ICT, Digital Subscriptions and Cyber Security

Art Phillips

January 2023

Information and communication technology (ICT) products and services are playing an essential role in the business world to heighten productivity as well as with our personal family life.

These products are essential to running a successful and productive business as they provide solutions to accounting, i-cloud storage services, communication such as zoom, office essentials such as email, documents, presentation software, databases and many other. And when it comes to family life the subscription services are endless, such as Netflix, Foxtel, Stan, Apple TV, Disney and the like for visual entertainment viewing, and for music many of us use a variety of choices, such as Apple Music, Amazon, and Spotify for streaming music.

Most of the products we use today are subscription based which has added a new layer to our operating cost expenses, and family overheads. A subscription model is a type of business where customers pay a recurring fee to access desired content or services which can be paid monthly or yearly.

As Faisal Kalim writes in 'What's New in Publishing', 'The market for digital subscriptions is currently valued at USD 650 billion dollars according to a new report from 'Subscription Trends' (2022) from Lineup, a subscription management solutions provider. It's expected to reach USD $1.5 trillion dollars by 2025, more than double its size today - a strong indication that the rise of the subscription economy is not a passing fad.

At least one subscription service is now used by 205 million Americans, up 13% from 182 million in the first quarter of 2020. Last year, subscription commerce sales climbed 41%, and experts estimate their value at $28B'.

Australian Statistics

As PayPal Australia says, as reported in LSN Global, 'some 86% of Australian businesses that have implemented a subscription model have reported an increase in revenue'.

They also state, 'e-commerce is also booming on the continent, with three quarters of Australians shopping on their mobile phones. Furthermore, with subscription models increasingly popular among younger shoppers, these 'set and forget' services are paying off for businesses, as 86% of businesses reported increases in revenue after implementing these models.

However, there is still an opportunity for brands looking to maintain a recurring revenue stream, as only one in 10 Australian businesses currently offer subscriptions. Opting for a subscription pricing model can significantly drive revenue'.

Kalim, from What's New in Publishing (online) also writes,'The subscription economy has been growing since before the pandemic. The increasing number of options available to users created concerns about subscription fatigue. However, the pandemic showed that subscriptions have staying power as demonstrated by many publishers who continue to register growth post-pandemic highs.

Gannett, a subscription-led, digitally focused media and marketing solutions company empowering communities to thrive - https://www.linkedin.com/company/gannett/ reported a 46% year-over-year increase in digital subscriptions in November 2021 to reach 1.5M subscribers. Hearst (magazine online) https://www.hearstmagazines.co.uk - grew its digital subscriptions by 50% over 2021'.

These subscription statistics also indicate that consumers now have more choice than ever before, so they're less loyal to the usual brands that may have been the flavour of use previously. This means an IT company needs to concentrate on catering extra-well for consumer needs in order to reinforce the value of the service they are offering.

Subscription Based Platforms

Recently when analysing my own business requirements, that of a music production library label and music publisher, I realized just how critical each and every product and platform choice is that I use in my business; from online accounting software, marketing platforms, music digital delivery and storage services, customer relationship manager software, F2F meeting software, storage and sharing platforms, audio recording platforms including audiomovers software to record remotely from one country or city to my Sydney recording studio base, as well as many others services. We can now access orchestral sample sounds and sound libraries via i-cloud seamlessly, meaning for me as a music creator, composer and music producer that I only need to take a small easy to carry laptop anywhere I travel to accomplish some very big tasks, which normally required full-blown state-of-the-art recording studio facilities do so.

The below is a spreadsheet of all my subscription services relating to the running of my music business. I track this periodically as it is critical to realize what each and every program and service is doing, why you require them, how you are using them, if they are effective for your purpose and if they are doing the intended job. In addition, the spreadsheet allows me quick reference to the services that I engage, where I can then research to see if there is something better for each task.

The products and services that I currently utilize are:

PRODUCT	SERVICE	EFFECT OF USE
XERO	Accounting software – cloud-based	Bookkeeping using bank feeds, reconciliation, BAS exports to the ATO, invoicing, and allowing accountant access rather than having to prepare documents for them at the end of the year.

Pipedrive	CRM, customer relationship manager, cloud-based program that has exceptional tracking and a depth of analytics available.	One-stop contact database with historical note keeping, tracking of projects + progress of, marketing planning and implementation, auto promotional sends, reminders, email functions that lock to your main mail client program.
Harvest PRO 3	Product audition and licensing website – a search engine of all my production music library assets for clients to license the product with agreements automatically going through APRA AMCOS – the Australian music broadcast and mechanical right organisation.	Storing of product / music assets, in-depth metadata storage and tagging, creation of various music formats, encoding copyright protection methods and making available all my music product in categories, album genres, styles, mood, flavours, instruments used, notes on the emotional sound of each asset and a concise description of every track.
Zoom	On-line meetings	Essential for F2F efficiency.
Mailchimp	Marketing platform	I utilise this method for each new product release, as well as reminders and new marketing tactics to all my distributors, clients and my global audience.
Dropbox	Storage and sharing ability of anything and everything digital.	I use this extensively for all files that I need to share with my team, with my sub-contractors, collaborators, and the like.
Microsoft	Office 365 programs, including outlook client email.	Word docs, excel data, powerpoint, email, etc
AudioMovers	Remote recording globally.	Ability to record to and from anywhere, back to my studios in Sydney.
Apple	Music, visual content, etc	Music, visual content, etc
Spotify	Music streaming service	Being able to listen to everything in the global marketplace on the go that has been commercially released – essential for my business to understand currency of product and the markets.

Linkedin	Bio storage and advertising of personal and company profile.	Bio storage and advertising of personal and company profile.
Lawpath	Professional documents for business with e-docsign ability.	At times, helps with legal costs for the small general agreements. I generally use a solicitor for most legal matters and recommend doing so.
Adobe	Various - photo, visual, pdf extractions.	photo, visual, pdf extractions.
Shutterstock	Stock images at reasonable costs.	Use in marketing and album artwork, etc.

There is a digital program solution for almost everything – or so we think. And for the techy' entrepreneur – here's an incentive to discover and create something new, something needed, something that has not been done before to solve a problem in the IT area for businesses and for the individual, and I suspect there are still hundreds of opportunities ready to be grabbed. **Thinking caps on!** And don't forget to trademark and register your idea and IP before offering it to the world.

The greater the innovation, the greater success!

Data Security

With the increased use of subscriptions and digital programs in our world there is a heightened rate of security issue breaches that we need to risk manage, and some breaches can be catastrophic!

Individuals, small businesses, large organizations and governments are all at risk. A security breach can affect anyone who has provided personal information and anyone who has collected and stored it.

Cyber security threats span many styles of security invasion, but the seven threats that most professionals should be aware of are:

1. Malware threat

Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software. Cisco reports that malware, once activated, can:

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

2. Emotet

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as “an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware.”

3. Denial of Service

A denial of service (DoS) is a type of cyber-attack that floods a computer or network so it can’t respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the handshaking process and carry out a DoS.

4. Man in the Middle

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

5. Phishing

Phishing attacks use fake communications, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as - providing a credit card number. “

6. SQL Injection

A Structured Query Language (SQL) injection is a type of cyber-attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

7. Password Attacks

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that relies heavily on human interaction and often involves tricking people into breaking standard security practices. Other types of password attacks include accessing a password database, finding dates of birth, places of birth and the like.

As IBM says, ‘When properly implemented, robust data security strategies will protect an organization’s information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization’s visibility into where its critical data resides and how it is used. Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements’.

The value of data in both business and personal life has never been greater than it is today.

As advised from the cyber.gov.au website, here are three tips on how to keep your data secure:

1. Limit the amount of personal information you share online, especially on social media. Only tell the organisation what they need to know to provide goods or services. For example, if you are asked for a home address consider if the organisation asking for it really needs it. That way, if the organisation is ever affected by a data breach, less of your data is impacted.

2. Look for organisations that have a commitment to cyber security. Don't use platforms that have a bad cyber security reputation or that you are unsure about.

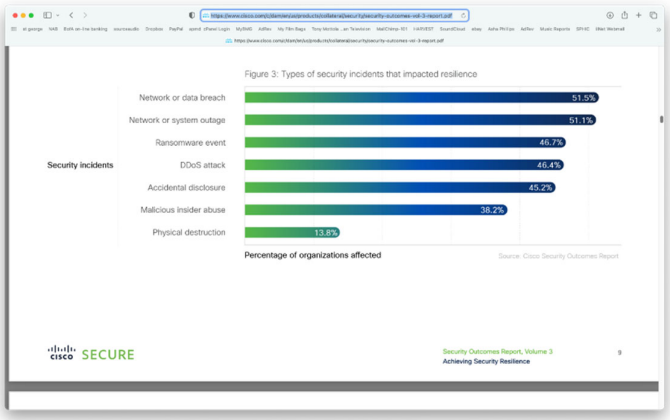
3. Avoid reusing passwords for online accounts. If you reuse passwords and any of your accounts are compromised, all of your accounts could be at risk. A password manager can help generate or store different passwords for you.

The Australian Government cyber security website continues with quoting, 'A password manager is an application that securely stores, generates and manages passwords for all of your accounts. With a password manager, you only need to remember one master password, the password manager takes care of the rest. Think of a password manager as a safe for your passwords and the master password as the key to the safe. You can use password managers on computers and mobile devices'.

As Cisco reports in their Security Outcomes report, Volume 3, Achieving Security Resilience, 'We asked (survey) respondents about the level of interest and importance top executives at their organization place on security resilience. The message couldn't be clearer. A full 96% of executives consider security resilience highly important.

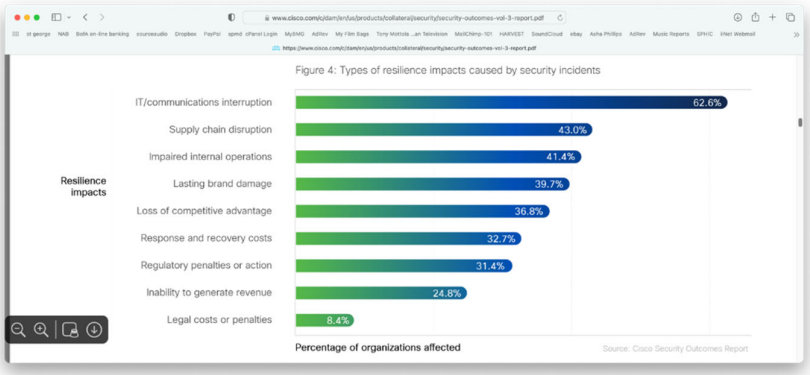
We also asked respondents to elaborate on the types of resilience-impacting incidents they experienced. As seen in Figure 3, network/data breaches and network/system outages were both cited by over half of participants that reported prior incidents. Ransomware and distributed denial-of-service (DDoS) attacks were the next most common event types, each affecting about 46% of organizations.

While some of the aforementioned incident types almost certainly involved employees as a vector of attack (e.g., clicking on a phishing email), overt, malicious abuse by insiders was reported by about 38% of organizations. Acts of physical destruction and sabotage were also cited, though substantially less often than the other incident types.



Respondents also had a lot to say about how these events impacted their organizations (see Figure 4). Over 60% referenced IT and communications disruptions, as well as the critical role ICT plays in security resilience. Supply chain disruptions landed in the #2 spot for business-level impacts. We've all been living with that pain lately, so it's no surprise that organizations are feeling it too.

While impacts to supply chain operations affect entities outside the victim organization, impaired internal operations (reported by roughly 41% of firms) wreak havoc on the inside. Brand damage sits at or near the top of the "what keeps you up at night" list of many executives, so it's telling that roughly 40% of these incidents result in that outcome. Loss of competitive advantage is another top concern, and it rounds out the top five resilience impacts'.



Authentication Security Methods

There are generally 6 common factors used with authentication:

- Password-based authentication. Passwords are the most common methods of authentication – but now outdated as the only source to authenticate.
- Knowledge-factor authentication – questions you decided to use as a 2nd back up method.
- Biometric authentication – facial, fingerprint, voice recognition.
- Token-based authentication – such as a dongle inserted into a computer to allow bank security codes to be sent via satellite.
- Multi-factor authentication – password and one or and two additional methods (as above).
- Certificate-based authentication – scan of a document verification (license, passport, etc).

As we are all experiencing today, every time we log into one of our regular subscriptions or programs we need to verify our name or email, enter our password and then we are now required to view our mobile telephones 'authentication app' to gain the ever changing / revolving digital security code. Life has gotten complicated, but we can rest assure that these extra safety factors are proving good risk management tactics.

As ‘Computing’ website UK states: ‘We are fans of authenticator apps, these take over from SMS text messages (doing) the job of sending you a one-time code to confirm that it’s you logging in to an account by generating the code securely on your phone’.

They continue to write: ‘Why is that safer than an SMS text message?

SMSs are vulnerable to a couple of types of attack. The most likely is that someone convinces your mobile provider to send them a SIM card for your number, which would mean they could get all your codes and get into your accounts. Less likely, but still possible, is what’s called a ‘man-in-the-middle’ attack that intercepts your SMS messages. An authenticator app doesn’t rely on your SIM card or the mobile networks’.

How authentication apps work

Authenticator apps generate a one-time code that you use to confirm that it's you logging in to a website or service; they provide the second part of what's called two-factor authentication (2FA).

When you set up an authenticator app with a website, that site generates a secret key - a random collection of numbers and symbols which you then save to the app. The site usually shows you that key in the form of a QR code. When you scan that with the app, the key is then saved to your phone. Then when you log in again to that website, it asks you to check your app for a code which it displays for a short time, usually 30 seconds. The app generates that code by combining the key the website gave you when you first set it up with the current time. If the key in the access code matches the one the website holds for you, it knows the right person is trying to sign in.

Conclusion

The ‘set and forget’ convenience of subscription-based programs is certainly a great convenience - however it has added a substantial layer of cost considerations for businesses and the individual consumer. We need to be mindful of what we require and keep track of the hidden, so to speak, annual charges coming onto our credit cards.

When setting passwords it is recommended to choose carefully, and to change often. Advice from many experts has been never use birthdays, pet names, nicknames, favourite names or numbers, city you were born in, etc – as hackers use many tricks to obtain breaching ability. You often see facebook posts from unknown entities which are very tempting to reply to - posts saying things like ‘bet you cannot find a word starts that in p and ends in p’ for example, ‘what is the tv show you most miss’, ‘what song would you play at a ------ ‘ (whatever), ...and these posts occur constantly. Clear advice - do not ever be tempted to write in your answers, as these are red-flags to security breaches, so - do not be enticed into interacting.

References

Australian Government Cyber Security website, sited January 2023, https://www.cyber.gov.au/learn/threats/data-security

Australian Government Cyber Security website, your password manager, sited January 2023, https://www.cyber.gov.au/acsc/view-all-content/publications/quick-wins-your-password-manager

Cisco, 2023, Security Outcomes report, Volume 3, Achieving Security Resilience, https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-vol-3-report.pdf

Computing, UK website, sited January 2023, https://computing.which.co.uk/hc/en-gb/articles/360006153539-How-to-set-up-an-authenticator-app-for-two-factor-authentication

Gannett, a subscription-led, digitally focused media and marketing solutions company empowering communities to thrive - https://www.linkedin.com/company/gannett/

Hearst (magazine online) https://www.hearstmagazines.co.uk

IBM website, sited January 2023, https://www.ibm.com/au-en/topics/data-security

Kalim, F, 2022, What's New in Publishing, Digital subscription economy to grow to 1.5T by 2025: Key trends for publishers https://whatsnewinpublishing.com/digital-subscription-economy-to-grow-to-1-5t-by-2025-key-trends-for-publishers/

LSN Global web publication, 2023, Subscription models drive business growth in Australia, PayPal quote, https://www.lsnglobal.com/news/article/22892/stat-subscription-models-drive-business-growth-in-australia

Adjunct Professor Art Phillips is Director, UBSS Centre for Entrepreneurship