathy and understanding of colleagues who may otherwise not have been cyber aware.

We aren't expecting employees to become cyber experts, but that shouldn't mean they're ignorant of good security practice or what a good standard looks like. When we deliver awareness training, we need to design engaging content that connects those personal experiences to the behaviours we would like to promote.

Say an employee is working remotely at a coffee shop. Do they go to get more hot water for their coffee and leave their laptop unattended with the screen open, meaning someone could gain access to sensitive information? In the same scenario, would they leave their personal banking signed-in? These are things we need people thinking about.

Q Good cyber hygiene isn't just a defensive measure. How do businesses with actively cybersecure employees gain competitive advantage?

A Organisations with great cyber risk posture, a strong security culture and demonstrable accreditation in protecting their people, value chain and shareholders are well positioned to outperform their counterparts. For example, many organisations will ask to review a potential supplier's cyber credentials and this will play into the ultimate award of contracts.

Impacts of cyber attacks on an organisation can include business interruption resulting in loss of production, direct financial impact as a cost of recovery and loss of reputation within your customers, suppliers and shareholders. These are serious consequences.

Q Cybersecurity is a highly regulated, complex set of policies. How do we translate that to the average employee so they can absorb and understand their role?

A It's our responsibility as an organisation to create links between action and consequence – and showcase them. This goes back to company culture. There is a policy-and-compliance approach where you're presented with a long document with lots of dos and don'ts and a space to sign at the bottom. It covers compliance and audit requirements.

The reality is that people have information overload. The likelihood that someone has fully read through and understood that document is low. Also, the speed the world moves at means these documents struggle to stay current.

It's important to use relatable, storytelling-driven approaches. There is much more demand today for impactful, engaging commentary than there might have been five or 10 years ago. Content that is topical and relatable and contains a personal experience that is still connected to the world of work is key.

We can't get away from a compliance-driven approach entirely. We must make sure our reports to the market are accurate and safe. Agreements won't be going away any time soon. But above all, we have to connect with the employee's sense of purpose – their 'why' – and that means connecting their personal safety online with that in the workplace. Making them aware of how good digital decision-making can have a positive impact on the organisation and how the reverse can also be true.

Q When threats are evolving and becoming more sophisticated, how can a business create a culture that is safe but accepting of the fact that no-one and no policy is 100% bulletproof?

A Business owners must foster an environment where speaking openly is encouraged. I've seen organisations that have managed to turn a potentially negative situation into a positive. Blaming, shaming and whistleblowing are counterproductive – fear doesn't drive good cultural behaviour and that creates poor outcomes. By encouraging openness and accountability without blame, the business can learn, fix and move on.

> “Organisations with great cyber risk posture, a strong security culture and demonstrable accreditation in protecting their people, value chain and shareholders are well positioned to outperform their counterparts

Q How can businesses promote their cybersecurity preparedness as a positive brand attribute?

A I'd love to see accreditation similar to the Red Tractor for British produce or the B Corp certification for ongoing ESG commitment. We do have some level of this with programmes such as the ISO 27001, SOC2 Type 2, TISAX and various other accreditations. But most of these are controls focused, require certification on a periodic basis and the scope can vary drastically from organisation to organisation. These are all great starting points but don't always accurately represent the culture of cyber risk awareness that you've worked hard to promote.

However we approach cybersecurity – and we must because the costs involved in not doing so are too great from multiple angles – we must do it with our employees at the heart of the process. We can't remove all risk; mistakes will be made. But if we invest in our people, put the right training in front of them and remove barriers to compliance, our employees will feel empowered to make the right decisions and feel supported throughout their careers and cybersecurity journeys.

To find out more, visit mimecast.com/this-is-personal

mimecast™