EMPLOYEE DEPARTURE CHECKS

Best practices

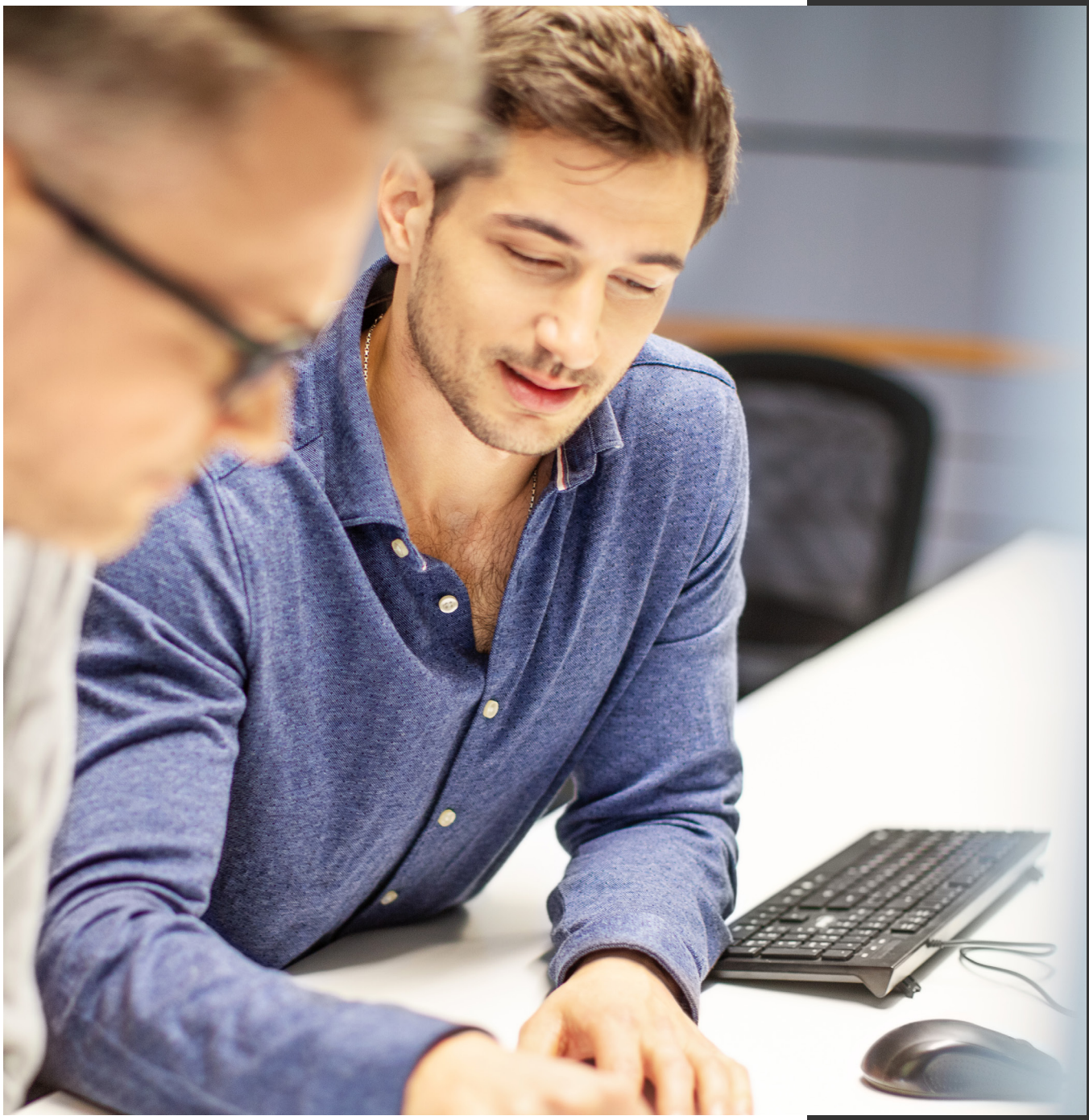
IDEAS | PEOPLE | TRUST

BDO

DEPARTING EMPLOYEES: WHAT ARE THE RISKS?

Intellectual Property (IP) and other Commercially Sensitive Information (CSI) are valuable assets to any organisation. Most of the time when employees leave, there should be no cause for concern around them taking CSI or IP with them. However, sometimes additional risks present themselves and further analysis is warranted. In our experience, if a disgruntled or otherwise acrimonious ex-employee wants to damage your organisation's reputation, they will overtly or covertly find a way to do so.

BDO aims to provide you with information and a checklist to act appropriately and respond to these risks proportionally, so that you can protect your organisation. .



PREVENTATIVE CONTROLS

> *An ounce of prevention is always better than a pound of cure*
>
> **BENJAMIN FRANKLIN**

It is important to not just consider your response, but to start with prevention. There is benefit in having employment lawyers check your employment contracts on a regular basis, including any clauses that deal with IP and CSI. Ensuring that contractual clauses are in line with your business practices will go a long way when managing risk and protecting sensitive information. It also allows for the IP and CSI to be identified with greater ease by all stakeholders. This does not only apply to information (security) controls, including access management based on the principle of least privilege, but also regarding whether your employees have been adequately and regularly trained.

Employees should only have access to the information required to perform their role. For example, an employee working in your logistics team does not require access to the human resources or payroll files. Similarly, a salesperson doesn't need access to the blueprints for your latest ground-breaking software innovation.

In this modern environment of cloud and hybrid IT landscapes, better practice can look very different from organisation to organisation. An IT or Cyber professional adviser should provide advice and recommendations for your organisation's unique circumstances.

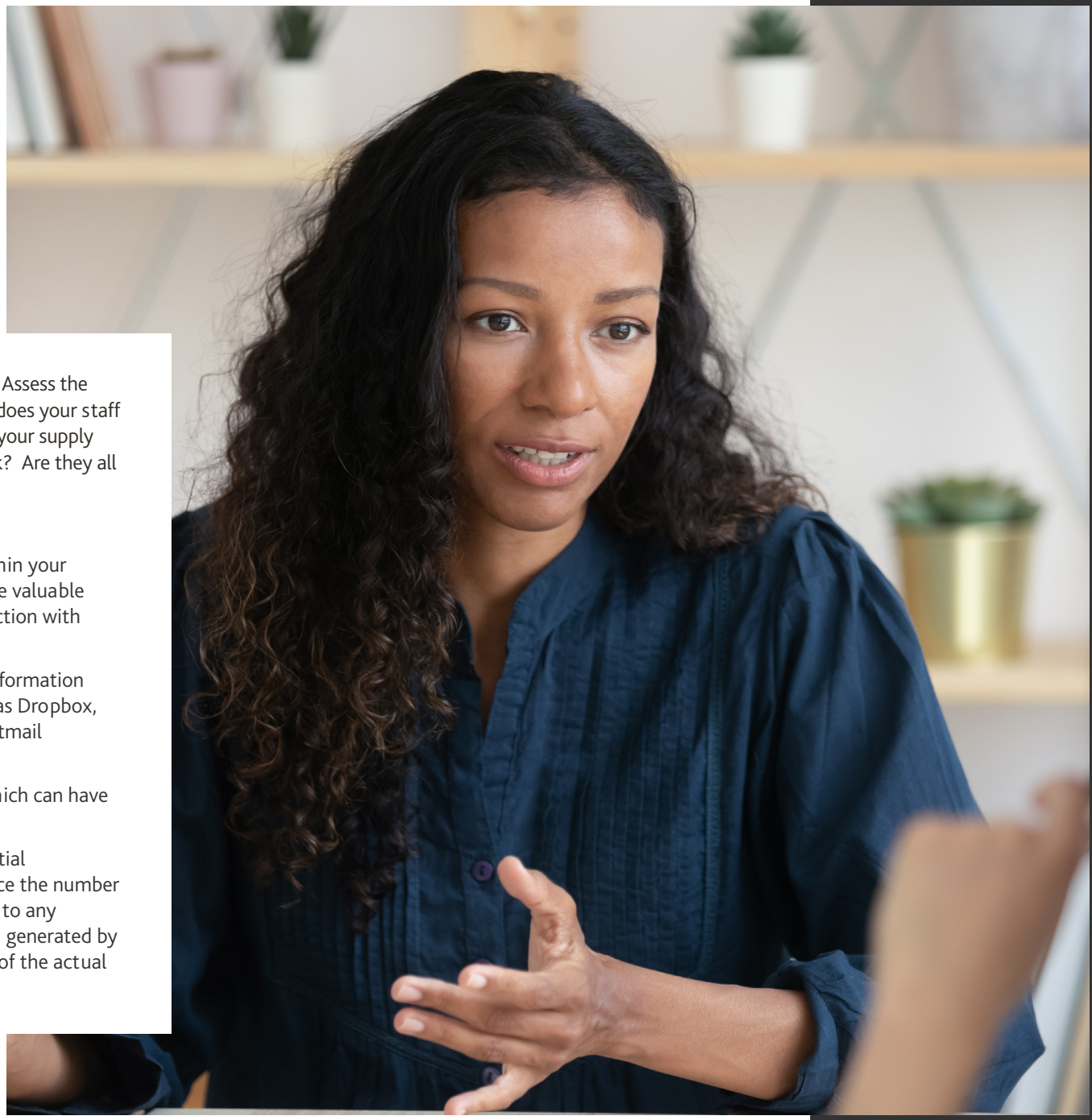
At BDO we recommend that at the minimum you should consider the following elements:

- ☐ Implementing extra protections around your network, its perimeter, and areas of the network where sensitive or otherwise valuable information is held
- ☐ Applying the principle of least privilege across all users, groups and roles whereby using controls to limit access to relevant employees/services/devices only
- ☐ Using a security/information classification system for documents to indicate the information's private or confidential nature.

In addition, the following measures can be implemented to prevent information loss:

- ☐ Consider using encryption to protect sensitive or valuable information on your network but enforce its use on portable storage devices. Most modern email clients also allow encryption on emails to protect valuable information in circumstances when it needs to be shared with third-parties. This helps control who has access to the information, if it is distributed outside of your organisation
- ☐ Consider whether it is beneficial to remove write access to storage devices (USB drives or portable hard drives).

DETECTIVE CONTROLS



Modern technology allows for the detection of information theft. Assess the methods in which information can leave your organisation – how does your staff interact internally and externally? What are common practices in your supply chain? How does information exchange with your customers work? Are they all required for business-as-usual (BAU) activities? Are they secure?

BDO suggests considering the following detective controls:

- ☐ Implementing audit logging on areas of your network or within your document management system where sensitive or otherwise valuable information resides. This will provide a record of user interaction with critical documents
- ☐ Utilising a proxy server or web filter to restrict or monitor information leaving your organisation via internet file sharing sites such as Dropbox, One Drive, or web-based personal email services such as Hotmail and Gmail
- ☐ Implementing and keeping print and security access logs, which can have automatic alerts sent when unusual activity occurs.

Whilst these measures won't guarantee that private or confidential information will not leave your organisation, they certainly reduce the number of ways it can. The correct messaging can also act as a deterrent to any employees considering taking confidential information. Log files, generated by monitoring efforts, may also provide vital evidence in the event of the actual or suspected loss of information.

DEPARTURE CHECKLIST

If the unfortunate situation occurs that a disgruntled employee departs your organisation, it is important that you hold an exit interview with them. Not only to learn as an organisation around what can be improved in the employee experience, but also to remind the employee of exit protocols.

To prevent information leakage BDO also recommends that further action should be taken:

- ☐ Formally requesting the employee to return any CSI and IP (or any other assets for that matter) in possession of the employee
- ☐ Revoking systems access and physical/building access as soon as practicable
- ☐ Proactively analysing the print and security access logs, as well as any other relevant monitoring information available in your organisation, for any indication the employee might have (including inadvertently) taken CSI, IP or any other information that is not public
- ☐ Ensuring the final pay and transfer of knowledge where possible.

While not a definitive list, this departure checklist focuses on the most important steps to mitigate the risk of misappropriated or otherwise lost information. It's important to note that additional steps such as final pay, and transfer of knowledge where possible, should also be considered in the employee offboarding process.

RESPONSE CHECKLIST

An organisation needs to respond quickly to any allegation or concerns regarding information leaks. This is vital in order to secure available evidence in a forensically sound manner, help uphold evidential integrity for the investigation, and to help mitigate the distribution of the information and any legal or reputational damage caused by the theft.

Often, if the information theft is intentional, the perpetrator knows digital/web-based exfiltration leaves a trail of evidence. To avoid leaving this evidence, they might opt to use physical storage media. Therefore, in the event of a suspected information theft by a (departed) employee, the potential evidence on the employee's devices needs to be adequately collected and defensibly stored in a forensic image. This needs to be done in addition to analysing the relevant logging and monitoring information mentioned in the departure checklist above.

However, this can't be done for every departing employee. Further, if the theft is discovered late after the employee has left, their device/s may have been wiped or re-purposed to someone else.

Therefore, it could be beneficial to create a shortlist of critical, high risk or senior employees (those with most access to CSI/IP) for whom it would be necessary to proactively image their device/s upon departure - and upon review, act on any suspicions that arise.

The analysis of a forensic image needs to be conducted by a suitably qualified and experienced Digital Forensic examiner. This ensures proper protocol is adhered to, evidence is interpreted appropriately and isn't contaminated in the process. This process will be critical if legal action, in any form, ensures.

A forensic examination can identify:

- Deleted emails containing suspicious activity
- Information or evidence which may substantiate any allegations of inappropriate or suspicious activity
- Metadata regarding files written to physical storage devices like USB drives or portable hard disk drives and further evidence of confidential information that may have been copied to those devices (even when the USB drive or disk is no longer available). Computers retain this type of information for longer than you might expect.
- Any documents printed or records accessed in the lead-up to the departure, that contain CSI and/or IP. Inspection, where available, of logs pertaining to documents printed or records accessed by the departing employee. Think client databases or secret recipes/blueprints, for example.
- Conduct interviews with other staff members the departed employee worked with.

Despite taking precautions, should you have a rogue employee or former employee attempting to use your CSI or IP for their own benefit or the benefit of a competitor, you should obtain legal advice from an appropriately experienced employment lawyer.

ABOUT BDO

As one of the world's leading Audit and Accounting organisations, we have clients of all types and sizes from large corporate organisations to private business, entrepreneurs and individuals across an array of industry sectors.

We are guided by our values that are the foundation of what we deliver – **IDEAS I PEOPLE I TRUST**.
This is about: delivering ideas and advice that create value; quality-driven people who are motivated by providing exceptional client service; and being trusted to get the job done.

BDO IN AUSTRALIA

With 245 Partners and over 2,100 staff, BDO in Australia has 12 offices located across Australia.

2,141 PEOPLE
12 OFFICES
245 PARTNERS
FIGURES TAKEN AS AT 01 APRIL 2022

To learn more about our services
CLICK HERE

NETWORK OF THE YEAR AWARD WINNER
INTERNATIONAL ACCOUNTING BULLETIN
AWARDS 2018

For more information on BDO visit our website:
www.bdo.com.au

OUR GLOBAL NETWORK

BDO's global network extends across 164 countries and territories, with over 95,000 people working out of 1,713 offices. But we're all working towards one goal: to provide you with exceptional client service. That means local resources who understand your business and industry, backed by a truly global network. No matter where you do business, we have people who know your business.

95,414+ PEOPLE
1,713 OFFICES
164 COUNTRIES
FIGURES TAKEN AS AT MARCH 2022

1300 138 991

www.bdo.com.au

NEW SOUTH WALES

NORTHERN TERRITORY

QUEENSLAND

SOUTH AUSTRALIA

TASMANIA

VICTORIA

WESTERN AUSTRALIA

This publication has been carefully prepared, but is general commentary only. This publication is not legal or financial advice and should not be relied upon as such. The information in this publication is subject to change at any time and therefore we give no assurance or warranty that the information is current when read. The publication cannot be relied upon to cover any specific situation and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances.

BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not give any warranty as to the accuracy, reliability or completeness of information contained in this publication nor do they accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it, except in so far as any liability under statute cannot be excluded.

BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee, is a member of BDO International Ltd, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2022 BDO Australia Ltd. All rights reserved.

22-06-0325