Information Security Forum Explores the Risks and Challenges of Open Source Software

Latest Digest Helps Security Professionals Recognize the Challenges and Appreciate the Benefits of Using Open Source Software

According to the Information Security Forum (ISF), trusted resource for executives and board members on cyber security and risk management, open source software (OSS) is emerging as a core part of IT infrastructure and applications, largely due to the growing popularity of agile development methodologies and DevOps practices. With a substantial number of commercial and custom-made applications incorporating OSS, it cannot, and should not, be ignored.

In an effort to support global organizations, the ISF announces the release of Deploying Open Source Software: Challenges and Rewards, helping security professionals recognize the benefits and perceived challenges of using OSS and set up a program of protective measures to effectively manage OSS. OSS is often seen as being insecure and unsupported. As these negative connotations continue to taint its reputation, some organizations officially prohibit it, even though they may unknowingly be using OSS. Others enthusiastically adopt OSS, harnessing its advantages, such as aiding flexible and rapid development. The latest paper from the ISF demonstrates that OSS can be a positive influence on software development, if used and managed responsibly.

“Many organizations are adopting agile and DevOps methodologies, which is driving an increased uptake of OSS and, in turn, the creation of new mixed source applications,” said Paul Holland, Principal Research Analyst, ISF. “The growing prevalence of OSS needs to be balanced by a concerted effort to manage its use appropriately and effectively. For some organizations, the first step is to realize that the myths surrounding OSS are simply illusions. For other organizations, the appeal of OSS and mixed source software is already apparent, allowing them to develop new applications securely and increase speed to market for new ideas.”

With OSS becoming commonplace within organizations, it brings a different set of risks and perceived challenges compared to closed source (proprietary) software. Establishing the difference between the myth and the reality will be critical to securing OSS. As it becomes the mainstay within application development and infrastructure, security professionals will need to understand OSS and manage the challenges associated with its components. Fixes to these security challenges should be implemented as part of an OSS management program, led by a senior individual appointed to the role of OSS Program Manager. Integrating all these measures into a single, overarching program will enable a holistic and coordinated approach to managing the risks of OSS.
The OSS Program Manager should be supported with the necessary funds and resources to develop a viable program and team. While in some instances, existing tools for closed source software can be extended to secure and manage OSS, the program team may need to procure additional tools to further enhance OSS security. The team should also monitor threat intelligence feeds for mentions of OSS components that the organization is using.

“Resisting the move to OSS could limit an organization’s ability to progress and evolve. If harnessed effectively, OSS can potentially be an accelerator for the business,” continued Holland. “Fostering an OSS management program is therefore vital to securing and managing OSS, allowing the organization to use it safely. Combining this with established practice around the management of closed source software will deliver a coherent, all-encompassing software management program, providing the best opportunity for success.”

With many traditionally closed source software vendors adopting OSS principles, OSS is here to stay. The flexibility of both open and mixed source software could lead to a decline in closed source software, resulting in a fundamental shift in software management, licensing and security. Organizations must be prepared.

*Deploying Open Source Software: Challenges and Rewards* is available now to ISF Member companies via the [ISF website](http://www.securityforum.org).

---

**About the Information Security Forum**

Founded in 1989, the ISF is an independent, not-for-profit association of leading organisations from around the world. The organisation is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

For more information on ISF Membership, please visit [www.securityforum.org](http://www.securityforum.org).