MARCH 2020

IGAMES DATA MANAGEMENT

L.Arbuckle Consulting

PREPARED BY:

Liam Arbuckle
Consultant, Database Administrator
Google Doc:
https://m.acord.software/ikrfho

APPROVED BY:

Dervish Musovic
CEO at iGame

TYPES OF WEBSITES

Overview

Retail (Myer Online, Target Online, etc)

Freelancing (Fiverr, Freelancer.com, etc)

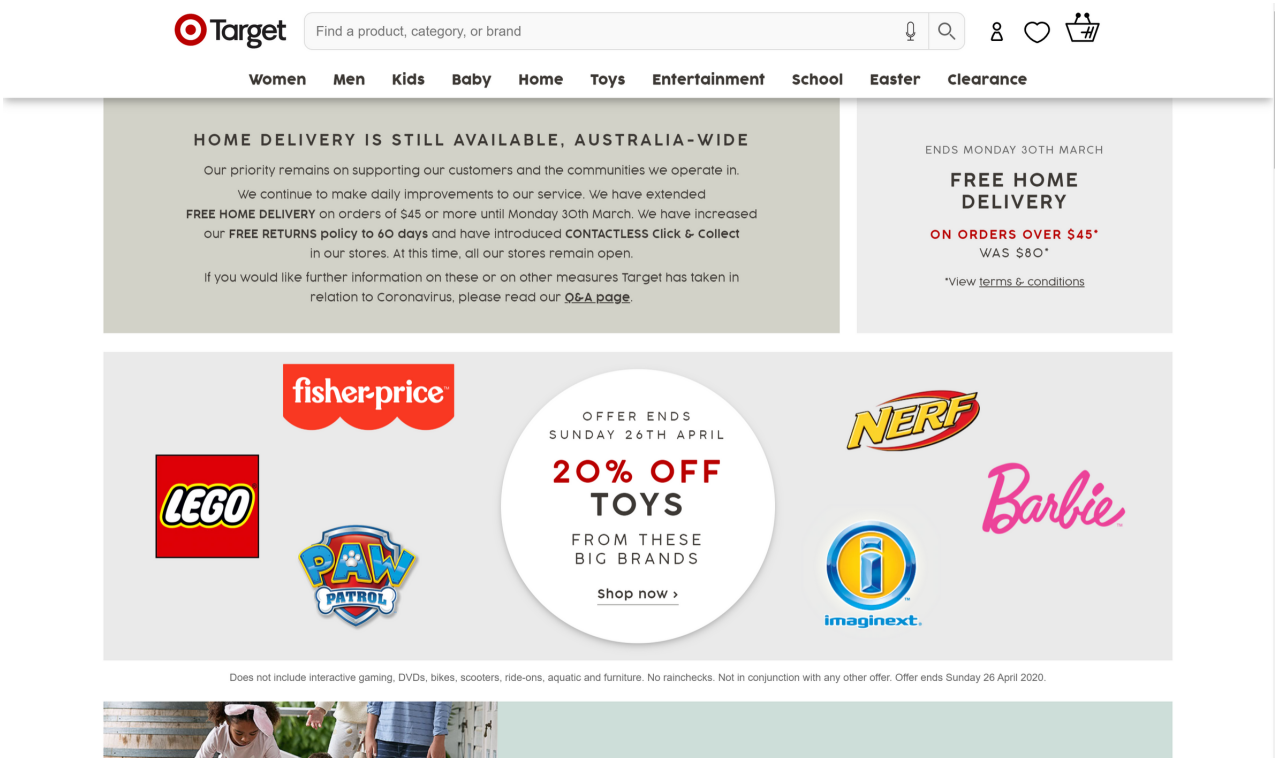
E-Commerce (Amazon, Ebay, etc)

Cloud Computing (Google One, Microsoft Azure, Amazon AWS, Hostgator, GoDaddy, Github & Gitlab Enterprise, etc)

Media Sharing (Youtube Red, Various Adult Websites, Vimeo (P.S. nobody uses Vimeo))

Retail Websites

Almost every big franchise, like Myer, Target & Woolworths have large websites with the capability to buy & order products online, and have done for some time. The websites exist for two main reasons: to sell their products, and to grow their business; this can be done through data mining (Andrew Pole is a name that is regularly thrown up due to his controversial tenure at Target, which started in 2002) and email subscriptions.



Best Practices

Each retail site follows a similar pattern. They have a clean and minimalistic header menu, which functions as a “mega menu” for easy and vast navigation of the entire website. To buy items from a retail store, you need to be signed in with an account, the details of your account that a company like Target would require are noted down below in the section “Data Dictionaries”. The most profitable items or categories are often displayed underneath the main menu on a retail site in a large “call to action” section, or this CTA is taken up by the current ongoing sales that the store is providing, making it one of the first things your eyes are drawn to when you open the website.

Data Dictionary - Target

Retail (Target Online)

Column	Data type	Description	Constraint
j_username	email	Customer's email	Required
firstName	text	Customer's first name	Required
lastName	text	Customer's last name	Required
optionalMobileNumber	tel	Customer's mobile phone number	Optional
countryCode	text	Country code for customer's address destination	Required
search	text	Nearest target store lookup	Required if store pickup
line1	text	Customer's address line 1 (i.e. street address)	Required
line2	text	Customer's address line 2 (i.e. apartment/suite)	Optional
paymentMethod	text	Chosen method of payment	Required

Data Dictionary - Amazon Ecommerce

(Included in rest of assessment)

E-Commerce (Amazon)

Column	Data Type	Description	Constraint
userFirstName	string	First name of the user	Required
userLastName	string	Last name of the user	Required
userDOB	string	Date of birth of the user	Required
userCard	integer	User credit card information	Required for purchasing/selling items
userAddress	string	User physical address	Required when purchasing items
userEmailAddress	string	User email address	Required
userPassword	string	Custom-chosen password for the user to verify identity when logging in	Required

Data Dictionary - Google Cloud Computing

Cloud Computing (Google Drive)

Column	Data Type	Description	Constraint
userGoogleAccount	string	The email address that is linked to the customer's Google Account	Required
userPassword	string	*Connected to "userGoogleAccount"	Required
userBilling	Boolean	If the user/customer wants to have more storage (google drive) or Gsuite (emails), then the boolean is set to 1, true, or yes	Optional (if user wants premium plan)
userCard	integer	Credit card information	Optional (see above row - "userBilling")
numberOfEmployees	integer	Number of employees, including you (customer/user)	Required - to determine amount to be billed to the user
userDomain	boolean	You'll need a domain, such as *example.com*, to set up email and a G Suite account for your business Options are: yes (I have a domain), no (I don't have a domain)	Required - can't set up emails, google account without a domain

Managing Data Glossary

Managing Data Terms - Glossary

Term	Definition
Entity	An entity is an object that exists. It can be a single thing, person, place, or object
Attribute	A characteristic of an entity. It refers to a database component, such as a table or entity, and they describe the instances in the row of a table.
Database	An organised collection of data
Data redundancy	When the same piece of data is stored in two or more separate places
Data integrity	The consistency of data in a database's life cycle
Data mining	The process of processing large sets of data to find patterns
Data mart	A segment of a data warehouse that is designed to be used for a specific line of business
Data warehouse	A collection of data marts

SECURITY MEASURES

"HTTPS IS USED FOR SECURE COMMUNICATION OVER A COMPUTER NETWORK, AND IS WIDELY USED ON THE INTERNET. IN HTTPS, THE COMMUNICATION PROTOCOL IS ENCRYPTED USING TRANSPORT LAYER SECURITY OR, FORMERLY, ITS PREDECESSOR, SECURE SOCKETS LAYER."

Almost every website today that takes some sort of important & private information regarding a customer, consumer or subscriber has what is known as “SSL encryption”, which is shown in the address bar of a web browser with the prefix “https”. HTTPS stands for Hypertext Transfer Protocol Secure.

While websites and applications that rely on HTTPS encryption are by no means unhackable (look at the iCloud NudeGate scandal or the Heartbleed bug), they are much more secure than regular HTTP. There is a small cost when purchasing the domain name and hosting for the website that comes with SSL, but it keeps the information of its customers private and secure. For start-up businesses or smaller companies (like iGame), it is simply not worth attempting to bypass the encryption on a website, as the payoff (customer data) will be smaller - as there are less customers - than if they focused on attacking a company like Myer, JB Hi-Fi or Facebook.

REFERNTIAL DATA INTEGRITY

To maintain referential integrity, we need to make sure each FK has a PK. Referential data integrity between tables can be enforced by using referential constraints (constraints that ensure the data inserted into a particular column has matching values in another table), because the maximum number of references allowed for a single table is 200. If a table exceeds that limit, or has special referential integrity needs, use referential integrity triggers.

ENTITY DATA INTEGRITY

To maintain entity integrity, a table must have a primary key that uniquely identifies each row in the table.If a table does not have a primary key, you can't be sure that the row retrieved is the one you want.

Entity integrity can be maintained by specifying that the column (or group of columns) making up the primary key is NOT NULL. In addition, you must constrain the primary key to be UNIQUE. Some SQL implementations enable you to add such constraints to the table definition.

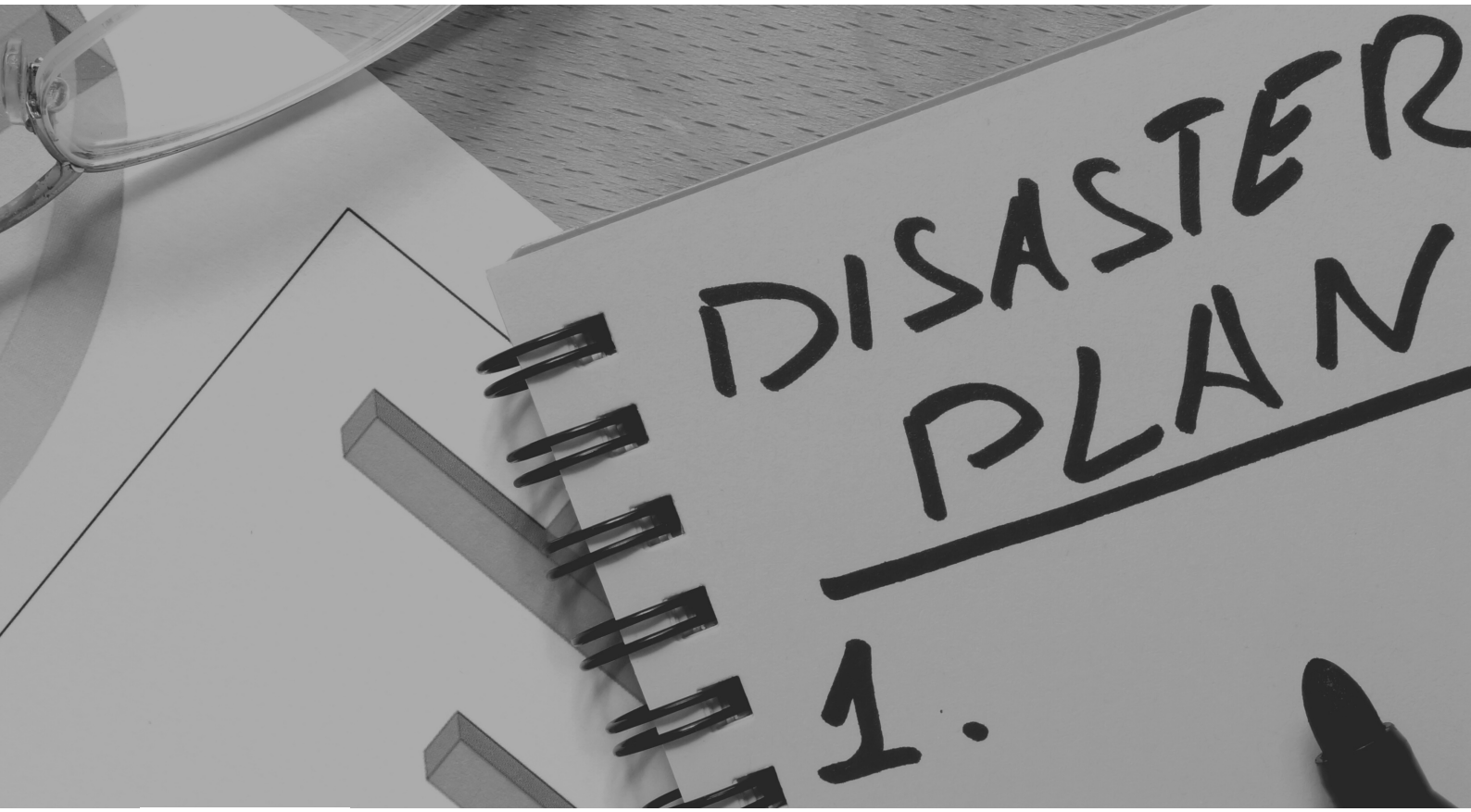
DISASTER RECOVERY PLAN

A disaster recovery plan helps individuals or organisations prepare, prevent, and handle a disaster - for example, a natural disaster like bushfires - if and when it occurs.

Cloud Backup

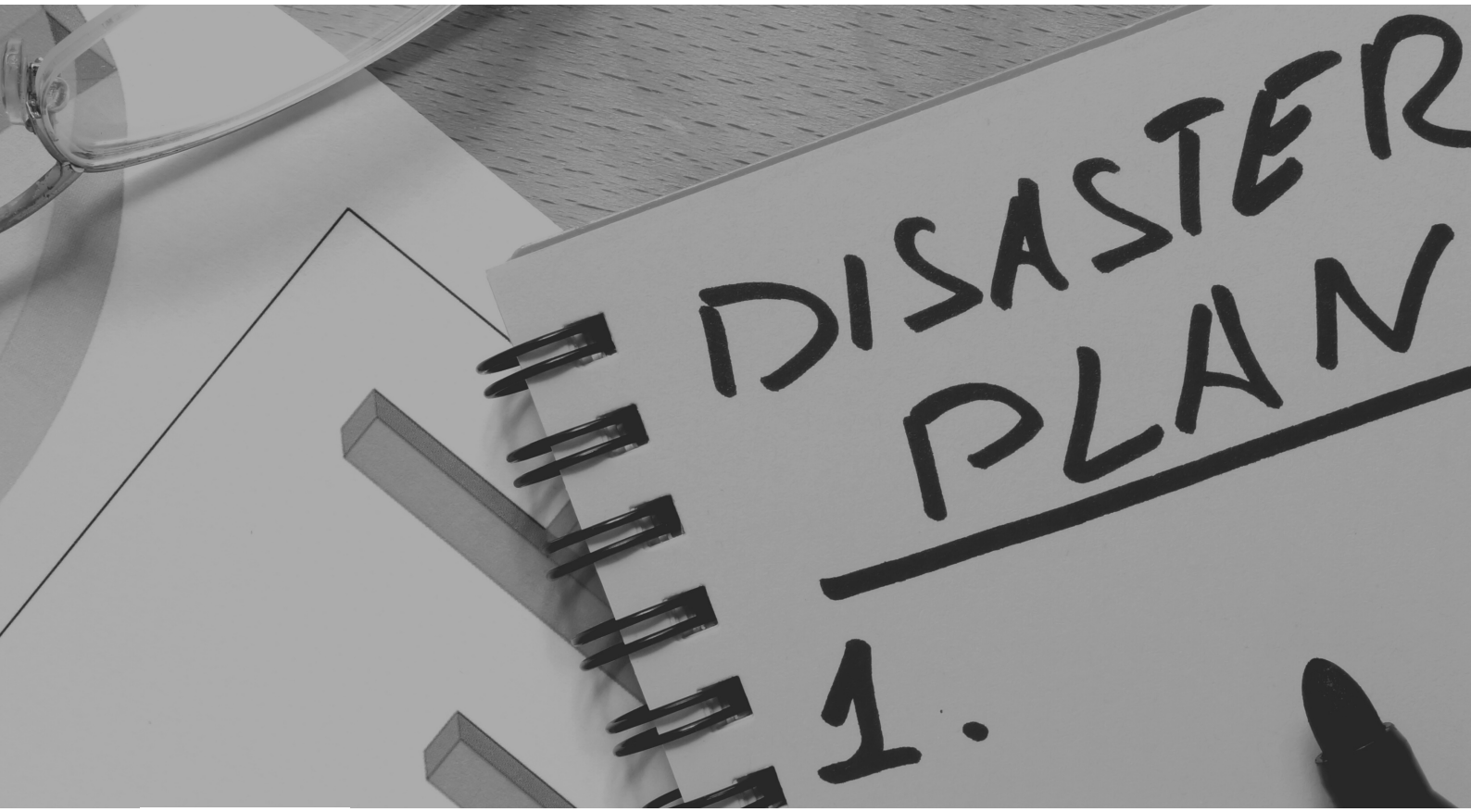
A cloud backup is a service that provides individual users as well as organisations and businesses with a system for the backup, storage, and recovery of computer files, like the database and files included on the iGames website.

Pros	Cons
Backup and restore can be initiated practically anytime, anywhere	Hosts may have a limit to how much data can be saved due to availability and cost
Only pay for what is needed, and storage plans are flexible i.e. upgrades can be made on-demand	Full recoveries may take a long time and put stress on local system



Public Relations

If there is a bushfire and our customers' orders & data are vulnerable, it is up to us to keep the public updated on social media platforms. Not doing so will result in customers spending money on orders they won't receive because the order forms were lost, and this leads into the backup of our database. Without a cloud backup it would be impossible to verify order claims.



Insurance

If there is a bushfire (or other natural disaster), and any amount of stock is lost due to this event, it is up to iGame to put in an insurance claim to receive money to compensate for the stock & other equipment (like computers, desks, TVs, consoles, etc) that has been lost. The database, therefore, will need to be presented as proof of what iGame had in stock at the time of the event, and photographic evidence of items lost will also be required.

DATA BREACHES

Security problems regarding data breaches

Security risks involving data breach

- Virus/malware
    - E.g. trojan horse
        - A malicious application disguised as a legitimate one and may have similar interface & functionality. If careless and not downloading the app from its official website then “microsoftacess.exe” will steal whatever data is being stored, risking data leak
- Physical damage
    - E.g. water leakage
        - A water leakage will mess up the circuitry in the hardware
- Data corruption
    - Corruption of data
        - The data that was initially not corrupted is now corrupted, which means it is unuseable
- Unauthorised access
    - E.g. SQL injection attack
        - A type of code injection technique through a website’s SQL input statements
        - Can be prevented by sanitising inputs

Ethical Issues regarding data collection

With the collection of data comes risks, both financial and social risks, to the users that have their data collected by companies like iGame. As mentioned previously, it is therefore the moral - and legal - responsibility of iGame to ensure that the data collected (like emails, home addresses and date of birth) is protected behind multiple secure systems and is encrypted, processed and stored securely.

The physical safety of the customer should be the primary concern of iGame when regarding customer data. When data is stolen, users' finances are not the only thing that's vulnerable. When Dorian Nakamoto, a Japanese-American engineer, was claimed by Newsweek to be the founder of the popular cryptocurrency Bitcoin, his home address and photos of him were released, and this action drew widespread condemnation from millions around the world. While it is debateable the legality of Newsweek's actions (Dorian had no doubt shared information freely on the internet, and if it's shared publicly there's no law against resharing it), it was evidently a hot topic when considering the ethics behind the decision to share his personal information. The PR disaster for Newsweek is something that iGame will want to avoid, and it doesn't matter if iGame releases its user's data freely, or if it's hacked - if it's not stored securely, the iGame brand will suffer.

With the collection of data comes risks, both financial and social risks, to the users that have their data collected by companies like iGame. As mentioned previously, it is therefore the moral - and legal - responsibility of iGame to ensure that the data collected (like emails, home addresses and date of birth) is protected behind multiple secure systems and is encrypted, processed and stored securely.

The physical safety of the customer should be the primary concern of iGame when regarding customer data. When data is stolen, users' finances are not the only thing that's vulnerable. When Dorian Nakamoto, a Japanese-American engineer, was claimed by Newsweek to be the founder of the popular cryptocurrency Bitcoin, his home address and photos of him were released, and this action drew widespread condemnation from millions around the world. While it is debateable the legality of Newsweek's actions (Dorian had no doubt shared information freely on the internet, and if it's shared publicly there's no law against resharing it), it was evidently a hot topic when considering the ethics behind the decision to share his personal information. The PR disaster for Newsweek is something that iGame will want to avoid, and it doesn't matter if iGame releases its user's data freely, or if it's hacked - if it's not stored securely, the iGame brand will suffer.

After noting that, it is evident that there would be a number of security & ethical issues that would arise if a data breach occured.

In 2015, the website AshleyMadison was hacked, and the personal information (names, email addresses, etc) were stolen and published on the internet. Over the ensuing months, there were those who praised the hackers for revealing this information, while a vocal minority - comprised mainly of psychologists & those in the medical profession, resented the hackers for distributing this information.

THE DISSEMINATION OF USER IDENTITIES COMPROMISED AN UNKNOWN NUMBER OF RELATIONSHIPS, TARNISHED THE REPUTATION OF SEVERAL PUBLIC FIGURES, AND EVEN TRIGGERED SEVERAL SUICIDES... INDIVIDUALS REVEALED TO BE SEEKING HOMOSEXUAL PARTNERS FACED CAPITAL PUNISHMENT IN COUNTRIES WHERE HOMOSEXUALITY WARRANTS SEVERE PHYSICAL PUNISHMENT OR THE DEATH PENALTY... THEREFORE, THE COMPANY SHOULD HAVE HANDLED AND PROCESSED THE DATA WITH THE UTMOST CONCERN FOR PERSONAL SECURITY AND PRIVACY.

While the purchasing of games from iGames would not involved data that had the potential to compromise the psychological health & well-being of our customers in the way that the hacking of Ashley madison did, the data that we'd be collecting would still be ethically volatile. Let's look at the data that we're collecting from the users and the data that will be present in the iGame database:

- First name
- Last name
- Address
- Suburb
- City
- Mobile Phone Number
- Payment type
- Order date
- Delivery date
- Game that was purchased (and also the studio)
- Customer payment information (unless the game was paid for in cash - see Payment type)

Apart from the last set, all of the above information would be freely available to the public if the data**base** was breached or hacked, and the payment details (like credit card information, if a game was purchased online) would presumably be available to any would-be hacker as well.

While there's a number of security issues which will be explored shortly, the above information - especially the games that were purchased, the home address and phone numbers of the customer - lead to ethical issues. Selling customer data to third-parties in return for those third-parties gaining information on who buys what product (and therefore allowing for targeted advertising to become a reality) is one of the most controversial topics being discussed in the tech world today. There are those who argue that giving up our privacy in return for algorithms that know us better than we know ourselves are a good thing; however the majority value and worship their privacy (regardless of how the user flounts themselves around with regards to their privacy, they will seek to blame the corporation rather than themselves) and oppose companies tracking their search history and getting bombarded with targeted ads.

If the phone number or email address of our customers is compromised, it leads to the potential for spam calls, emails and texts, which, while not strictly against the law in Australia, is certaintly a devisive issue that the 99% are against. If the database is breached, it opens up a possibility that our users will be inundated with spam through the mediums mentioned above.

This spam, or targeted advertisments will be further increased if advertising companies are aware of what games - or development studios, or the game genres - our customers are purchasing. By becoming aware of this, our customers' privacy is further decreased, and thus our public image suffers.

Phone porting is a big security issue right now.

A port-out scam, or unauthorized mobile phone number porting, is one where a fraudster uses your stolen cellular account information to transfer (or "port") your phone number and account to another carrier in order to take control of your phone while also shutting down your account

Not only does this scam allow unscrupulous people to gain control of users' phones, potentially revealing personal messages (again, an ethical issue as well as a security issue), if a phone is ported it means that the two-factor authenticiation format that is put in place by many websites around the world, as well as major banks like Westpac, is no longer secure, and the entire savings of an individual is at risk.

And it would be even easier for those people to take the money out of a bank account through the account details stored in our system.

A port-out scam, or unauthorized mobile phone number porting, is one where a fraudster uses your stolen cellular account information to transfer (or “port”) your phone number and account to another carrier in order to take control of your phone while also shutting down your account