Circle.

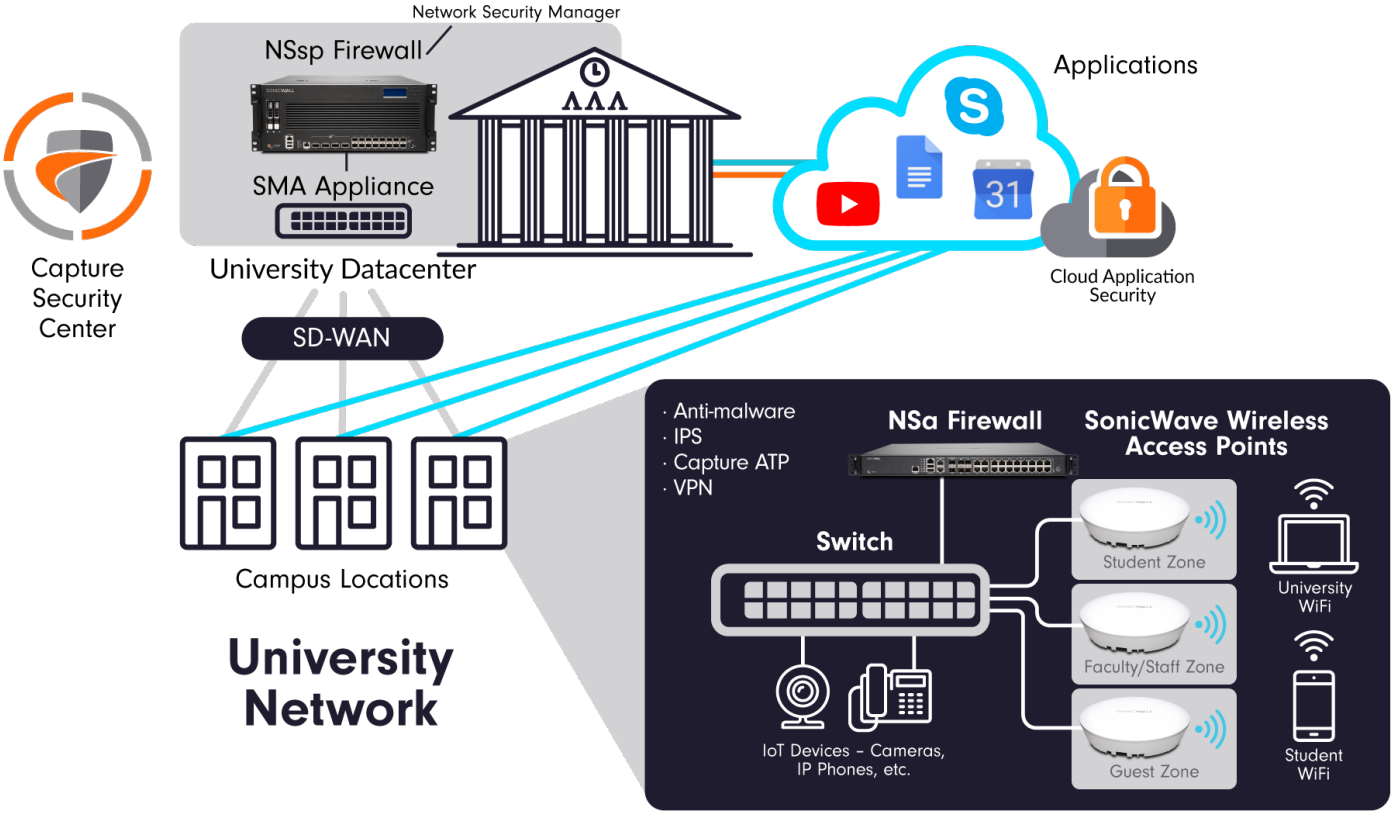
www.circleit.co.uk

Are universities at greater risk of cyber-attacks?

The last year has seen an unprecedented change in the way that organisations operate, with the education sector being a particular victim of this.

The rapid move to operating remotely due to the nationwide lockdown meant that universities had to quickly come up with alternative methods to continue their students' education. This often included moving services to the cloud to form a hybrid infrastructure service and utilising software-as-a-service products such as Microsoft 365 and Dropbox.

Previously, faculty and students would have predominantly accessed the network via campus and/or managed devices and would have been protected by the university's many layers of security. The network and users would have been protected by a robust firewall as the first line of defence, which includes services such as DDoS mitigations, malware blockers and content filtering. So, whilst on campus, the chances of malware getting on to a device were low.

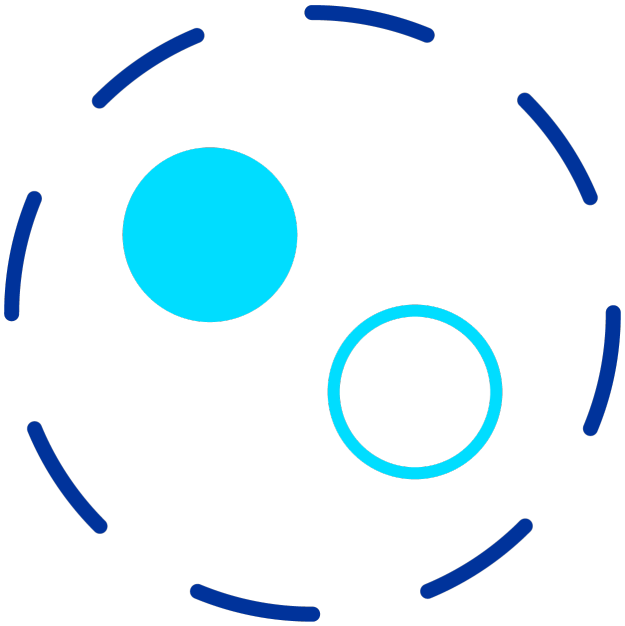


(Adapted from SonicWall's higher education structure)

With students and faculty now accessing services remotely, those protective measures don't cover all scenarios given the new use of cloud-based services outside of the campus network.

Policies and filters no longer restrict websites that could pose a security risk, therefore malware can find its way on to a user's device more easily, in turn putting the university's network at risk when they do remotely connect or return to campus and connect to the network.

For security and IT teams, this creates new challenges around how to manage access to services and the multitude of devices being used. They are not able to see the actions of users and therefore can't monitor behaviour for any abnormalities that could be fraudulent (without additional systems in place).



In an interview with Jonathan Monk, IT Director at the University of Dundee, he speaks about the likelihood of whether learning at universities will return to 'normal'.

> "We are likely to see continued restrictions for some time, so institutions will need to find more advantageous ways to adapt"

As we know, Firewalls protect devices that are physically plugged in, so that defence doesn't extend off-campus. However, there are software solutions available that extend that protection outside of the network which would enable a more secure solution for longer-term remote working.

As key contributors to the economy and hubs of innovation, every university has a wealth of assets that have a significant value - from personal details and passwords to confidential research, they are a prime target for cyber-criminals looking for a lucrative opportunity.

In a recent poll carried out by Top Line Comms, of the 105 universities that responded,

35

admitted to being attacked (33%)

25

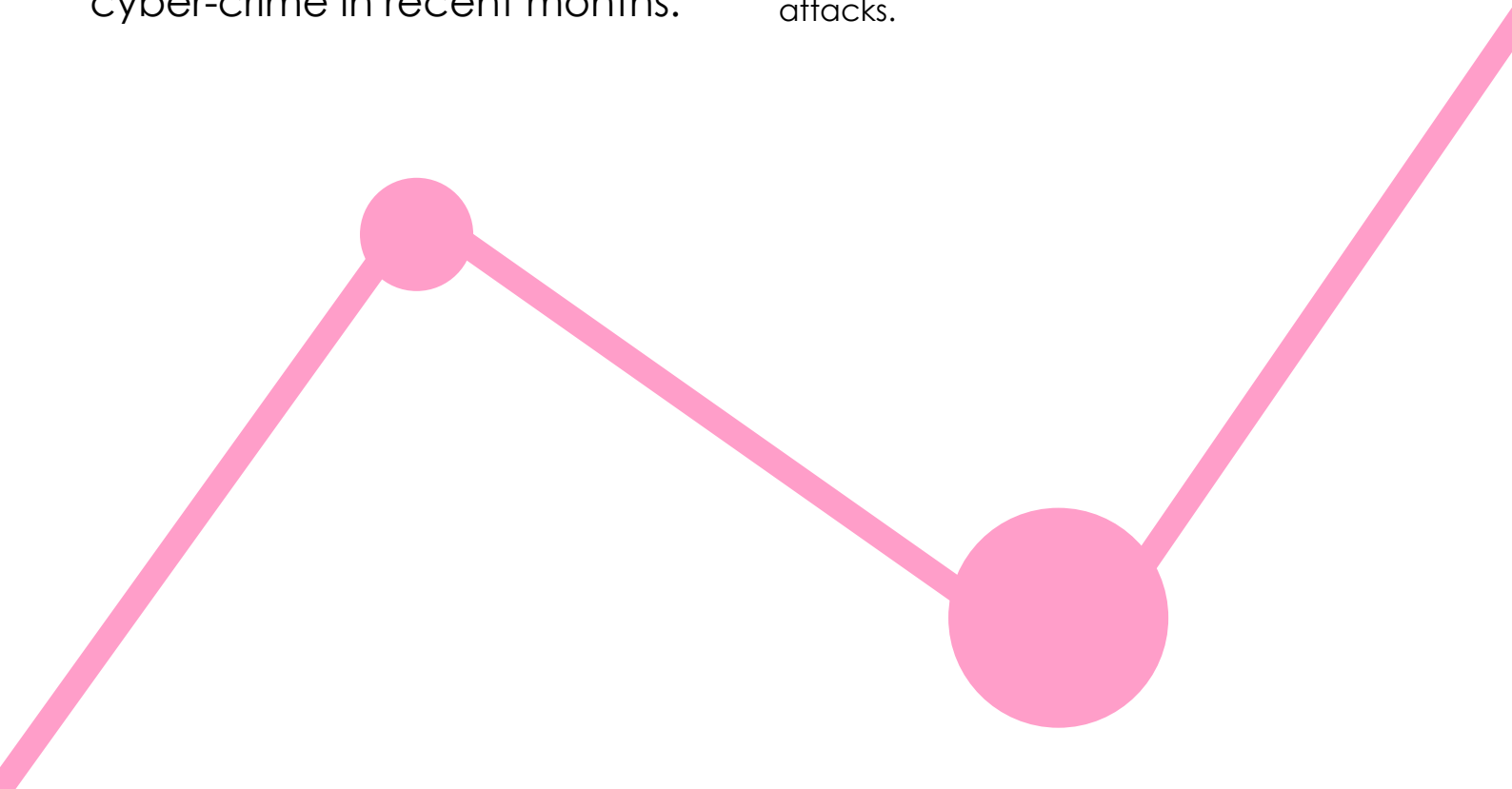
said they hadn't been (24%)

43

refused to answer (45%)

With the sharp move to remote teaching and learning, coupled with more advanced tactics universities have been some of the worst affected by cyber-crime in recent months.

In September of last year (2020) attacks had become so prevalent that the National Cyber Security Centre issued a cyber-security alert aimed at those responsible for IT and data protection within educational establishments in the UK in an attempt to mitigate the risk of future attacks.

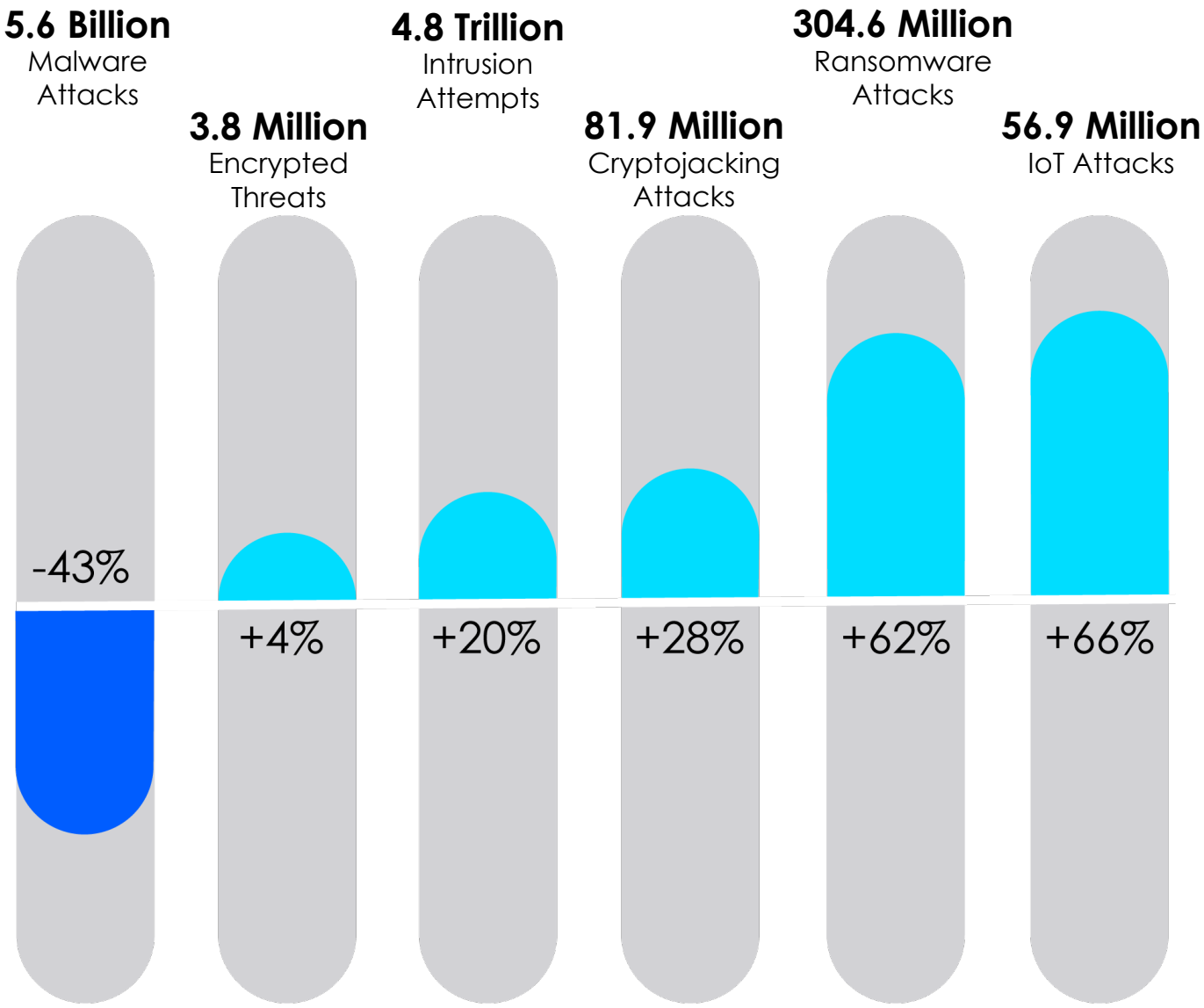


> **"I would strongly urge all academic institutions to take heed of our alert and put in place the steps we suggest, to help ensure young people are able to return to education undisrupted"**

Paul Chichester, Director of Operations at the NCSC

Unfortunately, for universities hit by ransomware, the disruption is not short-lived. When Newcastle University experienced a cyber-attack in September of last year, it left its IT systems impaired, only able to provide limited services for a number of weeks. In a recent attack on the 8th March, the University of the Highlands and Islands was forced to close multiple campuses to students.

2020 Global Cyberattack Trends



(Source – SonicWall 2021 Cyber-Threat Report)

It's clear to see that the pandemic has caused an increase in the risk of cyber-attacks, but these can have wider implications than just disrupted operations.

With universities playing a vital role in the fight against COVID-19 through research and the development of the vaccine, those involved are arguably more of a target for cyber-attacks. One of the world's top biology labs, Oxford University's Division of Structural Biology, whose professors have been researching how to counter the Covid-19 pandemic were compromised in February (2021).

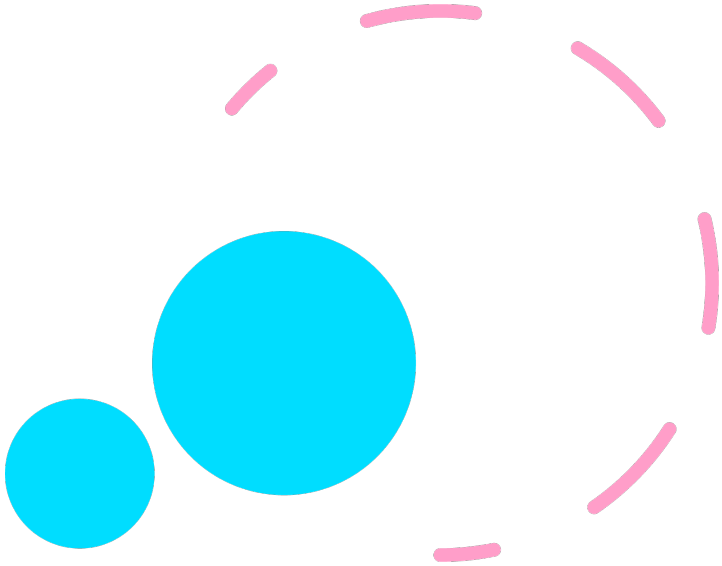
The threat actors were able to gain access to several systems, including machines used to prepare biological samples. It's currently unknown whether there have been any further implications from this attack, but it is a prime example of how a cyber-attack could potentially un-do years or even decades of vital research.

Whilst COVID-19 specific research has put some universities more prominently on the radar, the increased vulnerability can also be attributed to the technological advancement we have seen in recent years. Bring your own device (BYOD) is becoming more common and relied upon by students. With many having spent the last year working from personal devices, this trend will only become more common. Students, teachers, and other personnel bring an average of three devices per person to campus (teiss) and connect them to the WiFi, opening the entire network up to myriad vulnerabilities.

The rise in the development of the internet of things means university resources such as lab equipment, machinery and printers are increasingly being connected to the internet, making them a potential door for a threat actor. In 2017, threat actors acquired data from a North American casino by using a fish tank (Washington Post). The tank was connected to the internet via smart sensors that regulated the environment of the tank which created another entry point to the casino's network, where threat actors were able to enter and move to other areas where data was stored. So, even a seemingly 'simple' object can be used as an opportunity.

Despite the notable increase in cyber-crime within the last 12 months, the vulnerabilities of educational institutions are not new.

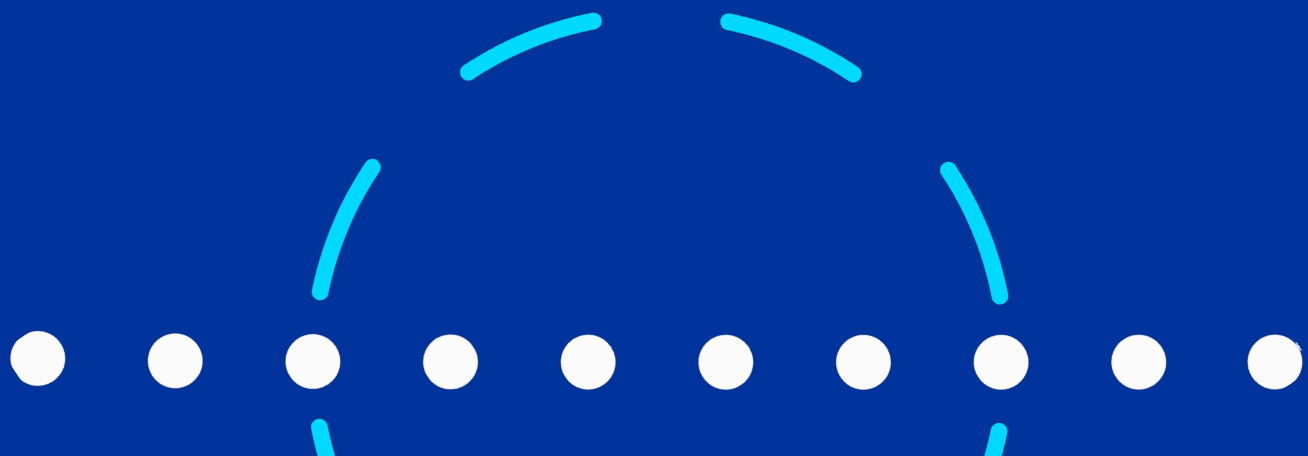
As we know, the main cyber threats to universities are likely to be either criminals looking for monetary gain or forms of state-sponsored attacks. These often have the goal of stealing intellectual property for strategic advantage or to damage the value of research being carried out by the target university. However, motives could also be to cause disruption.



The most prolific example of this is the 2017 WannaCry attack that infected more than 230,000 computers in more than 150 countries including the UK's NHS (Kaspersky). This caused the UK £92 million, it is arguably the largest ransomware attack we have seen.

In cases like WannaCry, the virus, just as a biological virus would spread, does not necessarily aim to kill its host but to spread and infect as many devices as possible. So, your organisation may not be the intended victim of the ransomware, but it will still cause the same damage as if it was. However, it isn't just the security of your own IT systems that you need to consider. The security of your service and solution providers or partners also need to be taken into consideration as they can cause additional risks.

In early 2020, threat actors (suspected state sponsored) secretly broke into Texas-based SolarWind's systems and added malicious code into the company's software system that was being used by 33,000 customers The following March, SolarWinds unknowingly sent a software update to all customers that contained the compromised code, creating a backdoor to customer systems.



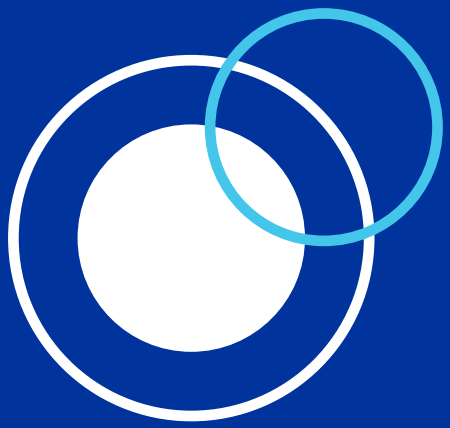
The attack was carried out so surreptitiously that it went undetected for months and experts say that some victims may never know if they were even victims or not due to lack of SIEM products deployed that would give the capability to detect and respond. As universities often have multiple software and service providers, ensuring that any third parties are monitoring their security is vital.

It could be argued that universities are more vulnerable to cyber-attacks than other sectors due to:

a. The size of their networks and the way they are accessed

b. The wealth of data they hold

Whether this is the case or not, it doesn't change that there is an inherent risk to educational institutions because of the nature of the information they hold and the way they operate. With the drastic changes that the pandemic has brought, the way universities operate may well have been changed for good. The way IT, security and data protection teams manage the IT systems must also change and develop in line with this.



To find out more about how The University of Dundee has adapted to the changes, tips on how to best manage security and thoughts for the next 12 months, watch our interview with Jonathan Monk, the University's IT Director.

Security And COVID Adaptations In Higher Education

Jonathan Monk, IT Director,
University of Dundee

Click Here To Watch Video

Talk to one of our security experts today