Reviewing IT security incidents in 2020, Patrick O’Connor MBCS CISSP CEH, finds that while society may have slowed to a crawl in the face of Covid-19 the cyber security world is more active than ever.

We all know that 2020 will be remembered for just one thing. While stuck at home, an increased reliance was placed on our various connected devices both for welcome social interaction and an ability to work remotely.

An explosive growth in the use of video conferencing software quickly brought to light security weaknesses in some products. For instance, Zoom (whose value increased more than 400%) found it was not long before some meetings and family gatherings were interrupted by hackers — with everything from political comment to pornography.

Lured by promises of the latest news of the virus, many were duped into visiting websites or opening emailed ‘reports’ containing graphs and charts showing current virus information, but which also installed malware. Researchers at security firm, Checkpoint, found that in the first month of the outbreak, more than 120 malicious and 200 ‘highly suspicious’ domains related to coronavirus were registered.

According to US sources, breaches at healthcare related companies have doubled over the same period last year with Ryuk ransomware still the tool of choice for attackers. Nation state actors have also been attempting to breach medical companies and universities to steal Covid-19 research data.

Not so happy new year
Even before 2020 had begun, things took a turn for the worse for Travelex. The currency exchange was attacked on New Year’s Eve 2019 and their website had to be taken down for three weeks. They were attacked by the cybercriminal group behind the Sordinokobi ransomware, also known as REvil. This downtime adversely affected several major banks in the UK, including Barclays, Lloyds and Royal Bank of Scotland, as they all use Travelex to provide foreign exchange and travel money services.

‘There is no evidence yet of how the attackers gained initial access, but it is likely to have been part of a Covid-19 related phishing campaign.’

Storm clouds
Cloud computing is proving an exciting new target for hackers. While offering a staggering range of services, the cloud providers’ environments can prove challenging to secure properly.

Early in the year, a poorly configured Amazon simple storage service (S3) database was found to have exposed almost half a million financial records. The database was linked to a financial app called MCA Wizard, launched in 2018 but no longer in circulation.

A security intelligence company called Binary Edge found 35,516 unsecured databases online worldwide. Of these, most were in China and the United States, with the majority in the cloud.

Many companies are now considering the cloud, especially with staff needing to work remotely during lockdown. The built-in accessibility the cloud provides would make future outbreaks less disruptive to a workforce. However, the problems of securing a complex cloud environment are significant.

No reward for loyalty
In March this year, Marriott announced they had been breached and that records for more than 5.2 million users of their loyalty app were compromised.

The intruder used the credentials of two employees from a Marriott franchise property, to access customer information on the loyalty app’s backend systems. Details leaked included name, email, postal address, phone numbers, birth dates, gender and various details of employment and travel preferences.

This is the second notifiable breach of Marriott systems in the last 16 months. In November 2019 Marriott confirmed that hackers had gained access to the Starwood Hotels reservation system. Through this they accessed the details of more than 383 million customers.

Easy Jet, easy target
It was revealed in May this year, that Chinese hackers managed to access records of approximately nine million Easy Jet customers. The actual breaching occurred in January and the UK Information Commissioner’s Office (ICO) and National Cyber Security Centre (NCSC) were notified at this time, but customers were not informed until four months later.
As a result, the airline is facing an £18 billion class-action lawsuit filed in the High Court in London on behalf of customers impacted by the disclosures. The lawsuit refers to aspects of the General Data Protection Regulations (GDPR). This allows consumers the right to claim compensation when their information is compromised in security incidents. There could also be heavy fines for Easy Jet under GDPR.

Losing control
The most sophisticated publicised instance of hacking thus far remains Stuxnet. This complex attack on an Iranian nuclear facility exploited supervisory control and data acquisition (SCADA) systems. It was the first to demonstrate the extreme vulnerability of industrial control systems being connected. Since then, there have been numerous similar exploits, often employing parts of the Stuxnet code, since it became public.

In June this year, Honda’s corporate network was breached. According to the security firm, Sentinel One, it found Ekans or Snake ransomware. Snake is designed to attack industrial control systems. The fact that Honda halted production in the UK, US, Turkey, Italy and Japan, implies some success.

Honda insisted that no data had been lost, suggesting they were able to restore from backups. This may have caught the problem early enough to minimise damage. There is no evidence yet of how the attackers gained initial access, but it is likely to have been part of a Covid-19 related phishing campaign.

Celebrity scam
Twitter was again the subject of a headline-grabbing breach in early July, which saw high profile accounts like those of Joe Biden, Barack Obama, Elon Musk, Bill Gates, Jeff Bezos and Apple taken over by hackers. Subsequent tweets promised their legions of followers ‘double their money’ if they deposited bitcoins to a particular account. Despite the unlikely sounding offer, more than $100,000 was actually deposited in the rogue Bitcoin account.

Such was the relatively amateur nature of this attack, authorities were able to identify and arrest the perpetrators within days. The 17-year-old ‘mastermind’ was also prepared to discuss details of the hack with journalists online. This attack was achieved through social engineering a number of Twitter employees over the phone.

Navigating a hostile network
In late July, users of Garmin satellite navigation devices and services found they were suddenly unable to use them. The company’s website was down, its call centre offline and, for a time, there was no way to contact them at all.

They had been attacked with WastedLocker, ransomware software developed by the notorious Russia-based Evil Corp group. Such was the disruption caused by the attack, that production was halted at Garmin’s factories in Taiwan for five days.

Chinese warning
Companies operating in China were placed on alert late in the summer, after hidden backdoors were discovered in mandatory tax-related software. China’s banks require all companies to download software from either Aisino or Baiwang to comply with its Golden Tax VAT scheme. This could indicate that the malware, labelled GoldenSpy, has either direct sponsorship from the government or is being deployed with its blessing.

More malware, dubbed GoldenHelper, which pre-dates GoldenSpy, has been found in the Golden Tax Invoicing Software (Baiwang edition) which is digitally signed by a subsidiary of Aisino, Nou Nou Technologies. GoldenHelper, while functionally different to GoldenSpy, has a similar delivery mechanism, according to security company, Trustwave.

Based on this, the FBI sent out an official warning to all US companies in China. They believed companies in the healthcare, chemical and finance sectors are in particular danger, based on China’s historical interest in these sectors.

The new normal
As we come to terms with how the world may be changed as a result of Covid-19, there are indications the cybersecurity landscape is also changing.

From this brief selection of some of 2020’s security incidents, it should be clear that they naturally fall into categories. There are tabloid-friendly hacks, like the one at Twitter — newsworthy only because of the names of those involved.

Then, there are the inevitable and escalating attacks on financial institutions and medical facilities with the growing use of ransomware as an effective means to extort money.

There are also the huge number of database breaches resulting in the theft of personal data. This problem could be said to have reached epidemic proportions on its own, as websites which try to catalogue all cyber incidents show data leaks on an almost daily basis.

Cyber criminals are industrialising their projects and state actors are being discovered taking even greater interest in

‘This complex attack on an Iranian nuclear facility exploited supervisory control and data acquisition (SCADA) systems.’

all companies to download software from either Aisino or Baiwang to comply with its Golden Tax VAT scheme. This could indicate that the malware, labelled GoldenSpy, has either direct sponsorship from the government or is being deployed with its blessing.

More malware, dubbed GoldenHelper, which pre-dates GoldenSpy, has been found in the Golden Tax Invoicing Software (Baiwang edition) which is digitally signed by a subsidiary of Aisino, Nou Nou Technologies. GoldenHelper, while functionally different to GoldenSpy, has a similar delivery mechanism, according to security company, Trustwave.

Based on this, the FBI sent out an official warning to all US companies in China. They believed companies in the healthcare, chemical and finance sectors are in particular danger, based on China’s large companies, while the ever-present threat to individuals is only getting more sophisticated. There is already evidence emerging of renewed interference by Russia in the 2020 US Presidential election.

In a year when a real virus monopolised our attention, those in the digital realm continued to develop and mutate.

While there is the possibility of a vaccine for one contagion, to eradicate the other may be considerably more difficult.

About the author
Patrick O’Connor (linkedin.com/in/pdoconnor) is a principal systems analyst programmer with Amadeus IT Group (www.amadeus.com), the leading travel technology company.