CYBERSECURITY TRENDS AND CHALLENGES AMONG IT PROFESSIONALS

New Research Highlights Data Breaches, Open Source Risks, and Network Vulnerabilities Among IT Professionals

ACDS
ADVANCED CYBER DEFENCE SYSTEMS

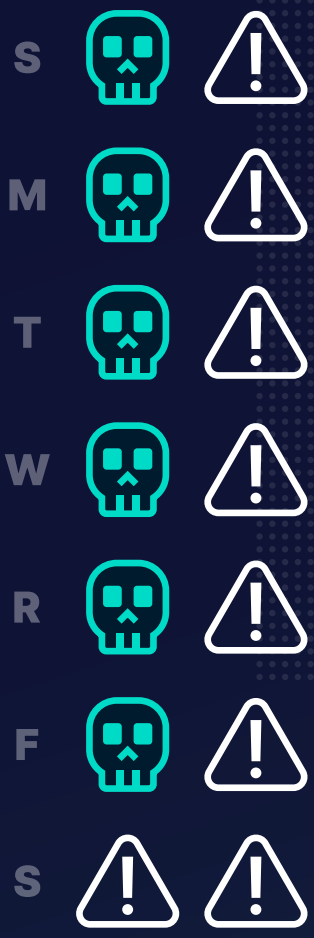
Advanced Cyber Defence Systems (ACDS) has unveiled the results of a survey of 250 IT professionals, highlighting significant cybersecurity challenges facing organisations today. The report, titled **Cybersecurity Challenges in 2024: Data Breaches, Open Source Risks, and Network Vulnerabilities**, offers an in-depth analysis of data breaches, detection times, reliance on open source software, network security issues, and the factors driving increased cybersecurity spending.

Key findings from the survey include:

FREQUENCY AND DETECTION OF DATA BREACHES

The relentless surge in cyber threats has become a defining challenge for organisations worldwide. **36% of organisations experienced three or more data breaches in the past 24 months.** This high frequency of breaches underscores the persistent and evolving nature of cyber threats, illustrating how cybercriminals continually adapt their tactics to exploit vulnerabilities. The sheer volume of breaches highlights the urgent need for organisations to enhance their cybersecurity defences to keep pace with the increasingly sophisticated threat landscape.

Compounding the issue, **20% of organisations took longer than five days to discover a breach**. This significant delay in detection can drastically amplify the damage inflicted by cyberattacks. The longer a breach goes unnoticed, the more time attackers have to exfiltrate sensitive data, disrupt operations, and potentially harm an organisation's reputation and financial standing. This prolonged exposure underscores the critical need for more effective monitoring and detection systems. Organisations must invest in advanced cybersecurity technologies, such as real-time threat intelligence and automated detection solutions, to identify and mitigate breaches more swiftly.



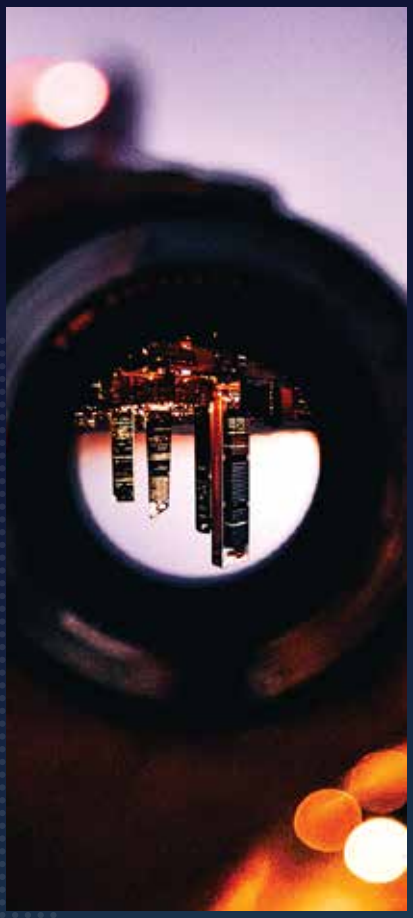
Together, these statistics paint a sobering picture of the current cybersecurity climate. The frequent occurrence of breaches and the delays in detecting them highlight vulnerabilities that cybercriminals are all too eager to exploit. In response, organisations are recognising the necessity of robust, proactive cybersecurity strategies to protect their assets and maintain trust with their stakeholders.

OPEN SOURCE PROJECTS

Open source software has become an indispensable component of IT infrastructure, driving innovation and efficiency across industries. While on the rise, actively funding open source software still is not the norm among organisations, **with only 39% of respondents reporting that their companies actively fund the open source projects they rely on**. These investments not only support the ongoing development and maintenance of these vital tools but also acknowledge their foundational place in modern technology ecosystems. However, it also raises important concerns about the security of these projects. As open source software becomes more integral to business operations, ensuring

its security is paramount to protect against potential vulnerabilities. Given this integral role played by open source software, we hope to see more companies materially investing staff time and resources into their protection.

There have been several notable contributions to the security of open source software by some of the big tech industry leaders in the past. In 2016, Google kicked off a project to run continuous scans of open source software packages.[1] They have since followed this effort up with funding for individual contributors integrating improvements into their scanning tools. More of this is needed by industry leaders and mechanisms should be improved to allow not just technical but also financial contributions from users of open source software to their improvement.



Over the past few years there has been a rise in the number of cyber attacks via widely used package managers to embed malicious code into systems.[2] A notable example of this is **the Python Package Index (PyPI), which over half of the respondents use**. PyPI has recently been highlighted for vulnerabilities and vulnerable packages[3], underscoring the inherent risks associated with open source software. Given its extensive usage, any security flaws in PyPI can have far-reaching consequences, potentially affecting countless applications and systems. This widespread dependency necessitates vigilant security practices, including rigorous code reviews, continuous monitoring, and timely updates, to mitigate risks and safeguard against exploitation.

Late in 2023, PyPI completed its first external security assessment, with funding provided by the Open Technology Fund, supported by the US

[1] https://security.googleblog.com/2023/02/taking-next-step-oss-fuzz-in-2023.html

[2] https://arstechnica.com/information-technology/2023/02/451-malicious-packages-available-in-pypi-contained-crypto-stealing-malware/

[3] https://securitylabs.datadoghq.com/articles/malicious-pypi-package-targeting-highly-specific-macos-machines/

Government as well as Okta and Github corporate social responsibility arms.[4] More programs like this are needed to help fund independent research on the integrity of critical software like package manager systems and the packages they deploy.

Together, these points emphasise a dual reality in the realm of open source software. While it offers significant benefits and efficiencies, it also demands a proactive approach to security. Organisations must balance their investment in open source projects with robust security measures to ensure that these critical tools remain reliable and secure. By doing so, they can harness the full potential of open source software while minimising the associated risks.

NETWORK DEVICES

When it comes to enterprise networks, maintaining comprehensive visibility over all connected devices is becoming increasingly challenging. Alarmingly, **50% of respondents acknowledged the likelihood that there are devices connected to their company's network that they are not aware of**. This lack of visibility poses significant security risks, as unidentified devices are likely not protected to the level set by the security team. These unmonitored devices can become entry points for cyber threats, bypassing traditional security measures and exposing the network to potential breaches and data loss.

The gravity of this issue is further underscored by the fact that **nearly 60% of respondents stated that insecure devices on their network would pose either a 'very high' or 'high' threat to their organisation**. This widespread recognition of the dangers associated with unsecured devices highlights the critical need for robust network security protocols. Organisations must implement continuous monitoring and comprehensive

[4] https://blog.pypi.org/posts/2023-11-14-1-pypi-completes-first-security-audit/

asset management strategies to identify and secure every device on their network.

Ensuring that all devices are accounted for and properly secured is essential to mitigate the risks posed by potential vulnerabilities. Advanced security solutions, such as automated network scanning tools and real-time threat detection systems, can help maintain visibility and protection across the entire network. By prioritising these measures, organisations can significantly reduce the risk of cyber threats originating from unknown or insecure devices, thereby safeguarding their critical assets and maintaining the integrity of their operations.

TRIGGERS FOR INCREASED CYBERSECURITY SPENDING

Organisations worldwide are increasingly recognising the need to bolster their defences against sophisticated threats. Recent events have particularly underscored this necessity, leading many to significantly increase their cybersecurity budgets. Respondents cited three standout occurrences when asked about the most influential incidents prompting this shift.

Nation-state attacks, specifically suspected targeting of UK electoral systems by Chinese state-affiliated actors.

The threat of nation-state attacks has loomed large, with one particularly alarming incident involving the suspected targeting of UK electoral systems by Chinese state-affiliated actors. This high-stakes cyber espionage underscored the vulnerabilities inherent in critical national infrastructure and the potential for foreign interference in democratic processes. The implications of such an attack are profound, pushing organisations to invest more heavily in advanced threat detection and prevention measures to safeguard national security and public trust.

XZ Utils backdoor, an open source vulnerability.

The discovery of a backdoor in XZ Utils, a widely used open source project, sent shockwaves through the cybersecurity community. Open source software, while often praised for its transparency and collaborative development, also presents unique security challenges. The XZ Utils backdoor highlighted the risks associated with dependencies on open source projects, prompting companies to allocate additional resources towards code auditing, vulnerability management, and ensuring the integrity of their software supply chains.

MOVEit breach, a significant supply chain attack.

The MOVEit breach represented a significant supply chain attack that further accentuated the interconnected nature of modern business operations. By compromising a popular file transfer application, attackers managed to infiltrate numerous organisations, demonstrating the cascading effects such breaches can have across industries. The MOVEit incident galvanised firms to reassess their third-party risk management strategies and enhance their defences against similar supply chain threats, investing in more comprehensive security solutions and incident response capabilities.

These three incidents collectively served as a wake-up call, driving home the critical importance of robust cybersecurity measures.

The survey findings underscore the pressing cybersecurity issues organisations face, including frequent data breaches, delayed threat detection, dependence on potentially vulnerable open source tools, and substantial network security blind spots. These challenges point to the urgent need for more robust and proactive cybersecurity measures. Organisations must continuously invest in security technologies, enhance monitoring and detection systems, and develop comprehensive strategies to manage and secure all connected devices.
To effectively address these challenges, organisations must stay vigilant and adaptive, anticipating emerging threats and responding swiftly to incidents to safeguard their digital assets and maintain operational integrity.

SURVEY METHODOLOGY

This online survey commissioned by Advanced Cyber Defence Systems (ACDS) and conducted by market research company OnePoll, targeted 250 cybersecurity decision-makers at companies with over 500 employees. It was carried out between 30th April and 8th May 2024, in accordance with the Market Research Society's code of conduct.

UNDERSTANDING AND SECURING YOUR ATTACK SURFACE

Advanced Cyber Defence Systems (ACDS), a UK based cyber security company, is a disruptor in attack surface management with ACDS OBSERVATORY. ACDS integrates multiple massive data sources into its powerful anomaly detection engine, identifying configuration errors and vulnerabilities that often go undetected by others. Regular monitoring of an organisation's external attack surfaces for changes and new assets will alert of any weakness or vulnerability that might be exploited.

ACDS assists customers in discovering all their internet-facing devices and assets, including IT (on-premises, cloud, hybrid), Operational Technology, IoT, Shadow IT, and unapproved personal devices. This enables immediate action on critical vulnerabilities through its proprietary risk identification and prioritisation algorithm.

For more information, contact: info@acdsglobal.com

www.acdsglobal.com

ACDS
ADVANCED CYBER DEFENCE SYSTEMS