Are you as protected as you think? This month we dive into data security, employee awareness, identity risks & solutions, plus professional longevity.

The future of work, today.

“It’s a fair question: if we are the guards, who’s guarding us?”

Chris Cotterrell
General Manager, TIMG

"Who will guard the guards themselves?"
Juvenal, Roman poet

Maintaining good privacy practices is a "good housekeeping" matter for

Here I will share what we do, and what you should consider for yourself or business:

- Know the essentials for security.
- Understand your rights. Only give out information that you feel comfortable
any organisation. But when you’re the custodian of your clients’ confidential information, it’s even more critical. Our clients trust us with their most valuable and mission-critical information. So it really is up to us to be worthy of that trust by making sure our own privacy and security are the best they can possibly be.

It’s a fair question: if we are the guards, who’s guarding us? At TIMG, we take privacy very seriously. We benchmark our privacy and security practices against those of the most secure organisations in the world. At an organisational level, we’re audited against ISO 27001 Information Security standards. At the personal level, we ensure that our staff is equipped with all the tools and behavioural skills they need to recognise and deal with threats to our clients’ privacy.

Privacy Awareness Week is a good time to focus on renewing your company’s efforts to protect itself from cybercrime. While it’s great to have a week of dedicated awareness raising, the reality is that privacy is a 24/7 concern for all of us. "This year’s Privacy Awareness Week (PAW) theme, Privacy in your hands, reinforces the message that organisations, agencies and individuals must be vigilant in maintaining a good understanding of their rights and responsibilities for the handling of personal information," according to Timothy Pilgrim, OAIC Commissioner.

The funny thing about privacy and security, and our innate human nature, is that subconsciously we tend to think breaches will happen to the other guys – not us, not our business. But then we hear sharing. Ensure you are involved with a trusted party. Only click on links from a reputable source.

- Protect yourself online with strong passwords. How many of us are guilty of not doing this? Even if a company allows us to proceed with a ‘weak’ password, do not be tempted. Also, remember to frequently switch up passwords between accounts.
- Securely dispose of personal details. Don’t leave sensitive customer, client, patient or personal information lying around. Locked cabinets, password-protected files, shredding, and Verification of Identity are helpful measures to take. Employees should typically only have (restricted) access to information that is needed to perform their particular role.
- Perform a quick audit. How does your team handle personal information? Have you assessed your risks and threats? Are your antivirus and antispyware up to date?
- Does your business need a revamp of their privacy actions? Is it time to establish or revise procedures? Consider how greatly technology has evolved over the past five years. Our privacy policies should reflect this!
- Ensure your network is secure and that WiFi passwords remain robust and protected. Install encryption on mobile devices including laptops and tablets to protect against intrusion.

While each industry faces their own unique challenges when it comes to privacy – private client data, credit card details, employee contracts, etc., technology is growing at such a rapid rate that it seems laws and privacy standards sometimes cannot keep pace with each of the many dynamic and evolving complexities in the digital space.
about familiar companies you wouldn't think it would happen to either, like when Kmart Australia customers’ identity and purchase history was hacked. The threat is a reality for us all.

What can we do to protect ourselves and thus our businesses? At TIMG, we often hear of these breaches and understand our clients’ privacy concerns. We specialise in a variety of solutions, which is why we have such tight security measures implemented including very thoroughly trained staff. Together we should remain robust and proactive against threats!

Ultimately, what we specialise in providing is peace of mind, so you can work with that free feeling of reassurance, knowing that there is a cushion of security around privacy.

Contact us about TIMG privacy-related products:
- Intellectual property management and protection
- Backup media storage
- Complete archiving
- Secure destruction

One of the most significant security vulnerabilities sits right in the heart of your organisation. You know it as your staff. And no, we're not talking about disgruntled staff with an axe to grind. We mean your mild-mannered, everyday staff who are increasingly the targets of cyber criminals.

No matter how sophisticated a company's processes and protocols might be, staff members remain individually responsible for managing threats to privacy. Security firm Symantec recently published an interesting report showcasing an alarming surge in social engineering phishing attempts preying on employees within certain departments. Social engineering refers to psychological manipulation through highly developed and refined attacks which rely on human interaction.

The scammers’ technique provides a deceptive sense of authenticity and attempts to build a relationship with an employee. They typically use insider knowledge such as executive staff names. They send malicious links or what looks like official documents such as invoices or spreadsheets. They might also falsely use what appears to be a reputable company email address or logo with seemingly undetectable tweaks, say, with just one
letter off.

We can learn from companies that have lost millions of dollars all because their employees accepted wire transfer requests as true.

In order to consistently stay one step ahead of cyber criminals, it is no longer enough to just capitalise on current security measures. We must actively increase employee awareness. This month, TIMG is rolling out a training programme across the organisation. The programme is designed to equip staff with the behaviours and skills that will reduce the threat posed by these attacks. As each team member goes through training, potential weaknesses are discretely revealed, not to embarrass, but to teach.

A collective commitment and particular investment in employee vigilance should become the priority for businesses today, as phishing attempts are growing more and more prevalent.
How the Gmail Scam Works

1. An attacker obtains a victim’s email address and phone number – both of which are usually publicly available.

2. The attacker poses as the victim and requests a password reset from Google.

3. Google sends the code to the victim.

4. The attacker then texts the victim with a message similar to:
   “Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity.”

5. The victim therefore expects the password-reset verification code that Google sends out and passes it on to the attacker.

6. The attacker can then reset the password and once they have what they want or have set up forwarding, can inform the victim—again posing as Google—of their new temporary password, leaving the victim none the wiser.

Source: Symantec

Take My Stress Away...
Day after day, you might find yourself with many copies of passports, drivers' licences, and the like. In the back of your mind, you know you must comply with the Privacy Act, consider legal ramifications, Verification of Identity (VOI) requirements, and so on. The bulk of the paperwork storage results in a headache and a sigh when you just want to enjoy your coffee and get down to your real work.

Paper copies aren’t a workable solution and scanned images on your server pose too great a risk. The consequences of a data breach can cost. Fines can total up to hundreds of thousands of dollars. Storing VOI reports in multiple locations and formats, lack of backup, theft of server and unauthorised access are risks that have resulted in breaches for one too many organisations.

If only there were an easier answer to all of your administration problems! Wouldn’t a perfect solution be to quickly upload to your smartphone? An app to automate and digitise? One second to snap a pic of the identification document? Ten seconds to type in the name, reference number, etc., and then be done?

It all makes sense. And it turns out, it's already a thing. It's the free TIMG VOI Report Vault app. With extra layers of security, TIMG VOI takes the risk away. If this sounds like what your work life is missing, give us a quick call to find out more. Easy!

- Centralised storage of VOIs from all sources
- Controlled access to all images and data
- Easy tracking and management
- Eliminate risk of privacy breach
- Secure online hosting
- Support 24/7
- Free when used in conjunction with TIMG closed file archiving service
Hi James, tell us a bit about yourself.

Technology has been a part of my life, starting with my uncle’s Commodore 64 at age 8, and my Atari ST at age 10. From modifying games and phones to building PCs and apps, I’ve always enjoyed reassembling things that were not always designed to be deconstructed in the first place.

How did you first get involved with TIMG?

I joined TIMG 10 years ago in Operations: I was seeking a change of scenery from technical support. But it wasn’t long before I was back in IT. I had submitted an extensive report on how to improve security in our internal applications, which I was able to implement shortly after as a developer.

James, you are our go-to guy for all things information security. What do you love most about working in this area?

Security isn’t just about keeping information confidential. It is equally important to ensure it is accessible and

TIMG is working towards full PCI-DSS certification. How will that affect TIMG’s standing in the market? Will there be any flow-on effects through the rest of TIMG’s security?

Definitely. TIMG already has physical PCI-DSS (Payment Card Industry Data Security Standard) certification. Our work towards the digital equivalent will allow us to offer services that are relevant beyond the handling of credit card data. PCI-DSS is a proprietary information security standard for organisations handling branded credit cards. At TIMG, we treat all our clients’ data with the same respect as if it was credit card data. Our PCI-DSS certification will prove this, give peace of mind to new customers, and confirm what our existing clients already know about our security.

Apart from the use of TIMG services, what advice can you offer to other businesses looking to successfully protect their data online?

Defence in depth has always been a mantra of the industry. Security isn’t an appliance, or a policy: it is a series of...
to preserve its integrity. Working with the team to design, build and deliver solutions that perfectly balance these aspects is very rewarding, with the hands-on prototyping phase being my personal favourite.

In your role as Information Security Manager, you are responsible for steering TIMG's implementation of comprehensive security and privacy protocols. How does TIMG compare when it comes to information security?

TIMG has always looked towards the policies and controls already in place at the most secure entities on the planet as the standards to measure ourselves against. NIST and FIPS standards relevant to US Government entities, as well as our own Australian Defence Signals Directorate controls, are all referenced in forming the foundation of TIMG policy. These agencies always revise and improve; as they do, so do we.

If you could invite any business person to lunch, who would they be and why?

Elon Musk. Anyone who is able to invoice NASA for the use of their spacecraft makes for good company.

Maintaining professional longevity through the "promotion from within" idea continues to be key for exceptional TIMG team structure and culture. This concept successfully put into practice promotes a sense of satisfaction, motivation, and an ever-evolving lifetime value for the employee.
To steadily strengthen the next generation of TIMG leaders, we aim to leverage our current depth of talent, expertise and experience that is embodied in our staff. One particular team member who has consistently exemplified these positive traits is Rick Garry. As such, it is with great pleasure that we announce the promotion of Rick as our new Operations Manager in South Australia.

In 2011, Rick started with TIMG as a Service Representative in Queensland. Over time, his TIMG journey has seen him grow as an Assistant Site Coordinator to a highly valued Service Coordinator. In these roles, he obtained an invaluable skillset and a vast amount of knowledge necessary to take the next steps into the Operations Manager role.

And what does Rick enjoy most about working for TIMG? "Always the people. Everyone in Queensland was always such a joy to work with. Now in South Australia, the people share the same enthusiasm and always have a smile on their face. It makes everyone's job that much easier and more satisfying if we all enjoy what we do."

Welcome to the South Australia Team, Rick!

For more information:
Visit timg.com or call 1800 464 360

While every effort has been made by TIMG to ensure that the information contained in this newsletter is up to date and accurate, TIMG does not give any guarantees, undertakings or warranties in relation to the accuracy completeness and up to date status of the above information. TIMG will not be liable for any loss or damage suffered by any person arising out of the reliance of any information in this newsletter.