

MARKET UPDATE

Emerging vulnerabilities in PHP and potential claims implications

Incident Overview

Newly identified security vulnerabilities in PHP, a programming language widely used across websites globally, have resulted in multiple websites being taken offline amid concerns over potential exploitation.

The vulnerabilities may enable a range of attacks, including remote code execution, denial of service and unauthorised access to information.

In response, PHP has released two security updates and urged organisations to identify all affected installations, prioritising internet-facing systems, and apply the relevant patches as a matter of urgency. Where immediate patching is not possible, organisations have been advised to isolate affected systems from public networks until remediation is complete.

Given the widespread deployment of the programming language, the potential exposure extends across multiple platforms, industries and jurisdictions. While this creates the potential for a significant increase in cyber incident notifications, precautionary enquiries and claims activity, the ultimate insured loss impact remains uncertain and will depend on multiple factors such as the extent of exploitation, resulting business disruption and the availability of policy coverage.

Risk Management and Incident Response

The immediate priority for organisations is to establish whether their systems are affected, assess the extent of their exposure and implement appropriate mitigation measures. These include identifying vulnerable installations, applying security updates, reviewing system logs and monitoring for indicators of attempted or successful exploitation.

Organisations are also seeking guidance on potential exposure and appropriate response measures. This is driving precautionary system shutdowns, forensic investigations, incident-response engagements and Notices of Potential Claim (NOPCs), including in circumstances where no confirmed compromise or insured loss has yet been established.

The distinction between precautionary action and a confirmed cyber incident will be important when assessing the resulting claims and determining whether policy triggers have been satisfied.

Key Claims Considerations

Business Interruption (BI)

Business Interruption is likely to be a key consideration for many organisations, particularly where affected businesses have taken systems offline to facilitate patching or contain a suspected threat.

Where systems are taken down temporarily to apply security patches, insurance policy waiting periods and the requirement for a covered security event may limit the scope for recovery. Conversely, more material exposures are likely to arise where a threat actor successfully exploits the vulnerability, leading to system compromise, data exposure or prolonged business interruption.

Security Conditions, Patching and Legacy Systems

Policy terms relating to minimum security standards, vulnerability management, timely patching and the use of unsupported or legacy systems may also be material to coverage assessments.

Third-Party Liability and Subrogation

Where website hosting, infrastructure management, patching or other relevant security responsibilities have been outsourced, questions may arise regarding the allocation of responsibility for identifying and remediating the vulnerabilities. This could give rise to professional liability claims against service providers, as well as potential subrogation claims.

Outlook for Cyber Claims

This incident demonstrates how rapidly a vulnerability affecting widely deployed technology can develop into a cross-sector, multi-jurisdictional event. It further highlights the concentration and risk aggregation inherent in organisations' growing dependency on shared digital infrastructure and technology providers. The immediate impact may be reflected in increased enquiries, precautionary notifications, forensic investigations and incident-response costs, even where confirmed exploitation is limited.

More broadly, the event reinforces the insurance industry's increasing focus on cyber as a distinct and systemic risk class, while also highlighting the growing influence of artificial intelligence on threat actor capability and the frequency, scale and sophistication of cyber events across multiple lines of business. This aligns with Crawford's increasingly integrated Cyber & Technology proposition, recognising that technology driven incidents can give rise to interconnected exposures spanning Marine, Major & Complex Loss, Renewables, Technology Professional Indemnity and other specialist disciplines.

Global Response and Client Support

Crawford is available 24/7 to support clients worldwide. Our ability to mobilise specialist cyber resources globally, coordinate a consistent response across regions and scale rapidly enables us to support clients and insurers facing multiple potentially affected insureds.

Providing claims management leadership throughout, we are supported by a leading global network of contracted incident response, forensic, legal, notification and recovery specialists, enabling us to manage surge events and deliver a coordinated response from first notification through to recovery and claim resolution.

Our teams can also engage during the early risk-management and incident-response phase, helping clients assess potential exposure, coordinate specialist investigations and establish the facts needed to inform subsequent claims handling and coverage considerations.

Should you require any support, please contact one of our global experts.

Global coverage with local insight



CANADA

Rob Holmes

M: +1 289 684 3501
E: robert.holmes@crawco.ca

USA

Robert Welsh

M: +1 646 627 5713
E: robert_welsh@us.crawco.com

LATAM

Javier Yanez

M: +56 9 9743 1791
D: +56 2 2676 9239
E: jyanez@crawford.cl

SPAIN

Jaime Jalvo

M: +34 609 555 353
D: +34 917 713 600
E: jjalvo@crawford-spain.com

CENTRAL EUROPE/BENELUX

Derk Bruintjes

M: +31 6 23 36 61 01
D: +31 55 53 80 040
E: derkbruintjes@crawco.nl

UNITED KINGDOM

David Stirling

M: +44 07385 667904
E: david.stirling@crawco.co.uk

NORDICS

Oystein Gunleiksrud

M: +47 414 10 052
E: oystein.gunleiksrud@crawco.no

MIDDLE EAST/AFRICA

Ibrahim Mashal

M: +971 50 795 0424
D: +971 (0) 2 622 8114
E: ibrahim.mashal@crawco.me

EASTERN EUROPE

Piotr Wagner

M: +48 505 121 321
E: piotr.wagner@crawco.pl

GERMANY/SWITZERLAND

Andreas Zerres

M: +49 160 987 126 57
E: andreas.zerres@crawco.de

ASIA

Mark Adderley

M: +66 80 628 3232
D: +66 2676 5353
E: marka@crawford.asia

AUSTRALIA/NEW ZEALAND

Lucas Bressanutti

M: +61 448 600 557
E: lucas.bressanutti@crawco.com.au

For more information, visit our [website](#).

About Crawford & Company®

For over 85 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.

10K employees | **50K** field resources | **70** countries | **\$20B** claims managed annually