ARTICLE

Intellectual Property

Preventing and Managing an Intellectual Property Crisis in Open Waters

Your intellectual property (IP) could be spilling out of the corporate rockpool!

In early 2020, the COVID-19 global pandemic arrived on the sunny shores of Australia. The physical real-world quarantine, lockdowns, and social distancing that ensued had an immediate technological impact on the working practices of corporate Australia.

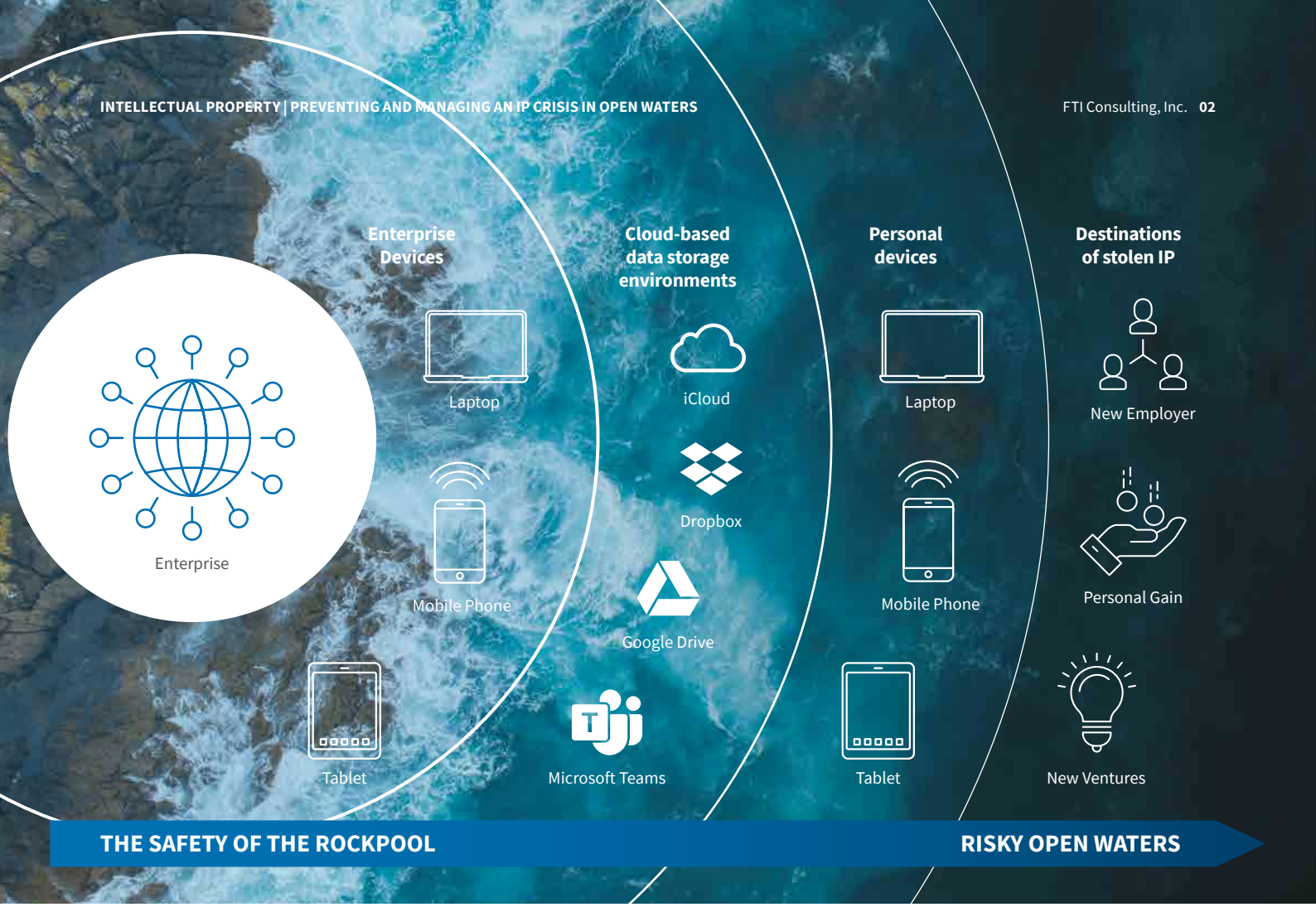
2021:
41%
of Australians regularly working from home.

Massive numbers of people were suddenly required to work from home. In response, corporate collaboration tools such as Microsoft Teams, Zoom and Google Suite boomed, adding tens or hundreds of millions of users in mere months. While a small pocket of early adopters of video conferencing and online collaboration tools revelled in the popularity surge of these platforms, most organisations were left with little choice but to deploy these new technologies without the due-care and consideration they would otherwise have applied.

Within a few short weeks, organisations across Australia nervously authorised the physical movement of critical corporate IP from a single instance of data securely stored in the enterprise – the safe, protected shallows of the corporate 'rockpool' – to the uncharted depths of the open ocean; multi-instance, synchronised and available on the personal mobile phones and laptops of staff working at home.

Like the rockpool, the solutions themselves could be implemented to be practical and secure when configured appropriately, but at such short notice the IP was very much thrown in the deep end without the supervision or control to detect or prevent a crisis. In March 2021, the Australian Bureau of Statistics (ABS) reported 41% of Australians were working from home at least once a week - nearly double the numbers prior to March 2020.

In this paper, FTI Consulting information governance and investigations experts explore some of the risk of IP being exposed in these open waters, share investigations know-how and outline prevention measures.



CONTROLLING & MONITORING THE DATA FLOW

Those organisations that have not yet knowingly experienced data loss through online collaboration tools may be under the false impression they've miraculously avoided a crisis. However, as the pandemic in Australia loosens its grip on personal mobility and the economy recovers, there could be new and emerging insider threats – current staff who are considering the value of the critical IP they have access to for personal gain, or future business ventures.

Organisations should carefully consider preventative and monitoring actions to ensure they:

— maintain **control**

— maintain **visibility**, and

— apply the rule that "**not all data is equal**" – different kinds of data may require different security controls.

1. Control

Start by locking down user accounts to allow only the access and rights required for the users' specific roles. In particular, where your organisation has expanded its network perimeter to include your staff's personal devices e.g., under a Bring Your Own Device (BYOD) policy, ensure that they cannot expand the perimeter even further. For example, disable:

— **email forwarding:** prevent users sending email on bulk to unapproved devices

— **synchronisation:** users cannot download archives to their personal devices

— **folder downloads:** so that users cannot download data in bulk to their personal devices

2. Visibility

Generate detailed logs and alerts to ensure that access to critical content and unusual behaviour is recorded, trigger alerts where appropriate, and retain information for a sufficient period, which will greatly enhance investigations when necessary. Example alerts could include:

- access to critical data
- large downloads (volume & quantity)
- access from unusual IP address or locations
- access at unusual times or days (e.g. late nights, early mornings, weekends, or when users are known not to be working)

INVESTIGATIONS INTO DATA LOSS

Investigations into the loss of data from corporate collaboration solutions have become commonplace in 2021. An important element of any investigation is the data logs that include detailed information about user activity within the relevant system.

Commonly investigated issues over recent months include:

SharePoint Downloads

With more people working from home than ever before, staff have found downloading or synchronising SharePoint data to their local devices too convenient and tempting to resist. Unfortunately, this practice can result in leakage of critical IP.

Generally, most staff are unaware that the SharePoint system (when properly configured) is logging their every action. During SharePoint investigations, we've been able to quickly establish a remote connection to the client's Microsoft 365 environment and harvest detailed user logs, which list activity such as Access, Download, Sync, Send, and Share. While these logs can be large and difficult to manipulate, we've found using forensic tools to visualise user activity over time to be an impactful and effective investigation solution that has enabled us to resolve cases faster and with greater clarity.

Email Forwarding

As investigators at FTI Consulting, we've found that email forwarding rules are often used to exfiltrate data. Professional external threat actors (hackers) who wish to compromise a user account will frequently establish a sequence of rules to forward incoming email to non-enterprise accounts, and then immediately delete the item from sent emails in an effort to remain undetected and not alert the user or leave a trail for administrators. In contrast, 'insider' threat actors (such as current staff seeking to steal IP) are generally less sophisticated. We've found that insider threat actors will often use forwarding rules unaware of the logging functionality of corporate email systems. Rather, they will simply establish rules to forward emails to their personal account, but make no attempt to cover their tracks.

Apple iCloud Backups and Sync Data

Bring your own device (BYOD) remains a popular choice for mobile device users in the workplace in 2021. A potential pitfall of this approach is that many users are encouraged to use their personal device account (such as an Apple ID), which synchronises data to the cloud and then to all devices associated with that account. When BYOD solutions are configured correctly, organisations can effectively manage and control their IP. However, our experience in recent investigations has been that appropriate configuration remains beyond the expertise and budget of many organisations. As a result, past employees are often left unsupervised to simply download corporate data onto their new post-employment device. Poor BYOD management has enabled sensitive communications, contact details, and even client or prospect information to simply (and literally) walk out the door.

USB Devices

A classic data egress technique that remains popular today, is to plug in a USB memory stick, drag the files over, then pull it out and walk away. However, with the post-COVID-19 rise of BYOD, the source device has changed. Staff are no longer connecting USB devices to just their corporate device; they're increasingly connecting them to personal devices enabled and authenticated as corporate collaboration tools.

As such, we've found that personal devices are an increasingly integral part of an IP theft investigation.

POWERS TO INVESTIGATE

Gaining access to personal devices can be problematic at best, and frequently relies on the careful deployment of legal search powers.

If the device owner does not consent to the examination of the device, a court order can be sought. Should this becomes necessary, the court order must be drafted with sufficient detail of known events and include all possible related devices, accounts, and authentication details. As such, successfully obtaining a suitable court order requires close collaboration between legal advisors and experienced forensic professionals.

In seeking an order, it's essential to have a sense of the logistical challenges of searching for your IP assets.

- Specifically, how long is it likely to take?
- How deep will the search need to go?
- Will it include deleted or partially deleted data?
- What tools can be deployed?
- Can keywords or indicators be used to narrow the search?

It's common for orders to set strict timeframes on how long investigators can hold target devices, so it's important to understand what will be required for a successful search when pursing such an order.

Additionally, you should consider any requirements to remediate IP found on the target devices. If IP is located, can this data be securely deleted and, if so, what level of certainty is required? Options range from performing a full wipe or factory reset of a device, selective deletion of data, the closure of accounts, and even confiscation of the device. These are factors that must be accounted for in the court order to enable you to protect and successfully regain control of your IP.

SECURE & LEARN

Learning from past events is essential. As the saying goes, 'never let a good crisis go to waste' - it's often easier to seek approval and budget to address a system that has been compromised and exploited. Review and take a proactive, preventative approach. In the wake of an incident, take action to close known security gaps, identify and address other security risks, and improve processes.

PRIVACY & FINES

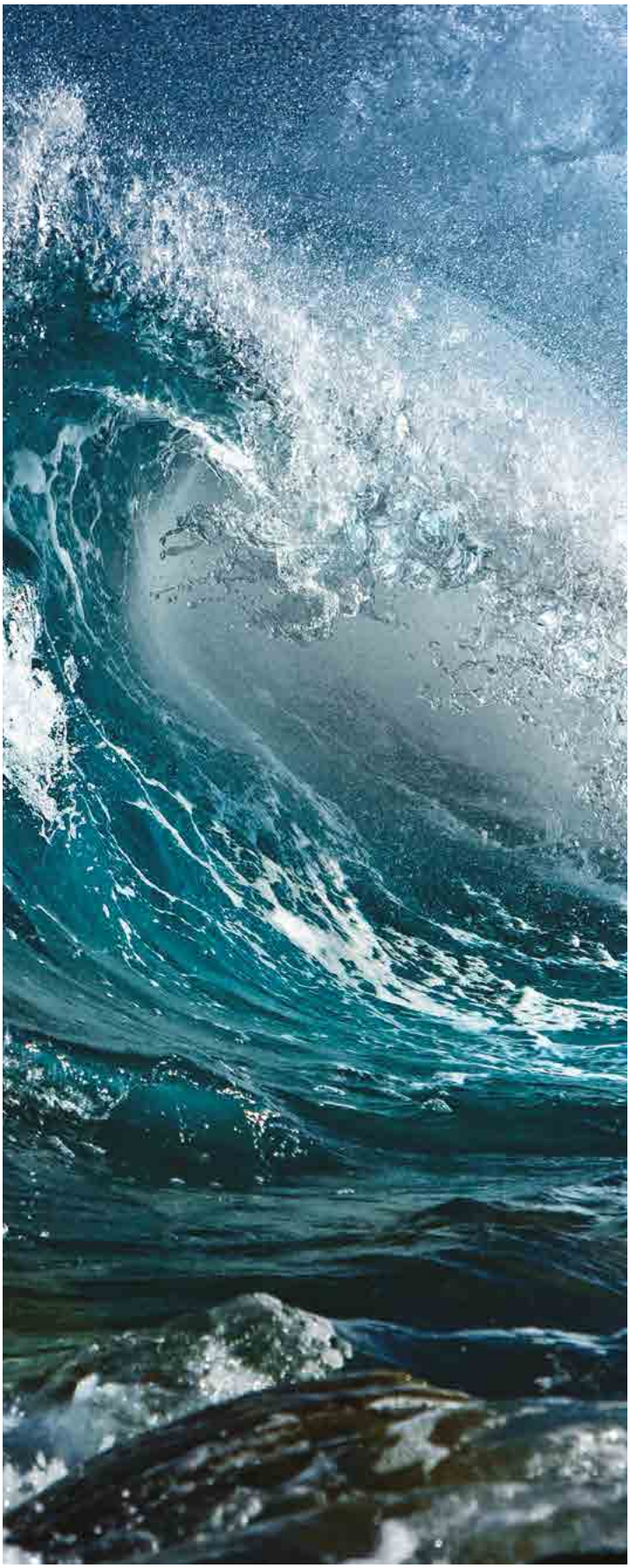
Against the backdrop of the challenges, it's also important to consider the perspective of the regulator.

The *Privacy Act* 1988 (Cth) ("Privacy Act"), requires that private sector organisations take 'reasonable steps' to keep personal information secure. Generally speaking, this means putting in place solutions and processes to mitigate known risks (Australian Privacy Principle 11.1).

Organisations are also required to destroy or de-identify personal information that they no longer require for a lawful business purpose (APP 11.2).

Additionally, the Privacy Act includes mandatory data breach obligations, with strict timeframes (Part IIIC).

During our observations of organisations experiencing an IP crisis, management often find themselves facing pointed questions from the regulator, especially when the data breach involves personal information. The crisis may further highlight flaws in security, or the "over" retention of personal data, which can lead to regulatory action such as investigations, enforceable undertakings, civil penalties, or unwanted media attention and public criticism.



CONCLUSION

Adopt a multidisciplinary approach

In recovering from an IP crisis, the key is to adopt a flexible, multi-disciplinary approach. These crises are frequently multi-faceted, requiring multiple disciplines including cybersecurity, digital forensics, privacy and strategic communications, to wage an effective response. Plan ahead so that you're not trying to find the "right people" in the midst of a crisis – it's best to identify your consulting and legal partners ahead of time (and, ideally, include this information in your crisis management plan).

Invest in crisis response capabilities

Organisations that proactively invest in their crisis response capability are the ones that weather the storm the best. In the end, fortune favours the prepared. Consider focusing on building capability and minimising your risk of an IP breach by understanding your data assets and enabling data minimisation, building your crisis response processes, training key staff, and testing and strengthening your security.

In the wake of COVID-19 and the changes it has instigated, you may not be able to bring all your IP back to the safety of the rockpool – but it's not too late to deploy the life rafts and patrols, and be prepared.

CHRISTOPHER HATFIELD
Managing Director
+61 (0) 437 373 130
christopher.hatfield@fticonsulting.com

TIM DE SOUSA
Senior Director
+61 (0) 413 248 107
tim.desousa@fticonsulting.com