

# Application Security – No Longer a Pipe Dream



Security professionals who find themselves struggling to chart a course through the application security minefield can take heart in the emergence of new tools and actionable techniques. The choice of which to use will depend very much on what's appropriate for your specific business' dynamics. What's important is that a strategy is selected and implemented as part of a robust information security management system.

Application security continues to represent a thorn in the side of many organisations' IT leaders. Over the years, various efforts have been made to assist organisations in understanding and mitigating application security risks. These include the emergence

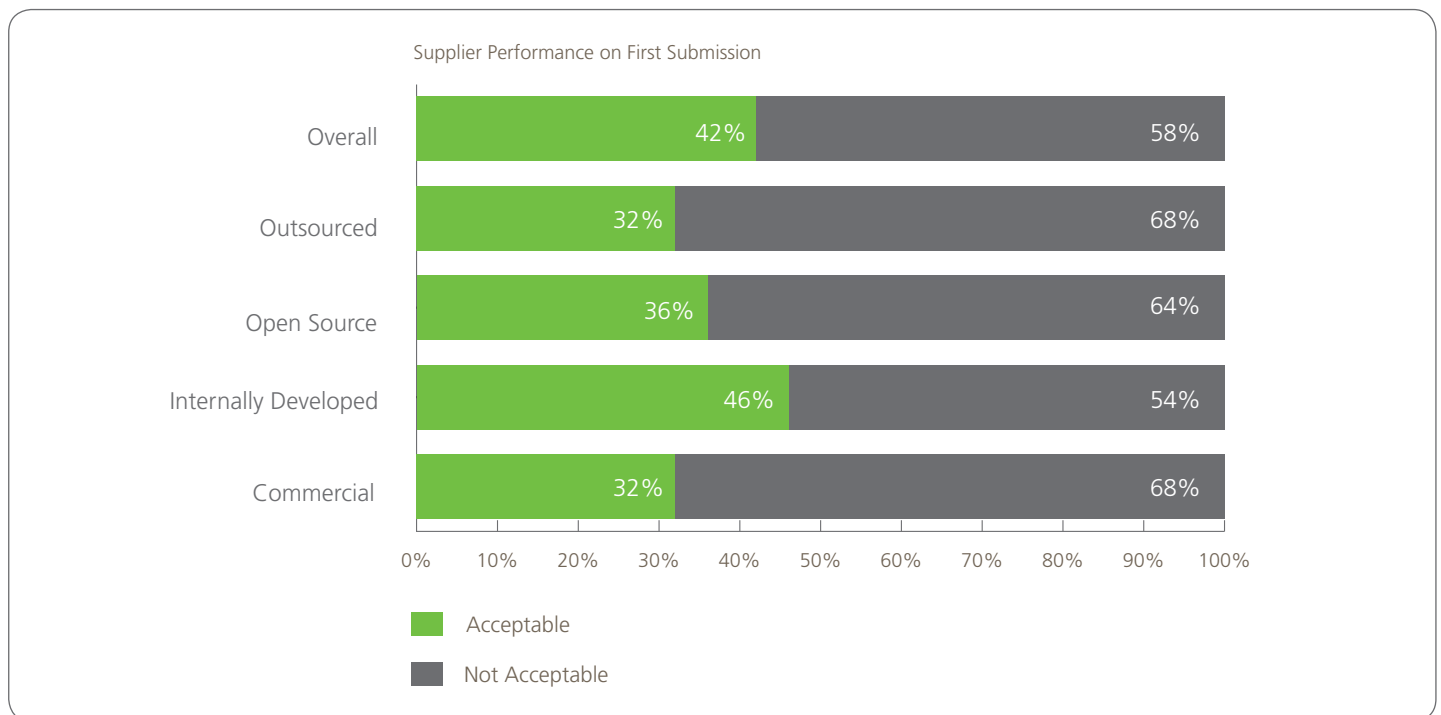
of communities and organisations such as the Open Web Application Security Project, and the Web Application Security Consortium. In addition, a variety of certifications specifically aimed at secure development practices strive to educate developers and security professionals about secure software design and coding. A number of secure development lifecycle approaches, frameworks and maturity models are also easily accessible.

Despite this abundance of resources, as well as a focus on application security and flaws attracting increasing levels of attention and press, application security still has some work to do on its reputation. Recent research confirms that that this remains an area of critical failing and risk.

Consider figure below, which appears in the Veracode<sup>1</sup> State of Software Security – Volume 3 report<sup>2</sup>.

**Despite this abundance of resources,** as well as a focus on application security and flaws attracting increasing levels of attention and press, application security **still has some work to do** on its reputation.

**Figure 1 – Acceptability of software security by supplier**



<sup>1</sup> [www.veracode.com](http://www.veracode.com)

<sup>2</sup> <http://info.veracode.com/state-of-software-security-report-volume3.html>

The issues are prevalent among open source, internally developed applications, as well as those developed by commercial providers of software – all suffering equally from security flaws and vulnerabilities.

### What's the impact?

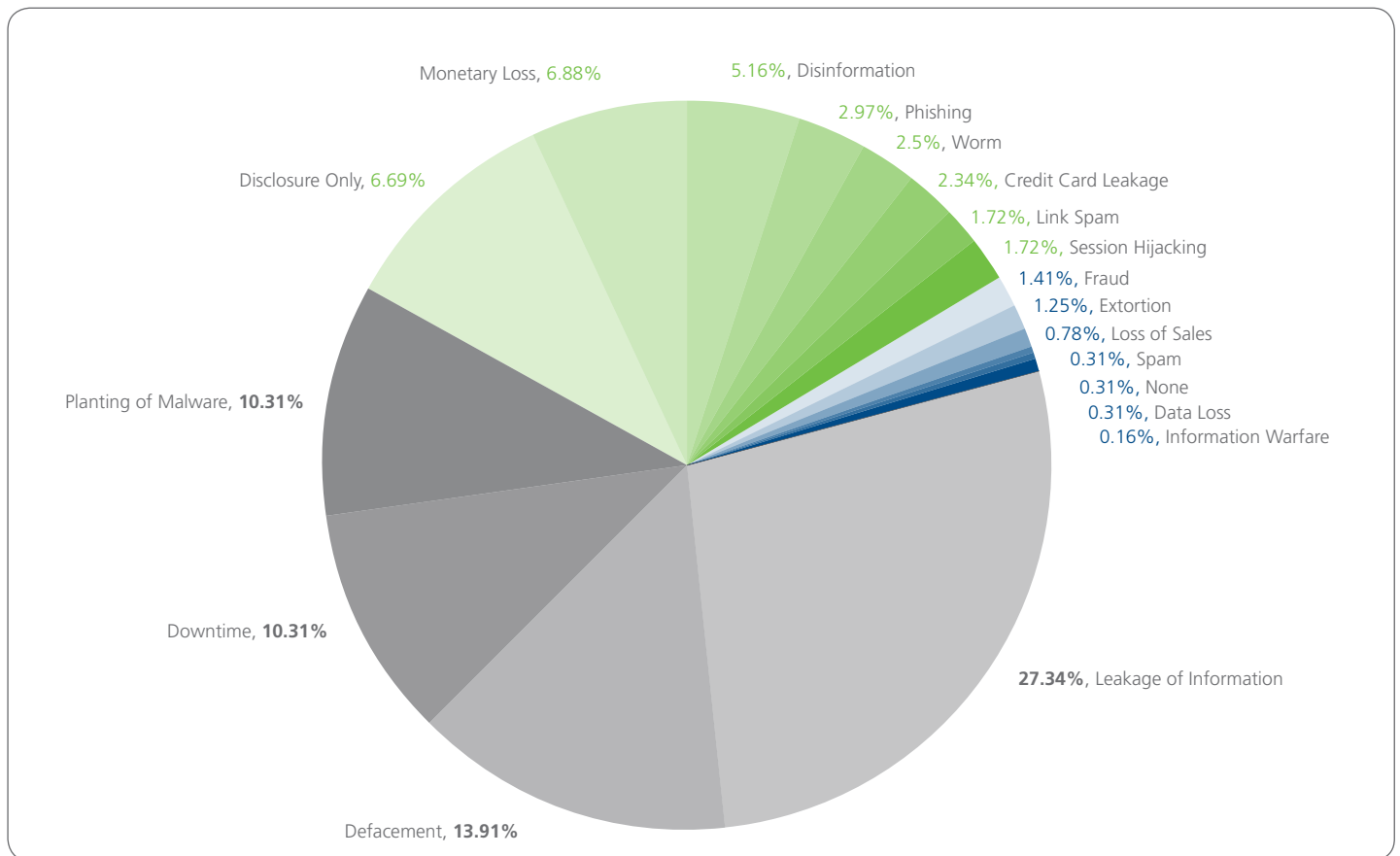
Software security flaws considered in isolation are difficult to contextualise unless the impact of the attack is quantified into something more tangible. The following data, drawn from the WASC's Web Hacking Incident Database, highlights the most common implications of web application attacks.

These statistics highlight the fact that data leakage is the primary casualty of application compromises. Considering that data is the lifeblood of most businesses, such attacks can seriously damage many organisations.

“The number of high-profile compromises and data theft for 2011 alone is alarming, and the trend is set to increase with the continued proliferation of mobile devices and applications and within businesses” says Nicholas Arvanitis, a Principal Security Consultant at Dimension Data.

“Mobile application security has been found wanting. SaaS and the advent of cloud solutions and delivery of data and core business services via the Web will only increase business' reliance on applications.”

**Figure 2 – Top Attack Outcomes –Web Hacking Incident Database**



Software and tool vendors promote **the value of automating static analysis and dynamic analysis** through their software solutions, and providing developers with the means to **assess the security of their own applications seamlessly**.

### Regulation and reputation

The need to put in place an actionable plan with respect to application security becomes even more critical, when you consider that organisations in all industry verticals are facing increasing pressure to protect sensitive or regulated data.

“These regulatory requirements are becoming far less toothless than initially perceived,”

says Arvanitis,

“with considerable civil and criminal penalties levied for improper protection and handling of information covered by the various regulations and standards.

“Of course, regulation is not the only driver – many organisations are at significant risk of compromise of client or internal information, and the associated impact on brand and reputation is often more costly than any penalties levied.”

“For instance, the widely publicised compromise of HBGary resulted in the contents of the organisation’s e-mail server being posted online, among other consequences. These included the CEO of HBGary Federal having his personal details posted publicly, and finally resigning. During the attack, additional damage included the leakage of various other compromises of high profile organisations.”

“The compromise of a web application played a key role in this attack, and it bears mention that the target was a security company – an organisation whose core focus is information security.”

Incidents such as this and the increased focus on protecting data have forced many organisations to take action to adjust their risk profile.

### Security assessment and testing

Security assessment and penetration testing are essential components of understanding the risks and exposures of critical data. A means of empirically determining and validating vulnerabilities that lead to compromised data will assist organisations in pinpointing the glaring risks that should be focused on as a priority, reducing the overall risk systematically.

Effectively assessing the security posture of an organisation and the threats to its protected data is best achieved through a combination of network-level and application-level assessment and penetration testing. However, at present, there is a lack of consensus regarding the best approach to testing application security within a Secure Development Lifecycle. Organisations are faced with a multitude of options in terms of tools, vendors, consultants, and approaches:

- External consultants aim to provide manual source code reviews, or static analysis, as well as penetration testing services
- Software and tool vendors promote the value of automating static analysis and dynamic analysis through their software solutions, and providing developers with the means to assess the security of their own applications seamlessly
- Other players espouse the benefits of a complete life cycle approach to security throughout the software development lifecycle

Which approach is appropriate? As with any aspect of information security, there’s no one-size-fits-all solution for any business. Further, each distinct approach has various benefits but, conversely, brings its own drawbacks. A mature approach will encompass a software security initiative that spans the entire software development lifecycle. However, for many organisations, this is labour-intensive and cost-prohibitive, which oftentimes leads to security initiatives stalling or the organisation defaulting to a traditional approach. This, in turn, results in incomplete coverage and an inherently tactical, responsive approach to application security.

### How SaaS can assist

SaaS has proven to be an effective and powerful means of lowering the total cost of ownership (TCO) of a variety of business functions.

The explosion of cloud services and offerings, ranging from full CRM tool suites, such as those offered by Salesforce.com to file storage and transfer solutions such as DropBox, has resulted in a significant shift in traditional business and technology paradigms.

The power of SaaS can also be leveraged in a blended approach to security testing and assessment, which combines automated and dynamic techniques with tailored and focused manual analysis, effectively providing the best of all approaches while limiting unnecessary overheads.

This is an effective way of reducing overall TCO and allowing organisations to focus on their core competency, while increasing security posture without the overheads traditionally associated with such an effort.

Perhaps more importantly, this approach can address some of the shortcomings of stand-alone assessment efforts being cobbled together in a piecemeal fashion.

Finally, a single portal, providing an integrated dashboard and overview of applications assessed either statically, dynamically or manually, or indeed all three, is extremely useful to developers or security professionals tasked with addressing vulnerabilities and flaws.

## Entrenching application security

If you want to gain the trust of your customers, whether they are internal users or the general public, you need to protect the applications that safeguard the data that the user cares about. Application security isn't an insurmountable challenge. There are tools and resources available. 'Application security' is not an oxymoron either, but it's up to each organisation to take a thorough investigation and appraisal of the tools and approaches available and entrench application security within its own information security management system.

If you want to gain the trust of your customers, whether they are internal users or the general public, **you need to protect the applications that safeguard the data** that the user cares about.

### **Dimension Data's Security Review and Assessment**

Dimension Data has developed a Security Review and Assessment methodology based on leading industry practices that address an organisation's risks through various services. This structured and field-proven assessment methodology has been applied and enhanced over the course of 15 years' experience in providing these services to the industry.

The combination of this background, experience and credibility, together with leading SaaS security service models and technologies allows us to develop a comprehensive and cost-effective approach to mastering the challenge of application security.

Dimension Data conducts key application assessment and security activities to assist our clients in understanding and addressing the inherent risks to protected data and core business functions. This is achieved through empirical enumeration of application vulnerabilities, followed by realistic, prioritised and immediately actionable remediation recommendations.

This provides a clear snapshot of the potential impact of flaws. The findings of the assessment may be indicative of deeper-seated underlying issues that are potentially the root cause of flaws pervasive throughout other aspects of the organisation. SaaS and tailored consulting services can be combined to address these issues in a scalable, efficient and effective manner.



**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • CONGO  
DEMOCRATIC REPUBLIC OF THE CONGO  
GABON • GHANA • KENYA  
MADAGASCAR • MALAWI  
MAURITIUS • MOROCCO • NAMIBIA  
NIGERIA • SAUDI ARABIA  
SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES • ZAMBIA

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES