BBD VIEW

9 TIPS TO SOFTWARE **CYBERSECURITY**

By Mike Geyser, BBD Tech Team Leader

www.bbd.co.za

PROTECTING CLIENT INFO IS KEY

27 Oct 2017

The heated commentary on South Africa's Cybercrimes and Cybersecurity Bill, the petition against it and the increased risk of global cyber attacks have placed large enterprises under pressure to ensure they have the most stringent cyber security.

The 2017 Ponemon Cost of Data Breach Study shows that data breaches cost South African companies R32 million and response fees cost (on average) R8.1 million - with malicious and criminal attacks being the most common data breaches in South Africa.

How would a big business go about ensuring their data is protected? Despite the myriad of tips floating around on the Internet, your first port of call is to understand the intricacies of cyber security.

I can easily chat about cyber security at length, as most organisations don't realise how very broad a topic it is. The first step is to understand the three cyber security levels required by organisations:

- **Infrastructural security:** protecting your systems and networks from viruses, spyware, worms and hackers;
- **Informational security:** protecting physical and digital data from unauthorised access, use, disclosure, disruption or modification;
- **Software security:** ensuring your coded software is not the weak point in your organisation's security. The last thing any business needs is for their software to be low-hanging fruit for unwanted parties.

> **"You will never be perfectly secure, but your aim should be a high percent coverage. Even a small breach, is a massive risk, especially when you're dealing with sensitive client information."**

Below are a few quick tips on protecting sensitive client information:

1. Quantify and understand your security exposure with a specialist company.
2. Restrict unnecessary software on your systems.
3. With cloud computing and the risk of threats at an all-time high, treat everything as hostile.
4. Secure your admin pages, even from your own users.
5. Look at having your internal departments treated as hostile to each other by your firewall. This will mean you have smaller "inside" fenced areas on your network.
6. Have tough access control, limit your access environment.
7. Regularly change passwords and use salted password hashing and encryption (and obviously don't write them down).
8. Limit uploads to reduce that threat vector.
9. Most importantly, educate your staff on everyday cyber security habits.

Ultimately, to protect your client information you need to make sure that everything has been coded defensibly. Without this, your enterprise could be at risk.

About Mike Geyser

Mike is part of BBD's R&D team involved in industry research, consulting and training. A Google Developer Expert (GDE), Mike is the only Web Technologies GDE in South Africa. He is also very passionate about the tech community and organises the local JavaScript, Jozi.JS and official Docker Johannesburg meetup groups.

About BBD

A provider of custom software development and application design solutions, BBD's 34 years of technical and developer expertise spans the banking, insurance, telecommunications, education and public sectors. Employing over 700 highly skilled, motivated and experienced IT professionals - BBD is South Africa's largest independent custom software development company.