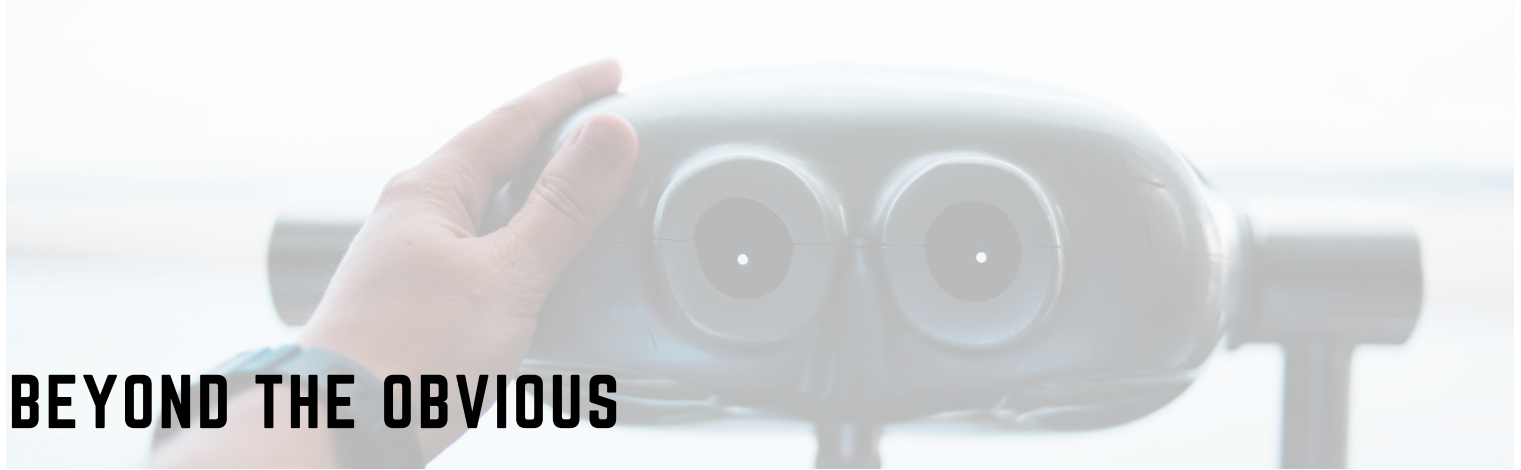


# CYBERSECURITY TALK

*Keeping you up-to-date with cybersecurity issues*



## BEYOND THE OBVIOUS

Bill Collins is relieved. He'd never imagined his company's TV was a security risk.

Another company made the news when hackers broke into their TV system; it started showing graphic scenes from horror films to customers in the reception area.

A few months earlier, Bill had asked his new SOC service company to do a full network audit. And they found a problem with the TV in the customer reception area: it had an easy-to-guess password.

The password had been changed from the default when the TV was added to the network, but the manager had used a temporary password that became permanent.

When the company later moved to a new passwordless authentication system, the TV was missed because it was switched off, waiting for repairs.

Bill asked the SOC team to check every device on the company's premises. A few days later, he saw the news about a hacked TV.

As Bill found, the key to finding these hidden and missing devices is to look beyond the obvious.

Check devices such as vending machines, smart appliances, thermostats, and coffee machines to see if they're connected.

Another potential problem is older devices that only connect to the network occasionally. They might have an obsolete operating system or poor passwords.

After all, no one enjoys being on the evening news for the wrong reasons.



# THE SECURITY RISKS OF CLIMATE CHANGE

Mentioning climate change and cybersecurity in the same sentence might seem odd, but changing weather patterns create new risks that companies can't ignore.

Hackers thrive on disasters and crises. In the US, the Cybersecurity and Infrastructure Security Agency urges people to "remain on alert for potential malicious cyber activity." In the UK, the National Cyber Security Centre has seen hackers use crises such as COVID-19 as a phishing lure.

When staff try to learn more about an event, or whether their area has been affected, they may accidentally visit a compromised site and give hackers a way into the company's network.

Let's say your company has to close because of flooding or a power outage. Staff now have to work from home, and some will still need access to sensitive data.

The critical in-between stage of staff moving from the office to working from home can be stressful if a company isn't prepared.

Hackers also like confusion, as it makes it easier to dupe staff or find a way into a network.

It's not only staff who can be affected. A critical supplier could suffer a fire or outage. Hackers could exploit this by sending phishing emails that appear to come from a supplier to gain access to a company's network.

Third-party software and cloud services are two other areas to consider, especially if they support a company's day-to-day operations. If a climate-related event compromises them, they could cause major disruption.

Including the effects of climate change in your security strategy, protocols, and procedures is vital if you want to keep your systems and data safe as the world's climate changes.

A good place to start is your business continuity plan, which often gets overlooked. Does it cover what to do when staff must start working from home immediately? What about suppliers who are affected by a flood or fire?

Climate change is giving hackers another means of attacking company systems and networks.