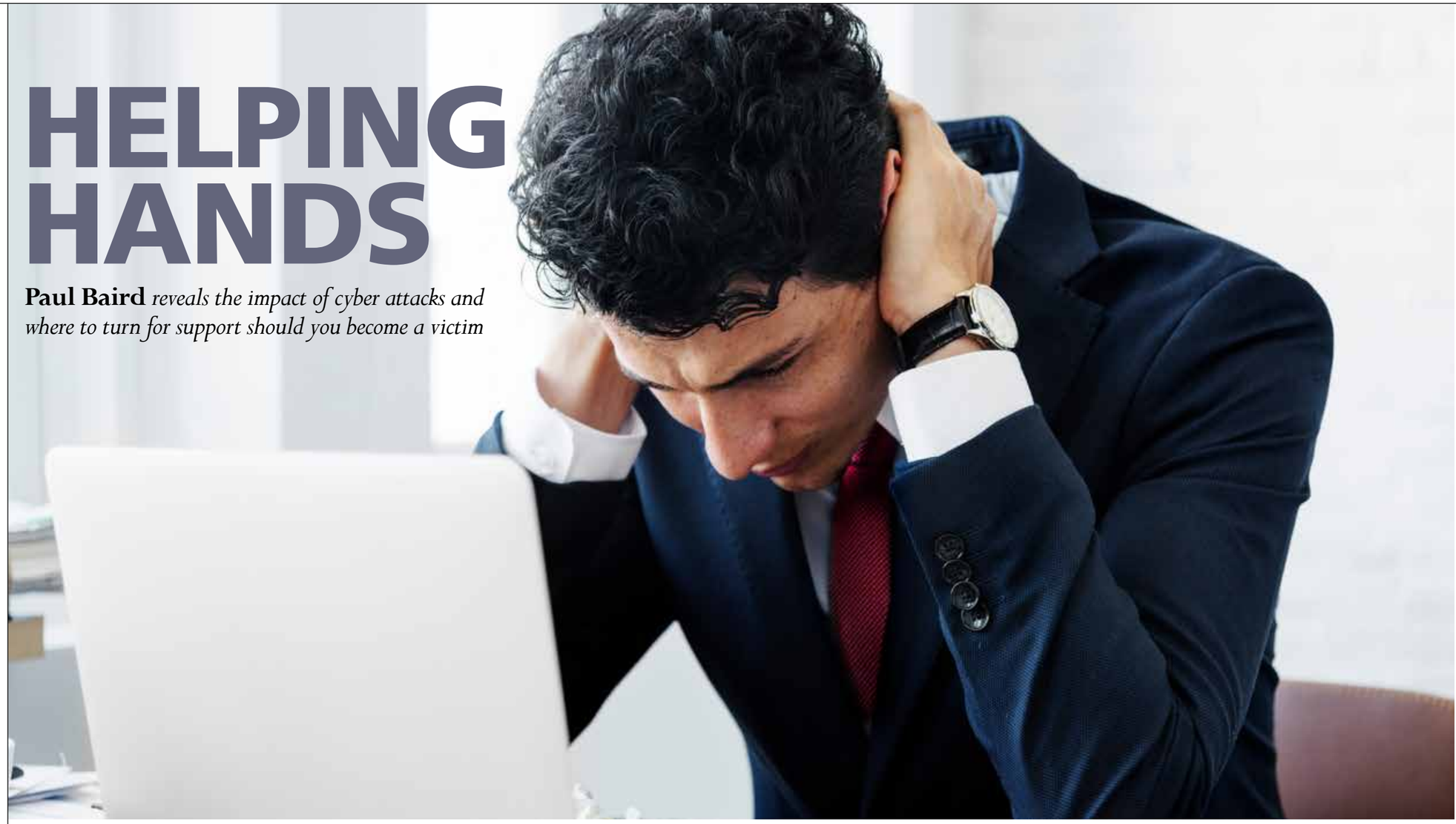
HELPING HANDS

Paul Baird *reveals the impact of cyber attacks and where to turn for support should you become a victim*



Picture credit: AdobeStock

Security incidents have huge impacts, whether they are successful or not. From direct costs due to ransomware payments or stolen capital due to business email fraud, through to indirect costs around incident response, clean-up operations and reputational impact, the cost for security breaches is significant. According to IBM's Cost of a Data Breach Report for 2023, the average cost for a data breach globally was $4.45-million, which has increased by 15 percent over the past three years.

However, while this is a huge amount, businesses should have the mechanisms in place to respond to these threats. From dedicated IT security teams that endeavour to protect their systems against attack, through to incident response teams that get systems running again after an attack, through to cyber insurance to cover the costs of clean-up, businesses can get themselves operational again. The same cannot be said for individuals or those running micro-businesses – organisations that employ one or two people.

According to the UK Government's Cyber Security Breaches Survey for 2023, micro-business operators do understand the risk that cyber security represents. However, the percentage listing it as a high priority has dropped from 80 percent in 2022 to 68 percent in 2023. This is most likely due to other issues taking over, like the cost of living crisis and worries about inflation. So even if we understand the risks, there may be other pressures that we have to take into account as well.

As private citizens, we all the same problems from hackers that businesses do. However, not everyone is equipped with the same knowledge and skills that we have around cyber security. The gamut of people on the internet is vast, it is a global network that connects billions from all walks of life, cultures and backgrounds. This diversity is one of the internet's most significant strengths, but also one of its biggest weaknesses as everyone on it is a potential target for hackers.

The average cost for a data breach globally is $4.45-million

Like businesses, individuals face a myriad of threats, from cyber stalking to attempts to invade their privacy. Attacks on social media accounts and fraud attempts are all too common. According to Harris Poll, 22 percent of Americans have lost money to phone fraud in the last 12 months. According to the Internet Crime Complaint Center, last year saw a total of 800,944-million complaints concerning cyber attacks with an associated loss of $10.3-billion. Over the past five years, the total number of complaints now stands at 3.26-million, with an associated loss of $27.6-billion.

Attacks can be linked to misuse of personal data. The FBI recently announced the arrest of a threat actor that ran marketplaces that traded in US social security numbers. These details can be used to commit various fraud attacks, from attempting tax fraud or unemployment insurance fraud through to obtaining loans or credit cards using those stolen details. During the investigation, it was found that one user on the site carried out money laundering and theft using this personal identifying information valued at nearly $10-million. This had an immense impact on all those affected.

Attacks are also often linked to trends that affect people. In 2023, loan scams have grown 170 percent, job fraud has gone up 131 percent, and there was an increase of 128 percent in investment scams, according to The Cyber Helpline. Job fraud is prevalent because individuals are desperate due to the cost of living crisis, and pay in advance to secure a job that should pay them back quickly. The average loss for a victim of one of these scams is £5,565, but these incidents also have a severe impact on victims' finances, ability to pay bills and overall mental health.

IN ITS FIRST TWO MONTHS THE CYBER HELPLINE SUPPORTED MORE THAN 1,200 PEOPLE IN THE US

Yet support for people who suffer these attacks is sadly lacking. Who do people turn to when they get hit by malware, when someone steals their account and carries out attacks, or misuses their personal data for fraud? For many of us, we don't know where to turn for help. Cyber security is a complex field, and individuals without technical expertise may find it challenging to navigate the aftermath of a cyber attack. Understanding the nature of the attack, securing compromised accounts, and recovering lost data can be daunting without proper guidance.

Cyber attacks, especially those targeting individuals, are often under reported. Victims may feel embarrassed, ashamed or fear legal repercussions, leading them to remain silent about the incidents. When attacks go unreported, it becomes challenging for support systems to identify and reach out to victims. The first challenge for many is understanding if a 'crime' in the eyes of the law has taken place or not. If it has, like any crime, police and law enforcement should be the first port of call for assistance. However, many police forces are not IT specialists, are under resourced and may not be able to help in the right way because they have not been trained on cyber attacks, online fraud or social media stalking. There are specialist groups set up to help, but getting to these is dependent on knowing where to turn. For those that are not familiar with the world of online security, this can be extremely frustrating when they are already at risk due to the attack they have suffered.

Professional cyber security assistance may come with a cost, making it inaccessible for some individuals, especially those who have already suffered financial losses due to the cyber attack. Luckily this is where the The Cyber Helpline can help, bringing that industry expertise to bear with individuals who are affected by attacks. This is a charity set up in the UK that supports IT security experts to volunteer and help people affected by cyber attacks. The charity provides self-help guides for those affected by common risks, and it also helps those in need get access to specialist skills around security based on their problems when circumstances go beyond those situations.

At present, the charity supports around 2,000 new cases per month. Since it launched, it has managed more than 30,000 cases in the UK, with the rate of cases growing at more than 100 percent year on year. The organisation relies on volunteers from the IT security community to bring their skills and knowledge to bear on issues, with more than 90 people taking part to run the helpline.

One victim found that her SnapChat account had been hijacked and accessed six times in three days. After this, she started receiving messages from strangers. This led through to requests for sensitive images based on private pictures that had been stored in her account. Following more requests, she looked for help.

Following advice from the Cyber Helpline, the victim was reassured that they had been affected by a crime and that they could report the incident to the police. She reported the crime online and quickly received support from law enforcement. This included an investigation into the source of the harassing messages. Based on information from SnapChat, the team was able to identify the IP address and device used to hijack the victim's account, and so the perpetrator was discovered.

The attack was possible because the victim's password was re-used across several accounts, one of which was SnapChat. One of the sites suffered a data breach, and all the passwords were stolen by an attacker. The data was then used to set up a sale site for access credentials, which the perpetrator used to get access to the account on SnapChat. Following the attack, the victim was able to regain control over her account and set up stronger security for herself.

Alongside services like The Cyber Helpline, there are other organisations looking into how to improve security for the wider population. The UK's National Cyber Security Centre runs an automated service that helps individuals check if messages they get are legitimate or scams. The Suspicious Email Reporting Service (SERS) received more than 7.1-million messages in 2022, up 33 percent from the previous year. This helped identify and remove 40,000 scam campaigns in 2022, as malicious links reported to SERS were removed from the internet, on average within six hours.

For The Cyber Helpline, the future is about finding more volunteers from the IT security industry that are willing to provide their time and expertise to support victims. At the same time, the organisation also needs to raise funds to cover the logistics, equipment and tools that volunteers have to use to deliver support, as well as carrying out background checks on those volunteers before they start working with potentially vulnerable people. This is a huge effort to get people ready to be productive and help victims, but it is necessary to safeguard individuals that may already be at risk.

In June 2023, The Cyber Helpline launched in the United States and in the first two months supported more than 1,200 victims get access to support and law enforcement. More than 8,700 people used the charity's content to support their own needs too. This expansion is a huge effort as well, as legal systems are very different in each country and state, so this all requires support to achieve. The Cyber Helpline has targeted October as its fundraising month, alongside the ENISA European Cyber Security Month and the Cybersecurity and Infrastructure Security Agency Cybersecurity Awareness Month.

For all of us, our lives are now more online than ever before. We run the risk of attacks that can steal our data, compromise our privacy or lead to theft. Knowing where to turn when this happens is important, but even more is the feeling that we can get the help that we need in times of trouble. Initiatives like The Cyber Helpline complement the work that law enforcement and government agencies carry out, providing that helping hand when we need it the most. This is a great opportunity for the IT security industry to give back and help others ●

Paul Baird is a highly experienced and accomplished IT and cyber security professional with over 25 years of industry experience. Currently, he is serving as the Chief Technical Security Officer (CTSO) for Qualys. Throughout his career, he has demonstrated a deep understanding of cyber security and has been instrumental in building several Security Operations Centres (SOCs). His achievements in the field were recognised in 2021 when he was awarded Fellowship of Chartered Institute of Information Security Professionals (CIISec) for his outstanding work in supporting cyber security.

The Cyber Helpline is a UK charity that supports people affected by cyber attacks