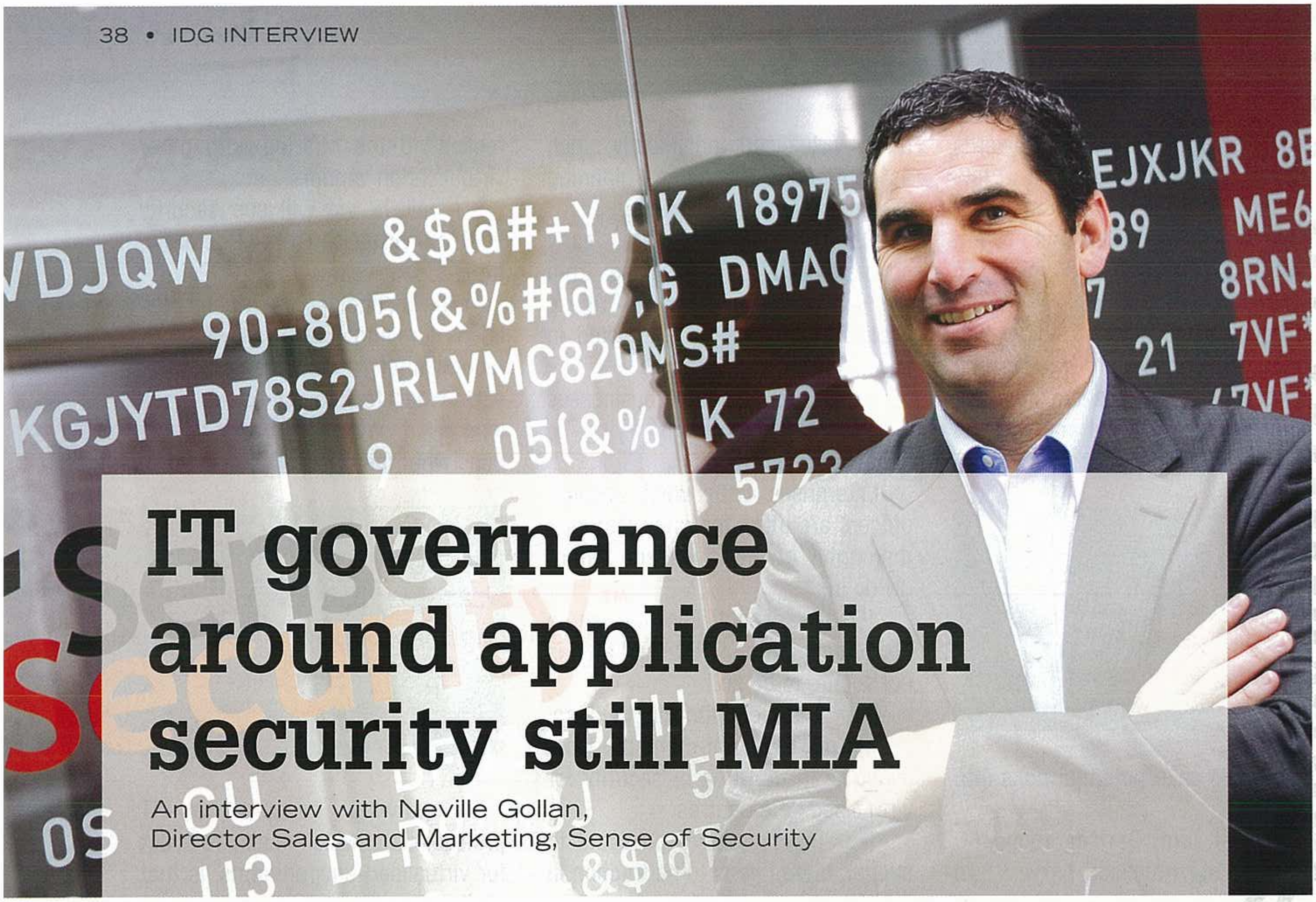

IT governance around application security still MIA

An interview with Neville Gollan, Director Sales and Marketing, Sense of Security

Web application development teams are still leaving security concerns by the wayside when pressure mounts to get an application online as quickly as possible.

"Security and risk teams at organisations know Internet facing applications should have penetration testing performed," Sense of Security Sales and Marketing Director, Neville Gollan, says.

"But due to the common cultural aspect on how applications are designed, more often than not security practices throughout the development lifecycle are overlooked."

"Some of these applications are critical to an organisation's marketing strategy and can be the game changers.

"The pressure mounts to get the application live as soon as possible and development teams often ignore security in the design and development stages, focussing on features and functions only."

As the development of specialised online applications are frequently outsourced, Gollan says third party development firms are generally not clear about the security requirements of an organisation, particularly if the organisation lacks structured secure development practices.

Gollan believes businesses, incorrectly, can be more relaxed about security best practices when using an outsourced provider.

"Many organisations consider that, since they are using a reputable development firm, they must be developing securely.

"There is often nothing in the contract about developing applications to a security standard and the code being audited during the development process."

Penetration testing, a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, can also be a half-hearted affair.

"All penetration tests need to be conducted comprehensively. A lot of companies are satisfied with rudimentary testing only and go live with significant risk.

"Most organisations assess application security at the end of the development lifecycle — they build the features and functions and security is often overlooked."

Gollan says best business practice for the development of a Web-based application would include the establishment of a standard that clearly outlines the security requirements before the development commences.

Source code auditing tools are also essential. Access to these tools enables the development team to assess the code for vulnerabilities throughout the development stages.

> **"There is often nothing in the contract about developing applications to a standard and the code being securely audited during the process."**
>
> Neville Gollan, Sense of Security

Gollan says source code-auditing tools must be able to perform static code analysis without having to compile the code into its final state prior to testing.

"Doing the code reviews regularly can help streamline the remediation effort.

"An independent organisation should then be engaged to conduct comprehensive penetration testing and the developers' then need to fix all the issues before the application is placed into production."

The policies and procedures established around security during the development lifecycle of the application can then be replicated for future development projects.

Gollan says Sense of Security's observation of small to medium enterprises is that those that have proper secure application development procedures are in the minority, less than 20 per cent.

The impact of not having secure applications in place can, among other issues, be detrimental to an organisation's brand and cost the organisation in lost revenue if an incident occurs.

The upside to employing secure application development practices are numerous.

"The development team is more responsible and comprehensive, the development team code securely and the application is far less likely to fall victim to incidents and require adhoc remediation, so the business saves money there.

"The business also does not have to worry about loss of brand, equity and future revenue," Gollan says, adding often applications can go live more quickly than otherwise if security is imbedded into the development lifecycle.

"There is less likely to be a high volume of issues identified during the penetration test. On the whole it is a more efficient way of bringing an application to market, quicker and more secure."

Employing a security framework around the development of online applications, in the end, comes down to good IT governance.

> **"Most organisations assess application security at the end of the development lifecycle — they build the features and functions and security is often overlooked."**
>
> Neville Gollan, Sense of Security