DIGITAL EDGE CLUB

2020 PREDICTIONS: WHAT LIES IN STORE?

Trends, insights and strategies from some of the UK's top fast-growth organisations

2020 | JANUARY

WWW.DIGITALEDGE.CLUB

THE DISCUSSION TOPIC

2020 Predictions Evening: What's Next?

Although predictions are notoriously wily things, the Digital Edge club does thrive on debate and, to this end, there is nothing like a bold prediction.

Our predictions event is the most popular in our calendar and this year we were no less bold. We debated whether Generation Z will be a catalyst for developing the workplace of the future. Wondered what ethical and security questions AI will ask of us in the forthcoming decade.

And we returned to the knotty topics of data and of tech debt.

To make sense of these predictions and dilemmas, Digital Edge convened some of London's most forward-thinking business leaders for its first session of 2020.

THE DISCUSSION

This report has been compiled based on the views and opinions of leaders from some of London's leading organisations, as voiced at the latest meeting of Digital Edge.

OUR SPEAKER

Leading the discussion is Timandra Harkness. Timandra is a technology writer, broadcaster and comedian. She has performed maths stand-up, presented on Radio 4, and written a book.

Now a regular writing and presenting on Radio 4, Timandra has fronted documentaries such as Data, Data Everywhere, and Personality Politics.

She co-hosts FutureProofing, with Leo Johnson, which sees her looking at the future of everything from language to war, ageing to food.

Her book Big Data: does size matter? gives a history of data collection and collation, how it's changing the world, and its shortcomings from politics to health to smart cities.

Combining unusual facts with insight and humour, Timandra looks at how the future will affect business and society. As well as looking at big data, she tackles AI and robotics, and considers topics around our relationship with science and technology.

TRENDS INTO 2020

The evening began with some predictions from our Speaker:

- People are beginning to wise up to the problems around the use of the term "AI" and in 2020 we might find that we need to find a new buzzword to describe this group of technologies.
- GDPR has sparked a little revolution and the march towards greater regulation of the tech industry will continue.
- The boundaries between geopolitics, economics and technology are more blurred than ever. In 2020, we can expect a cyberattack on western infrastructure, probably by Iran.
- Reputational risk with overtake financial risk as the major risk from a technology security breach.

THE QUESTION OF TRUST

Not everyone was convinced by the prediction of greater regulation.

"I'm not sure people really care about trust. I thought Cambridge Analytica was a tipping point, but now I'm not so sure. People still aren't taking their personal data seriously."

"Perhaps on a personal level Cambridge Analytica's intrusion into your data isn't a serious concern, but if we look at it on a political level it is horrendous. One person can't affect an election, but together…"

"The reasons for it are unclear: does it come down to a lack of awareness? Or is it a generational thing? Or about the circles in which you mix?"

"If you're someone who can already imagine how things might go wrong for you, for example, if you have experienced police stop and search, then you are much less likely to trust in how data might be collected and used."

"Cambridge Analytica exposed the fact the notion of privacy has gone. They are not the only organisation doing this. And once it is out there, you can't claw it back. So much is already out of your control."

"People say 'well, I've got nothing to hide, so I don't mind' but I don't see how that is a relevant response. The implication is if you've not got anything to hide, you don't need privacy. The two things are not connected."

TECH TRENDS FOR BUSINESS

Our panel made a number of short-term predictions focused on the needs of business.

- IT used to focus on "tech, process, people". But now we are trying to get these things in the right order: people, process and then the tech.

- There will be a greater focus on IT hygiene: organisations want to "excel at the basics".

- Third-party risk will ramp up massively. In the recent Travelex breach, the experience of the banks with which Travelex worked emphasised what can happen when you outsource services. Organisations will need to focus on how their business resilience is affected by outsourcing.

- Overall, there will be less focus on cyber security and more focus on cyber resilience.

DO WE NEED TO FEAR NATION STATE ACTORS?

The group participated in a lively debate about whether we need to ramp up activity to protect business systems and data from malicious national state actors.

"We don't have the resources or the scope or the budget to protect ourselves against such sophisticated and well-financed attacks, so what's the point?"

"You can't just say 'we'll do nothing!'."

"Nation states aren't interested in my company."

"Yes, they are. You are a prime target because of what you've just said. You are a vector to the others. They will try to find the weakest link in. Even if you are a little fish and they are not interested in your data, they are interested in what you have access to."

SOCIAL ENGINEERING

Social engineering was highlighted as another significant cyber security risk.

"We have to stop thinking in the first dimension trope; sophisticated threat actors are taking alternative routes."

"The reconnaissance involved is incredible. They used to just send out bulk emails and see who fell for it, but attacks are becoming more and more targeted."

"Human intervention is an increasing problem. Capable, comprehensive threat actors are now recruiting people to follow up their activities. People will give you a follow-up call and say, "can you open that email while I talk with you?'. We are living with a new level of threat."

"You might think that exposing one piece of data about yourself is not significant, but it isn't about that single piece of data. It is how all the various pieces are combined. Every piece is ratcheting up your vulnerability to social engineering."

GET THE BASICS RIGHT

There is a renewed focus on getting the basics right – perhaps something that wasn't so fashionable in the era of agile.

"Basic hygiene requires an access management infrastructure; anti-malware provisions; patching when you need to do so; ensuring your servers are correctly configured; undertaking the necessary firewall maintenance. It's just five things, but how many of us can say we are confident we have these measures in place properly?"

"Who has a MDM solution for BYOD in place… that you trust?"

"We're all attracted to the new and shiny. You get all these fancy solutions in, but do you then keep it all up to date? Buying the next toy seems to be preferable to keeping your existing tech updated."

DAMAGE LIMITATION

"How do you limit the damage an incident can do? To be successful, it has to happen in the first two hours of the breach happening. You need to get your systems offline."

"You must come up with a plan: how are you going to respond to an incident? How are you going to contain it? You need to run this game plan with your board."

"You need your board to define a policy on ransomware too. Ransomware is better, faster and more dynamic at what it does. It's probably something we'll all have to deal with in 2020. Has your board made a conscious decision about whether you will pay a ransom? This decision has to be part of your corporate governance scenarios. Because if you wait for an incident to happen before you have these discussions, it is too late!"

"How many people have practiced a ransomware event so you know what to do? Two people. Ransomware is one of the most revalent attack vectors and yet we're all going to deal with it for the first time when it happens!"

"We need to get more CSOs on the board."

THE CONCLUSION

Our discussion considered the different elements that make a successful technology leader in 2019. We considered how to build a team and create the right culture to support your organisation's change objectives.

CISOs, CIOs, CDOs and other senior leaders from organisations such as IAG, Natwest Markets, Zurich Insurance, Bupa Global and select others convened for this meeting of **Digital Edge** at the The Gherkin in London.

To gain the in-depth insights that our guests benefited from, book your place for next time via our website: **www.digitaledge.club**, or contact the Club's director, Philippa Brown at **ms@digitaledge.club** or by phone on **+44 (0) 203 322 6788**.

DIGITAL EDGE CLUB

With the aim of mixing business and pleasure, we believe in providing an exclusive environment for market leaders to network and exchange insights on today's greatest business challenges. Hosted in some of London's most elite venues, an evening with the club promises to impress.

www.digitaledge.club

We would like to thank Verizon Enterprise and the following partners for the support of the Digital Edge Club events and for the partnership with the club

JUNIPER NETWORKS
SKYBOX SECURITY
riverbed The Digital Performance Company
verizon
BlackBerry CYLANCE
VERSA NETWORKS
netskope