Case study: AusTechTrade data and cyber security

Introduction

The multinational business *AusTechTrade* has been operating in the e-commerce space for some time. Like many e-commerce businesses, they collect and process several streams of big data (private, financial, product, and internal data). These data streams give insight to customer bases and the running of the business, but their provenance and security must be rigorously and routinely inspected to protect against omnipresent cyberthreats, and to honour the responsibility AusTechTrade has to customers and employees. Failure to recognise this responsibility comes at a significant financial cost to AusTechTrade as outlined by the relevant Australian, US, and European compliance regulations.

Assessment of AusTechTrade's Cyber-Assets

A comprehensive review of *AusTechTrade*'s cyber-assets was conducted in order to measure risk and ensure security and compliance is being upheld to the best of the companies' ability (table 1).

Table 1: A brief summary of likely Data types and classification of the various associated data types AusTechTrade *may hold using a classification type first used in 2013 which I understand is now incorporated into ISO 27005 (Agrawal 2017; ISPB 2013).*

<table>
<tr><th colspan="2">Customer Data</th><th colspan="2">Business Data</th></tr>
<tr><td>Private data</td><td>Confidential Data:
Name
Address
Contact details
Financial information
Geolocation
IP Address
Behavioural data
Previous correspondence (complaints, reviews, chat logs, etc.)
Receipts
Basket items or in-cart items (not receipts)
Postcode
Restricted Data:
Authentication details</td><td>Proprietary data</td><td>Public data:
Marketing material
Policies (shipping, returns, data management, etc.)
Public website content
Social media posts
Catalogues
Internal Data:
Inventory
Project information
Receipts
Internal policies
Website and social media analytics
Internal processes and tools
Confidential Data:
Meeting minutes
Suppliers, Costs, and contracts
Mark ups
Future projections
Intellectual property and development plans
IoT data
Restricted Data:
Sensitive financial records</td></tr>
<tr><td></td><td></td><td>Employee data</td><td>Confidential data:
Name
Work contact details\
Restricted Data:
Authentication details
Private contact information
Tax file number
Financial information
Home address
Personal contact details
Work analytics</td></tr>
<tr><td></td><td></td><td>Patrol data</td><td>Confidential Data:
Third party research
Reconnaissance on competitors</td></tr>
</table>

Discussion

Cyber risks and threats

CIA risk

The ever-present risk associated with *AusTechTrade's* cyber-assets is the potential for the information to be incorrect or needlessly accessible. This relates to the confidentiality, integrity, and availability/accessibility (**CIA**) of the asset(s). As early as 1972, CIA has been a critical component of data security. It specifies that the data needs to be protected, have well recorded provenance, and be easily accessible to those with authorization in a timely manner (Anderson 1972). This is essential as it protects business and customer interests, ensures the data continues to hold meaning and relevance, and improves efficiency. These concerns warrant constant vigilance and sanitation of the crown jewels. As *AusTechTrade* is an e-commerce platform, its business is data. There are likely very few cyber-assets that do not require such sanitation, perhaps public data could be checked less frequently as it should be updated frequently with historical records being non-critical.

Data usage

Once CIA is confirmed, *AusTechTrade* needs to ensure that the data is being used lawfully and properly. *AusTechTrade* may have complete and accurate records, but this does not necessarily result in accurate outcomes. For example, we have recently observed worker efficiency being calculated based on hours recorded in payslips, however, this penalises workers doing overtime off the clock to keep projects within a budget. There needs to be an action plan to assess that data is fit for purpose, particularly when it impacts cybersecurity decisions.

External threats

There are several targeted and untargeted external threats that look to exploit cyber-risks. Common targeted attacks include:

- Hackers attempting to steal assets or disrupt service through brute force,
- Phishing or whaling attacks looking to exploit human error to obtain sensitive information or financial gain (Asbaş & Tuzlukaya 2022; Pienta, Thatcher & Johnston 2020).
- DDOS attacks looking to push the servers past breaking point as a distraction or as a ransom (Asbaş & Tuzlukaya 2022).
- Ransomware that encrypts specific data as a ransom (Asbaş & Tuzlukaya 2022; Koch, Stelte & Golling 2012).
- Supply chain attacks where attackers go through a third party with access to parts of the system (Wolff, Growley & Gruden 2021).
- Adversarial attacks that target algorithms to promote items being recommended to customers (Cao et al. 2020).
- Credential Stuffing where large databases of stolen credentials are trialled as user authentications (Ba et al. 2021).

- E-skimming and Form-jacking involves stealing user inputs, such as financial information (Dharmavaram 2021; Rouge et al. 2020).
- Man-in-the-middle attack where an attacker enters the middle of a communication between interlocutors (Asbaş & Tuzlukaya 2022).

Untargeted attacks tend to be introduced through employees inadvertently and include:

- Malware infecting systems from email attachments or downloads (Asbaş & Tuzlukaya 2022).
- Automated brute force attacks attempt to guess authorization codes or encrypt data (Asbaş & Tuzlukaya 2022)
- Scareware that results in employees inadvertently inviting infection (Koch, Stelte & Golling 2012).

Responsibility

AusTechTrade has many cyber risks and threats it takes on as a cost of operating. These cyber concerns exist because it is understood that there is value in the data, and with value comes responsibility. Fortunately, there are business incentives that support the proper management of these responsibilities.

- Private data is received through transactions, the company may also receive purchase/behavioural metadata and enhanced trust. These are valuable and may lead to repeat business and word-of-mouth advertisement. Protecting the customers personal data promotes repeat business and prevents negative impacts on customers and reputation (Martin, Kelly D, Borah & Palmatier 2017; Martin, Kelly D. & Murphy 2017; Mathur 2019).
- Public business data represents a direct line of communication with consumers. These assets usually have teams updating them regularly as they represent the brand and manage expectations. Protecting media accounts, policies, etc. from corruption or unauthorized access is vital to protect the brand, foster trust, and prevent misinformation (DiStaso 2018; Garfinkel 2016; Mathur 2019).
- Demonstrable cybersecurity capabilities may reduce insurance costs, promote investor confidence, and position the company well to handle evolving cybersecurity attack mechanisms (DiStaso 2018; Roger 2022).
- The costs of doing nothing could result in enormous financial loss, legitimate safety concerns, or hefty fines (Dynes, Goetz & Freeman).

Mitigation

The risks associated with CIA can result in cyber threats if left unchecked, especially if employees are put in a position where they need to attack internal systems to get to job critical information. It's well documented that employees are a significant security vulnerability, so education and policies that align with a solid framework, such as ISO 27001, are essential (Khando et al. 2021). On data usage, there are several evaluation techniques (SIFT, PROMPT, CRAAP, etc.) that can reduce data usage risks (Brodsky 2022). Additionally, having clear metadata will ensure the correct data is being used, or provide useful information to reviewers to promote a timely resolution.

In terms of managing cyberattacks, education plays a key role and protects employees both at work and at home. But there are additional safeguards that should be put in place such as:

Table 2: Controls AusTechTrade can and should put in place to manage cyber threats and reduce risk.

Control Type	Control
Preventative	▪ Firewalls to protect internal networks from external access ▪ Multifactor authentication and regular password changes ▪ SSL encryption to protect data transfer pipelines ▪ Ensure data is stored in secure locations ▪ Data encryption or anonymization to protect information in compromised data ▪ Consistently patching all OS and software
Detective	▪ Intrusion detection systems to identify suspicious activity ▪ Web application firewall(s) to monitor HTTP requests/responses for malicious content ▪ Auditing and testing control effectiveness
Corrective	▪ Business critical data is backed up ▪ Have security clearance levels for employees and regularly sight devices ▪ Measured consequences of human error ▪ If key personal leave, know who has the skills to manage while a replacement is found.

Employees could also be tested at random with questionable emails to assess cybersecurity literacy, and frameworks can be measured by third party vendors (Kritzinger & Von Solms 2010). But even the best defences can fail, so it is important to have an incident response plan to minimize harm, this should include notifying consumers impacted of the breach.

Compliance

Australia, the US, and the EU recognise in varying degrees the responsibility of businesses to protect customers from harm. Each have their own regulations for data processors and collectors that needs to be adhered to when doing business in those regions. The EU and Australia have explicit privacy laws, but the US has no specific federal regulation. Only eleven US states have privacy laws enacted and of those only four have them in operation in 2023.

Table 3: Comparison of privacy law regulations for the three relevant regions. Noting that The US relies on several regulations that broadly cover privacy concerns.

Principles	**Regional Regulations**		
	Australia	EU	USA - Federal
	APA	GDPR	FTC, COPPA, etc.
Lawfulness, fairness, and transparency	✓	✓	✓
Purpose limits	✓	✓	~
Data minimization	✓	✓	~
Accuracy	✓	✓	~
Storage limitation	✓	✓	~
Integrity and confidentiality	✓	✓	✓
Accountability	indiscreetly	✓	indiscreetly
Right to Anonymity	✓	✓	~
Right to erasure	✗	✓	~
Notification of collection	✓	✓	✓
Declaration of specific data tracking	✗	✓	✗
Must provide access to consumer on request	✓	✓	✓
Applies to all businesses	✗	✓	~
Consumer in control	~	✓	~
Age protections	~	✓	✓
Notice of breach	~	✓	~

It appears that the GDPR is the gold standard so all *AusTechTrade*'s policies should be governed around them (see *table 3*). In doing so, sizeable fines will be avoided and the company will be operating well within regulations in Australia and the US. It also gives consumers more control over their privacy than regulations may require which may be appealing.

References

Agrawal, V 2017, 'A framework for the information classification in ISO 27005 standard', in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud),* IEEE, pp. 264-269.

Anderson, JP 1972, *Computer security technology planning study*, ESD-TR-73-51.

Asbaş, C & Tuzlukaya, Ş 2022, 'Cyberattack and cyberwarfare strategies for businesses', in *Conflict Management in Digital Business*, Emerald Publishing Limited, pp. 303-328.

Ba, MHN, Bennett, J, Gallagher, M & Bhunia, S 2021, 'A Case Study of Credential Stuffing Attack: Canva Data Breach', in *2021 International Conference on Computational Science and Computational Intelligence (CSCI),* pp. 735-740.

Brodsky, JE 2022, 'Fostering college students' fact-checking skills: Three studies assessing lateral reading instruction in a general education course', City University of New York.

Cao, Y, Chen, X, Yao, L, Wang, X & Zhang, WE 2020, 'Adversarial attacks and detection on reinforcement learning-based interactive recommender systems', in *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval,* pp. 1669-1672.

Dharmavaram, VG 2021, 'Formjacking attack: Are we safe?', *Journal of Financial Crime*, vol. 28, no. 2, pp. 607-612.

DiStaso, MW 2018, 'Communication challenges in cybersecurity', *Journal of Communication Technology*, vol. 1, no. 1, pp. 43-60.

Dynes, S, Goetz, E & Freeman, M 'Cyber Security: Are Economic Incentives Adequate?', in Springer US, pp. 15-27.

Garfinkel, SL 2016, 'The Cybersecurity Mess', Citeseer.

ISPB 2013, *HSE Information Classification and Handling Policy*, HSE, HSE, Dublin, Ireland.

Khando, K, Gao, S, Islam, SM & Salman, A 2021, 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & Security*, vol. 106, p. 102267.

Koch, R, Stelte, B & Golling, M 2012, 'Attack trends in present computer networks', in *2012 4th International Conference on Cyber Conflict (CYCON 2012),* pp. 1-12.

Kritzinger, E & Von Solms, SH 2010, 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*, vol. 29, no. 8, pp. 840-847.

Martin, KD, Borah, A & Palmatier, RW 2017, 'Data privacy: Effects on customer and firm performance', *Journal of Marketing*, vol. 81, no. 1, pp. 36-58.

Martin, KD & Murphy, PE 2017, 'The role of data privacy in marketing', *Journal of the Academy of Marketing Science*, vol. 45, no. 2, pp. 135-155.

Mathur, M 2019, 'Where is the Security Blanket? Developing Social Media Marketing Capability as a Shield from Perceived Cybersecurity Risk', *Journal of Promotion Management*, vol. 25, no. 2, pp. 200-224.

Pienta, D, Thatcher, JB & Johnston, A 2020, 'Protecting a whale in a sea of phish', *Journal of Information Technology*, vol. 35, no. 3, 2020/09/01, pp. 214-231.

Roger, AG 2022, 'Cybersecurity Insurance', in *Ransomware Protection Playbook*, Wiley, pp. 85-112.

Rouge, P, Yeung, C, Salsburg, D & Calandrino, JA 2020, 'Checkout checkup: Misuse of payment data from web skimming', pp. 1-16.

Wolff, ED, Growley, K & Gruden, M 2021, 'Navigating the solarwinds supply chain attack', *The Procurement Lawyer*, vol. 56, no. 2, pp. 3-11.