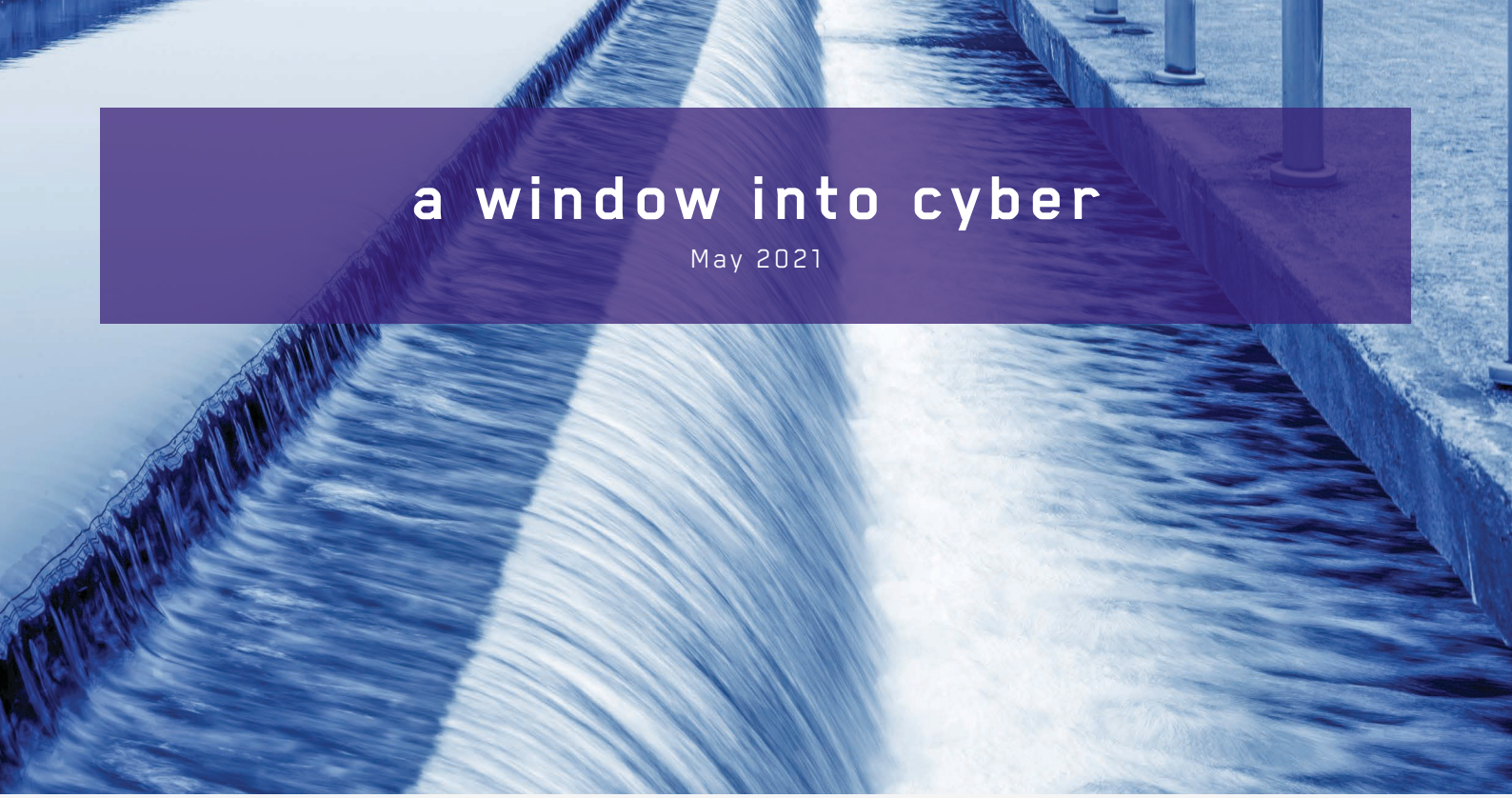


a window into cyber

May 2021

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

All too frequently, a new cyber breach story hits the headlines and makes us contemplate the possible consequences. The recent case of a hacker accessing a Florida city's water system highlights the vulnerability of such facilities – and is the focus of Dr Jess Barker's article this month.

Attacks like this are of increasing concern for operators of critical national infrastructure. Power plants, emergency services and transport systems are all attractive targets. With the pandemic prompting a shift towards more remote working, the need to maintain the highest levels of cyber security has never been greater.

We're also highlighting Brit Cyber Attack Plus in this issue. Our award-winning product offers extensive first and third party coverage that adapts to suit a client's specific needs. And as ever, Datasafe – our online training and risk management platform – provides a raft of resources, tools and information to support you.

Don't hesitate to call if you need us.

this month's author: **Dr Jessica Barker**

Co-CEO and Head of Socio-Technical Security, Cygenta

Dr Jessica Barker is a leader in the human side of cyber security. She has been named one of the top most influential women in cyber security in the UK and has been recognised with a TechWomen50 award. She is the co-founder of co-CEO of Cygenta, where she follows her passion of positively influencing cyber security awareness, behaviours and culture in organisations around the world.

Along with being the Chair of ClubCISO, she is a popular keynote speaker who regularly shares her expertise in the media. In 2020, she was the keynote speaker at RSA San Francisco and her book 'Confident Cyber Security; How to get Started in Cyber Security and Futureproof your Career' was published in September by Kogan Page.

The ultimate watering hole attack?

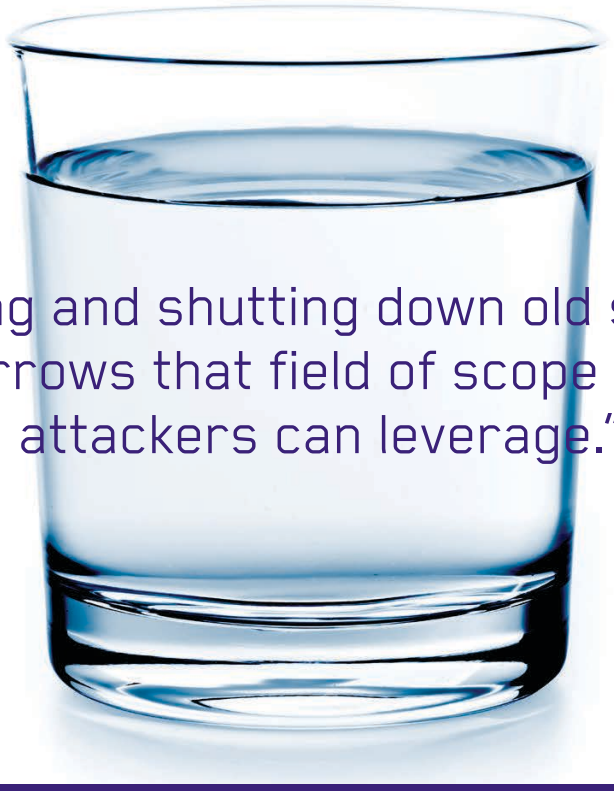
Dr Jessica Barker | Co-CEO and Head of Socio-Technical Security, Cygenta

In February 2021, cyber criminals attempted to poison the water supply in Florida, USA. They did so by trying to raise the sodium hydroxide content to more than 100 times its normal level, threatening human health. This attack represents a very challenging and vital area of cyber security: preventing and responding to attacks that cross the digital boundary into the physical space, to have lasting effects in the real world. The opportunity for cyber criminals is clear. As industrial systems become more standardised and are integrated more into office spaces (to provide data, safety and remote access), those systems become part of a larger interconnected space. That is an attractive, and growing, target for criminals looking for weaknesses to exploit.

Water filtration plants are part of Critical National Infrastructure systems that governments protect, because the failure of one of those systems can have a devastating impact on a country and its citizens. So how, in February, did cyber criminals manage to access Florida's water filtration systems – not just once but twice – on a sunny Friday?

The criminals gained access via old and unused software called TeamViewer, which allows the system's operators to connect remotely to the control computers to monitor and make changes if needed. The software was no longer used by the Florida water department, but had not been removed from the computers. This kind of technical legacy is a weakness for many organisations: dormant or out-of-date and unused software is one of the largest vectors of system compromise that we see. Many companies move providers or change their ways of working – and clean-up of old software is often postponed or forgotten about.

continued on next page



"Locating and shutting down old software narrows that field of scope that attackers can leverage."

In fact, in almost every penetration test we perform we find services that are no longer being used. These could be removed without any impact to the business, other than reducing the threat landscape and increasing the security. Software and security move at an incredibly rapid rate; unfortunately, so do criminals. Locating and shutting down old software narrows the field of scope that attackers can leverage to gain access to your company.

"Prevention and protection will always be a fundamental element of cyber security, but preparation and response are just as vital."

This is not the first time that attackers have targeted a water facility. In April 2020, Israeli water facilities were targeted in a similar way, so much so that the Israel National Cyber Directorate is working with the FBI on the Florida case to help the US track the attackers. For many years, the UK National Cyber Security Centre has been warning that the UK will experience a Category One national cyber emergency, for example damaging infrastructure. Authorities prepare for these scenarios on the basis of 'it's not a matter of if, but when' – and this kind of approach can be beneficial for private organisations, too. Prevention and protection will always be a fundamental element of cyber security, but preparation and response are just as vital: be alert to attacks and know what to do if – or when – the worst happens.

It was this approach that thwarted the hostile action in Florida: a worker at the treatment facility spotted the attack as it was happening and reversed the action. We can all learn from this case and heed the warnings about merging of our physical and digital spaces, the need to take care of technical legacy and the importance of being prepared for attacks – alongside preventing them in the first place.

@drjessicabarker
linkedin

news from Datasafe

BRIT

Datasafe provides the latest risk management resources, enabling Brit's clients to proactively manage their data protection and privacy risks.

Microsoft update

Over 30,000 organisations were affected by the Microsoft Exchange Server vulnerability featured in last month's newsletter. Experts learned that, after accessing the victim's environment, hackers leave behind a web shell or back door: a tool that can be used by criminals to subsequently access the same environment. **Critically, the web shell remains even after the Exchange Server is patched with the latest Microsoft updates. Therefore, all Exchange Servers should be inspected for signs of unauthorised access and any web shells must be removed.**

Find out what to do here

Was your Exchange Server compromised?

The list of compromised Microsoft Exchange Servers contains 86,000 IP addresses and domains of infected Exchange servers. The list can be accessed using a web service that helps identify which email systems were infected. Users can enter an email address and will receive an email if the organisation appears to be infected.

Click to access the Check my OWA tool

Brit Cyber Attack Plus

Cyber Innovation Product of the Year 2020 (Insurance Insider Cyber Rankings Awards)

Designed around the unique needs of Tier 1 industrial and trade businesses, BCAP's towers of coverage enable the perfect fit for every client.

For more information, click here

Coverage	Tower A Full BCAP	Tower B Cyber Property Damage writeback	Tower C Cyber Non Physical Damage
Physical Damage	✓	✓	
Business Interruption from Physical Damage Events	✓	✓	
Bodily Injury	✓		
Non Damage Business Interruption	✓		✓
Breach Response Costs	✓		✓
Data Restoration	✓		✓
Cyber Extortion	✓		✓
Privacy and Security Liability	✓		✓
Regulatory Fines and Penalties	✓		✓
PCI DSS Assessment	✓		✓
Limit	USD 150m	USD 150m	USD 100m