EMERGING TECHNOLOGIES

‘This happens more frequently than people realize’: Arup chief on the lessons learned from a $25m deepfake crime

Feb 4, 2025

Arup's Rob Greig: 'It's freely available to someone with very little technical skill to copy a voice, image or even a video.'
Image: Unsplash/Ales Nesetril

David Elliott
Senior Writer, Forum Stories

is article is part of:

- **Here, Arup's Chief Information Officer, Rob Greig, talks about the lessons learned.**
- **Cyber resilience in the face of increasing threats is a critical objective for any organization, according to the World Economic Forum white paper Unpacking Cyber Resilience.**

Early in 2024, an employee of UK engineering firm Arup made a seemingly routine transfer of millions of company dollars, following a video call with senior management.

Except, it turned out, the employee hadn't been talking to Arup managers at all, but to deepfakes created by artificial intelligence. The employee had been tricked into sending $25 million to criminals.

This wasn't a traditional cyberattack, the kind that compromises a company's digital systems. This attack used psychology and sophisticated deepfake technology to gain the employee's confidence.

It's an example of how cybercrime is evolving. At the time, Arup's Chief Information Officer, Rob Greig, said the company had seen the number of cyberattacks rise sharply, along with their sophistication.

This trend is underscored in a World Economic Forum report titled Unpacking Cyber Resilience, which aims to help companies become more cyber resilient.

Here, Greig – who was previously director of the UK's Parliamentary Digital Service – talks about what the company learned from its deepfake attack, and what organizations can do to protect themselves.

Cyber resilience is a critical priority for all organizations. Image: World Economic Forum

What was your first reaction when Arup was hit by the deepfake attack?

The first thing to say is we are attacked every day. I used to do a presentation that described it like this: if cyberattacks were bullets, we would all be crawling around on the floor because they would be coming through the window, thousands of rounds a second.

Organizations like mine – we are on the receiving end of attacks every week. And some are more successful than others. It's really important we're more open and transparent about this.

The more we talk about what is actually happening in our organizations and the impact it's really having on businesses and society and individuals, the more we can do to raise awareness and combat these threats.

People were deceived into believing they were carrying out genuine transactions that resulted in money leaving the organization.

My understanding is that this happens more frequently than a lot of people realize.

Audio and visual cues are very important to us as humans and these technologies are playing on that. I think we really do have to start questioning what we see.

Do you think the distinction you made with the terminology is important – in order to help people understand what happened?

The reality is that this crime has been taking place since history was written down. People have always tried to deceive others for some kind of gain.

What's different today is people are using technology to do that.

Deepfake sounds very glamorous but what does it actually mean? It means someone successfully pretended to be somebody else. And they used technology to enable them to do that.

So what has changed with technology to enable this?

Technology is becoming much more effective, convincing and accessible. It's freely available to someone with very little technical skill to copy a voice, image or even a video.

After the incident, I was curious so I attempted to make a deepfake video of myself in real time. It took me, with some open source software, about 45 minutes.

It wasn't particularly convincing – but it was surprising what can be achieved in such a short period of time.

What are some of the immediate actions an organization can take if faced with this kind of attack?

Firstly, it's about having visibility of what's happening from a technology and cyber and data perspective.

Being able to detect that allows you to respond. For us, the first thing to do was quickly assess the extent of the attack and identify if the entire organization was affected. Were our clients at risk? Were our people or their data at risk?

With that visibility, we were able to very quickly identify that we were not compromised and this was being caused by something else.

Second, it's important to have rehearsed a response, not to a particular incident, but to a general set of incidents that might occur so everyone knows what their role is.

Discover

How is the Forum tackling global cybersecurity challenges?

Show more

What are some other cyber threats that organizations are facing today?

We hear a lot about things like AI and quantum computing, and terms like quantum encryption and how this will change the technology landscape for ever. And it's a huge threat to us.

But the reality is, today, the same issues that we've been facing for the past decade and even longer continue to be a serious risk to individuals and to businesses.

compromise individuals or organizations – and even governments.

Quotes have been edited for length and clarity.

Have you read?

- **The US is drafting new laws to protect against AI-generated deepfakes**
- **4 ways to future-proof against deepfakes in 2024 and beyond**
- **Why cybercrime spikes in times of global crisis**

Stay up to date:

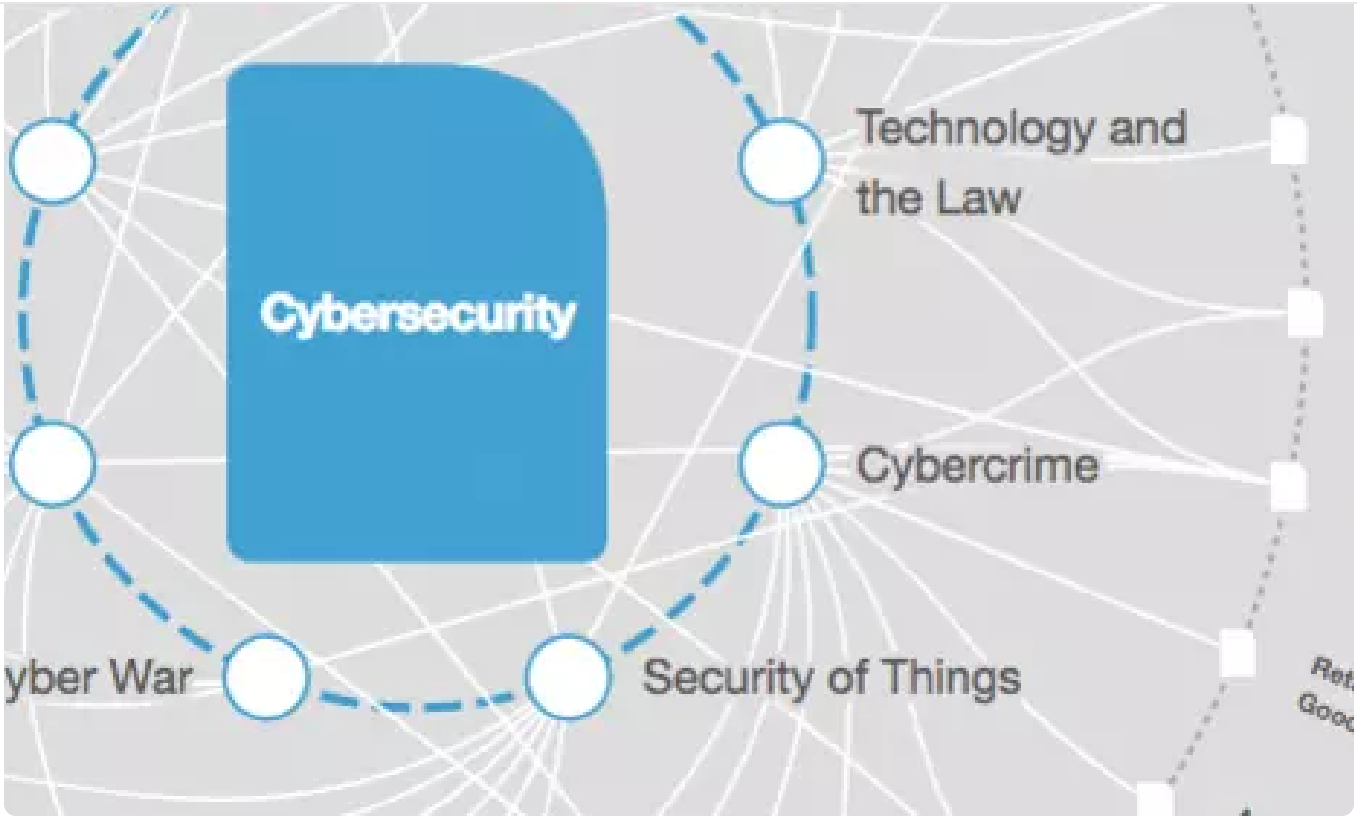
Cybersecurity

Follow +

Related topics:

Emerging Technologies | Cybersecurity

Share:



THE BIG PICTURE

Explore and monitor how **Cybersecurity** is affecting economies, industries and global issues

Bringing you weekly curated insights and analysis on the global issues that matter.

Subscribe today

More on **Emerging Technologies**

SEE ALL

Why we need to make safety the product to build better bots

David Sullivan

August 26, 2025

How blended care, combining therapy and technology, can improve mental health support

Hannes Klöpper

August 26, 2025

y targeting specific industry needs can make Europe an AI powerhouse

3 investment principles for building long-term resilience

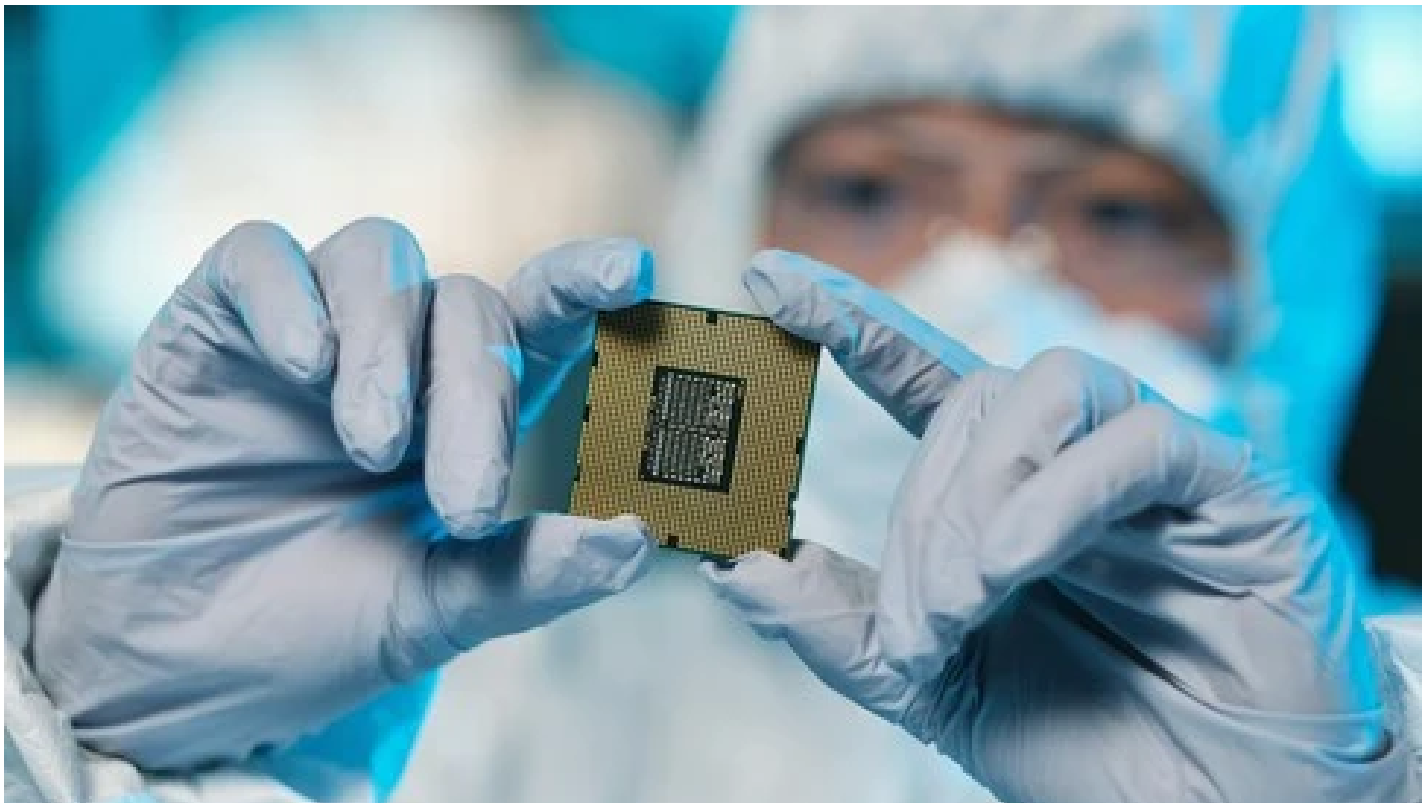
Lim Chow-Kiat

August 21, 2025

How Pakistan’s energy revolution can power affordable, reliable electricity for all

Charles Bourgault and Sarah Moin

August 19, 2025



olicy pivot on chip sales in China. What does it mean for global tech?

cer Feingold