Crossword Cybersecurity Plc Reveals 5 Cyber Admin Fails Still Happening in 2023

LONDON, UNITED KINGDOM, December 12, 2023 /EINPresswire.com/ -- Crossword Cybersecurity Plc, the cybersecurity solutions company focused on cyber strategy and risk, has today announced the 5 cybersecurity areas that its global consulting team has consistently seen fall short in 2023, and which are placing companies at higher risk in 2024.

> Whilst it is hard to accept, the reality is that many of the basics are hard to get right. Investments in software to bolster the cyber security posture can often create a false sense of security."
>
> *Phil Ashley, Managing Director – Managed Services, Crossword*

Crossword's cybersecurity consultants work with enterprises, SMEs and public sector organisations across the globe. Whilst every sector and business has unique technology challenges, Crossword has identified the following areas that every IT and cybersecurity team should check to immediately improve their cybersecurity posture in 2024.

1. Patch your patching processes – Patches missed on certain devices, or missed entirely remains a common problem. Whilst patching desktop machines is relatively easy, we see that critical servers are often left unpatched due to the services that run on them, and scheduling downtime. Even more of a culprit are network devices and external facing services such as those used for remote access. Whilst these are harder or more inconvenient to patch they are more important, as when compromised, the implications can be far reaching. Make sure systems are being monitored for missed patches and devices, and ensure you know your estate well with consistent and audited asset management processes.

2. Weak encryption mechanisms – Due to software backward compatibility, operating systems tend to have legacy encryption turned on by default. Even though these encryption protocols have been superseded by far stronger options, the weaker ones are rarely fully turned off. Companies should make the change, using the opportunity to check all sensitive data and traffic is strongly encrypted.

3. Generic admin accounts – These accounts pose significant risk to organisations and can be exploited by hackers – particularly if they have weak passwords. All admin activities that take place across an organisation need to be attributed to a specific person, the use of generic

accounts does not provide this. Passwords on generic accounts are often left unchanged due to the inconvenience of changing a password shared by all. An even bigger issue is when a user with knowledge of these accounts leaves the organisation, as the passwords are rarely changed. Start by conducting an audit of admin accounts and then review your offboarding processes. Remember admin account passwords should be changed regularly too.

4. Excessive back-up account privileges – Often admin accounts for back-up services are discovered with domain wide privileges. These accounts are sometimes left with the same passwords for a long time, and given that they typically access many systems, this password is often left cached on them. This cached password can be leveraged to grant an attacker domain wide access to a company's systems. Check your accounts to ensure that privileges are limited to the resources they need to access and with their own admin group, prevent the use of cached passwords.

5. Change management documentation failures – Documentation may be one of the less exciting jobs in the IT department, but many of the problems Crossword consultants find are the result of poorly change management processes across the IT estate. Often, not going through a formal change process can result in failing to fully consider the wider security impacts a change might have, leading to hidden vulnerabilities that a hacker will find and exploit. Make sure your processes are understood by all staff, not just in terms of how to record changes, but where to find information they may need.

Phil Ashley, Managing Director – Managed Services at Crossword Cybersecurity, said: "Whilst it is hard to accept, the reality is that many of the basics are hard to get right. Investments in software to bolster the cyber security posture can often create a false sense of security. Good cyber hygiene and processes are needed alongside great services and software to ensure a strong cyber security posture. Every company should check the 'repeat offenders' we have highlighted."

Those wanting to learn more about Crossword's assessment of the current threat landscape can watch the on-demand webinar "Exploring themes from across the threat landscape affecting organisations."

About Crossword Cybersecurity plc
Crossword offers a range of cyber security solutions to help companies understand and reduce cyber security risk. We do this through a combination of people and technology, in the form of SaaS and software products, consulting, and managed services. Crossword's areas of emphasis are cyber security strategy and risk, supply chain cyber, threat detection and response, and digital identity and the aim is to build up a portfolio of cyber security products and services with recurring revenue models in these four areas. We work closely with UK universities and our products and services are often powered by academic research-driven insights. In the area of cybersecurity strategy and risk our consulting services include cyber maturity assessments, industry certifications, and virtual chief information security officer (vCISO) managed services.

Crossword's end-to-end supply chain cyber standard operating model (SCC SOM) is supported by our best-selling SaaS platform, Rizikon Assurance, along with cost-effective cyber audits, security testing services and complete managed services for supply chain cyber risk management. Threat detection and response services include our Nightingale managed cyber security monitoring, our Trillion and Arc breached credentials tracking platforms, and incident response.

Crossword serves medium and large clients including FTSE 100, FTSE 250 and S&P listed companies in various sectors, such as defence, insurance, investment and retail banks, private equity, education, technology and manufacturing and has offices in the UK, Poland and Oman. Crossword is traded on the AIM market of the London Stock Exchange.

Visit Crossword at https://www.crosswordcybersecurity.com/

Crossword PR team
Ginger PR Ltd
+44 1932 485300
email us here
Visit us on social media:
LinkedIn