

NSW GOLF CLUB SINKS I.T. EAGLE

Innovation
Saves Thousands



When NSW Golf Club's IT consultant went missing in 2007 it could have been a calamity. Instead it proved fortuitous, opening the door to a new relationship that has saved the club tens of thousands of dollars.

For Warren Begg, the club's Assistant Manager to whom responsibility for all things IT falls, the relationship means far more - peace of mind and a sound sleep every night.

"Certainly at that time we were very vulnerable," Warren recalled. "Our previous supplier had vanished and even when he was around he just hadn't been responsive, let alone proactive."

Virtually within weeks of calling in club industry expert Jason Drew of Secom Technology, the club went from vulnerable to bullet proof. Problems as diverse as mountains of spam emails and a lack of connectivity for the all-important grounds staff disappeared.

When Jason first walked into the club, management's major challenge was a two-year-old works depot with only a dial-up connection and no connectivity with the club-house.

Anyone with the most rudimentary of knowledge on the benefits of remote control access for irrigation equipment and the importance of information sharing by professionals could see that this was a major obstacle to operations of this prestigious world ranked golf club.

10 Steps to Web Security

- 1. Ensure updates and patches are completed including Microsoft Office applications:** All operating systems are vulnerable but updates minimise security compromises.
- 2. Don't use personal media on work computers:** Using the same USB device between work and home can infect the office network.
- 3. Avoid email attachment links:** Links can be more insidious than attachments, leading you to sites that appear legitimate and seek private information.
- 4. Local Firewall enabled on personal PC:** Ensure your Antivirus has end point internet security protection. At a minimum ensure Windows Firewall is enabled and antivirus is operational and updated.
- 5. Use separate emails for social media sites:** When using multiple social media sites, register separate emails with each site. Avoid registering company email address within social media sites.
- 6. Safe Surfing:** DO NOT click on banners and ADs which say something like "You have caught a virus, click here for a full system scan" or "You are a Winner", these are viruses and spyware.
- 7. Encrypt files and folders using software such as Truecrypt:** Encrypt and password protect sensitive material.
- 8. Dont use bank sites via free wifi services:** Many free wifi services allow packet sniffing.
- 9. Change home wireless router password:** Ensure WPA encryption is enabled as a minimum, consider security measures such as Mac address locking and disable the SSID broadcast option.
- 10. Change logon user:** Create a separate non administrator user to log on to the PC. With limited local security rights you will not unwittingly install software when surfing the internet.

BYOD: The Next Threat To Clubs?

Proactive Strategy Needed

THE latest IT acronym, BYOD, could well come to mean Bring-on Your Own Demise for club IT managers without both eyes on security vulnerabilities.

Bring Your Own Device, as it actually means, is a good thing for clubs, part and parcel of improved communications, workflows and efficiencies with employees using their own iPhone or Android to access the club system.

However, IT specialist, Secom Technology, have found an alarming number of IT managers fail to realise that quite apart from managing club-owned devices issued to employees, they must manage devices employees bring into the club.

A club's information is at stake. Not only does the employee's device contain club information, but it is a portal into the club's IT system.

As part of a recent US experiment, 50 Smartphones were intentionally lost at busy locations in a number of cities. The phones contained simulated corporate applications and data and were tracked as they were found - 83 % recorded attempts to access corporate data, and only half of them were ever returned.

The data breaches were concerted attempts to access files such as "HR Salaries."

A specialist in the trend of consumer products driving business, Secom Technology has developed a **BYOD Checklist** and specific measures for its countless club industry clients.

As a first step, mobile protection and device management software is loaded onto each phone to reduce the risk of unauthorised access to sensitive corporate information.

Secom Technology advises that the following risk reduction factors are crucial:



- IT Managers must know what each employee needs to access and then take steps to ensure that only those areas can be accessed.
- Strategic thinking must guide the IT Manager's development of a mobile strategy for their employees. They should explore the risks and secure data wherever it resides.
- Effective management means being aware Smartphones etc. are endpoints and securing them accordingly.
- Mobile management must be integrated into the club's overall IT policies.
- Enforce appropriate policies to accommodate corporate and employee-owned devices alike.
- Plan to accommodate or deal with new devices as they come onto the market, before they are in your club.
- Security must be comprehensive – recognising that it's not just devices at risk, but the information that they contain. Password policies should be supplemented with other technologies that include data encryption, vpn authentication, antimalware and the ability to remotely wipe and disable the device.

Employee checks are vital. One inside man using Bluetooth could pass IT system access to an accomplice without even exchanging glances.

Secom Technology offers a free, no obligation BYOD security evaluation briefing for club IT Managers.

“The main club house had PC’s, a server and wireless internet connection but at the works depot 300m away our course superintendent had dial-up internet and emails,” Warren said

“We sat down with Secom and determined where all of our deficiencies were and where we wanted to get to. That list included increased security, anti-virus software, firewall protection, offsite backup of data and linking the workshop to the clubhouse so we could communicate easier and our Superintendent and his staff could communicate with the outside world far easier.”

At the first club meeting a number of options were discussed.

“To his credit, Jason quickly realised that when our state of the art works depot had been built two years previously, 30 pairs of standard telephone cable had been laid between the shed and clubhouse.

“His solution was a to use those telephone lines to virtually create our own ADSL network between the two locations, putting a black box at each end to convert the signals – a neat, tidy, effective solution that cost a mere \$5000 and also immediately afforded us the ability of two-way offsite backup.

“The fact that we didn’t have to go to the expense of laying another cable made it very attractive to us and it has worked a treat. The fact that the Course Superintendent can log in remotely and turn off the automatic sprinkler system in

Secom Solution Earns Praise

the event of rain is in itself a huge saving.” Warren said.

The club’s executive was more than impressed with the speed of the transition.

“Within weeks of our calling Secom, a comprehensive plan had been put together. Everything including the thorough rework of the entire IT system, firewalls and data protection was in place within four months.

“Subsequently, Secom has proven itself absolutely pro-active and Jason’s our go-to guy for providing solutions. Once a solution is put in place we see his technicians instead, but they know their stuff. They have always fixed things first time every time and it has been a great service,” Warren enthused.

“Jason’s strength is that he finds, or even invents, answers to problems rather than pushing hardware or software that he handles.

“Even with our computers, instead of pushing new ones on us he just makes them work better.

“He’s always making suggestions when we have discussions. He’ll give product recommendations, but with a rounded opinion, pointing out both the advantages and disadvantages.



NSW Golf Club Assistant Manager, Warren Begg.

“Jason has the advantage of broad industry knowledge. Because he’s dealing with clubs he knows their problems. He knows what systems and solutions have worked and what haven’t,” Warren said.

SMSmycustomers

Use SMS messaging to improve services to your members & increase your membership base. **FREE TRIAL!**

SMS “MYCLUB” to 0416906966 to try the power of SMS keyword marketing



www.smsmycustomers.com.au



- Electrical Data & Phone
- Club / Hotel Maintenance & Installation
- Commercial & Industrial Contractors
- Diesel Power Generation
- CCTV Systems

PH: 9525 1623
www.wedgroup.com.au

Does your CLUB’S WEBSITE have...

- a professional layout & design?
- an email newsletter for club members and subscribers?
- Page 1 Google rankings for your Events & Function Rooms?
- an easy-to-use website editor?
- Facebook and Twitter pages that engage your community?
- online membership payments?

...it should.

For more information, please phone
02 8006 1160

Club Tech Galloping Ahead



Technology is coming to the aid of clubs at an astounding rate thanks to a company relied on by more than 90 clubs for everything from IT and security to vendor liaison and advice on strategic purchases.

A provider of solutions rather than a purveyor of products, Secom Technology is in the process of launching a range of new products including:

- An Australian developed sign-in and photo ID scanning system with Optical Character recognition technology.
- A wireless broadcast TV system that is a stand-alone, plug-in which will allow clubs to broadcast any media to iPads, iPhones or laptops.
- Firewall technology that can be operated by anyone and reports irregular activity by e-mail direct to a nominated address.
- Web security designed to defeat the most devious miscreants.
- Sourcing and support for Apple TV that allows streaming of iPad content wirelessly to any TV.

Sydney-based Secom Technology's founder and Managing Director, Jason Drew, is justifiably proud that his company has saved clubs thousands of dollars with such things as multi-site wireless technology solutions and secure web page delivery.

A major player in the contentious area of gaming security, Secom provides a fully monitored IT solution that at any one time is monitoring 650 machines in the field live.

The company has grown rapidly by taking a proactive approach.

"We meet with all of our clients regularly to keep them up to date with technology so that they are not chasing the curve," Jason said.

"Our goal is to keep them one step ahead and to this end we annually attend the US Consumer Electronics Show as well as INTEROP which is the world's major IT networking conference."

"While most of the geeky type IT consulting companies attend INTEROP, we

have gained a decided market advantage through the Consumer Electronics Show as consumer electronics is now pushing business which has had to respond to the popularity of things such as iPhones and Netbooks. It's our role to show our clients ways to benefit from these innovations.

"Keeping abreast of the consumer side has allowed us to understand what we can utilise to give our clients an edge. I believe that that emphasis plus our service levels and the maintenance of an Australian-based support desk have kept us ahead," Jason said.

Secom Technology's support desk operates 9am to 5pm but engineering support is on call from 5pm through to 9am.

In the next issue we will look at some of the new Secom developments in detail, but for further information and even a demonstration at no obligation, contact Secom Technology direct on 1300 781 224.

How Secure Is Your Club's IT System?

Could cyber criminals be viewing your banking and member's data without you knowing?

Ring **1300 78 1224** for your **FREE** Network Security Audit

All audit participants receive The Essential Guide To Preserving Your Critical Data And Computer System

