



Information Security Pointers



Copyright and Disclaimer

© Boojum Pty Ltd 2003 - 2010 All Rights Reserved

Boojum Pty Ltd has supplied these materials in good faith, based on information known to us at the time of production. To the extent permitted by law, Boojum Pty Ltd and its employees, agents and consultants will not be held liable for any loss or damage (including indirect, special or consequential loss or damage) arising from the use of, or reliance on, the Information or Products it supplies, whether or not caused by any negligent act or omission. If any law prohibits the exclusion of such liability, Boojum Pty Ltd limits its liability to the extent permitted by law, to the re-supply of the Information or Products.

Revision History

Version	Description and reason for change	Author	Date
1.00	Initial draft	Dr R Hall	24 Jan 2010
1.01	Revised draft	Dr R Hall	25 Jan 2010
1.02	Edited and reformatted	R Maxwell	18 Feb 2010
1.03	Statistics display improved	R Maxwell	22 Feb 2010

Contents

Information Security	3
<i>Why take information security seriously?</i>	3
Action 1: Stay aware of the trends.	3
Action 2: Build checks and balances into software.	4
Action 3: Insist that your web applications are up to scratch, built to withstand at least the current OWASP Top 10 security breaches.	4
Action 4: Make use of the tools at your disposal.	5
Action 5: Keep the Rules of Thumb in mind.	5

Information Security

Why take information security seriously?

If you believe cyber attacks don't happen here, security vendor McAfee claims that 33 per cent of Australian businesses experienced a security incident in 2009.

The average financial loss per reported incident was \$34,000 in revenue, plus companies had to spend an average \$37,000 to fix the problem¹.

Willing to take about a one-in-three chance of being out of pocket \$70,000?

We don't think that it is worth the risk.

These 5 actions can significantly reduce the risk of data loss.

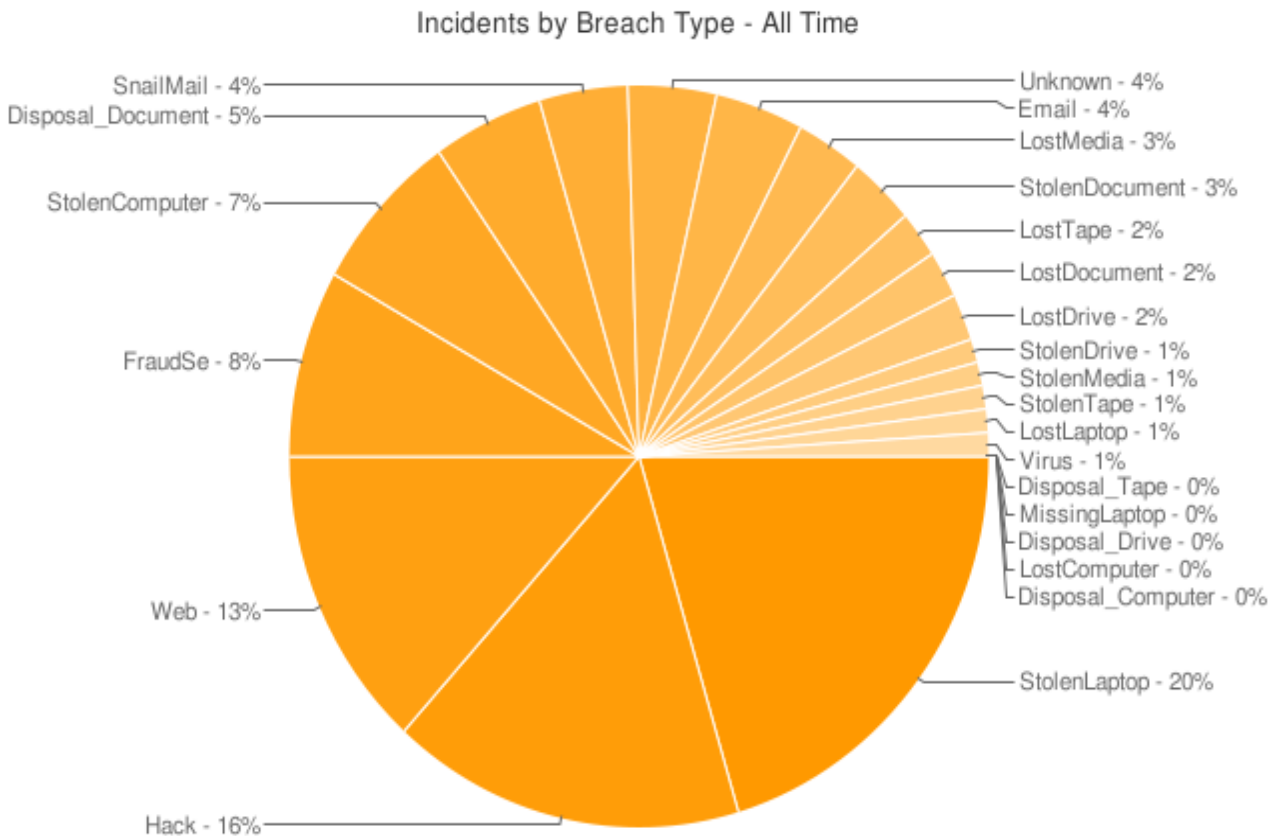
Two things you can do right now:

Stolen computers account for around 27% of information security breaches.

- Make sure all your desktop and laptop computers are secured by security cables.
- Make sure all your computers have strong password protection.

Action 1: Stay aware of the trends.

There are many reputable websites around with good advice that you should browse (eg. Cisco, Symantec). We recommend the Open Security Foundation website because it is a non-profit public organisation. Its DataLossDB Statistics web page¹ gives a good snapshot of the distribution of various aspects of data loss. For example, here is a snapshot of two important graphs (taken 15/1/2010).



¹ <http://datalossdb.org/statistics>

Action 2: Build checks and balances into software.

Software should not be made where there is any possibility of:

- Being unaware of undesirable changes to mission critical data and who made these changes.
- Being unable to reverse any change in the system.

Given the DataLossDB Statistics that ~30% of data loss incidents are caused by the users of the software, building checks and balances makes sense.

Action 3: Insist that your web applications are up to scratch, built to withstand at least the current OWASP Top 10 security breaches.

The Open Web Application Security Project² is also a not-for-profit organization focused on improving the security of application software. The OWASP Top 10 for 2010 are:

- Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration
- Failure to Restrict URL Access
- Unvalidated Redirects and Forwards
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection

Given that most data loss incidents are caused by people external to the organization, it is certainly worth taking care of the well-known low-hanging fruit.

² http://www.owasp.org/index.php/Main_Page

Action 4: Make use of the tools at your disposal.

Make sure that the following tools are turned on:

- Automatic patches for operating systems and applications.
- Firewalls and browser security features.

New patches for software are released all the time. Lean towards software that automatically updates itself. Who wants to have to think about having to update software? What is the use of anti-virus software that is out of date?

Action 5: Keep the Rules of Thumb in mind.

Recommended Reading:

- 10 Immutable Laws of Security - <http://technet.microsoft.com/en-us/library/cc722487.aspx>
- 10 Immutable Laws of Security Administration - <http://technet.microsoft.com/en-us/library/cc722488.aspx>