City of
Mount Gambier

Civic Centre, 10 Watson Terrace
Mount Gambier SA 5290

PO Box 56
Mount Gambier SA 5290

Telephone 08 87212555
Facsimile 08 87249791
**city@mountgambier.sa.gov.au**

mountgambier.sa.gov.au

**I hereby give notice that an Audit Committee Meeting will be held on:**

| | |
|---|---|
| **Date:** | **Wednesday, 15 May 2019** |
| **Time:** | **5.30 p.m.** |
| **Location:** | **Committee Room, Level 1**<br>**Civic Centre**<br>**10 Watson Terrace**<br>**Mount Gambier** |

# AGENDA

# Audit Committee Meeting
# 15 May 2019

**Graeme Maxwell**
**Chief Executive Officer**

**10 May 2019**

## Order Of Business

## 1 ACKNOWLEDGEMENT OF COUNTRY

**WE ACKNOWLEDGE THE BOANDIK PEOPLES AS THE TRADITIONAL CUSTODIANS OF THE LAND WHERE WE MEET TODAY. WE RESPECT THEIR SPIRITUAL RELATIONSHIP WITH THE LAND AND RECOGNISE THE DEEP FEELINGS OF ATTACHMENT OUR INDIGENOUS PEOPLES HAVE WITH THIS LAND.**

## 2 APOLOGY(IES)

Nil

## 3 CONFIRMATION OF MINUTES

## 4 QUESTIONS WITHOUT NOTICE

# 5 REPORTS

## 5.1 INTERNAL FINANCIAL CONTROLS - CUMULATIVE SPEND REVIEW 01/07/2018 TO 14/03/2019 - REPORT NO. AR19/18131

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/18131** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Kahli Rolton, Management Accountant** |
| **Authoriser:** | **Pamela Lee, General Manager Council Business Services** |
| **Summary:** | **A review of Council's cumulative spend by creditor for the period 01/07/2018 to 14/03/2019. Providing options for Executives to consider and implement in relation to managing creditor spending whilst adhering to Council's policies and procedures.** |
| **Community Plan Reference:** | **Goal 3: Our Diverse Economy** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/18131 titled 'Internal Financial Controls - Cumulative Spend Review 01/07/2018 to 14/03/2019' as presented on 15 May 2019 be noted.

## BACKGROUND

Cumulative spend analysis is an important part of ensuring that Council procures in an open and transparent manner in line with Council's internal financial controls procedure, procurement and acquisition planning procedure and procurement policy.

A recent review of Council's cumulative spends per creditor has highlighted the following areas for consideration:

1. How is Council ensuring it obtains value for money with its purchases in a decentralised purchasing environment?
2. How is Council maintaining control over its cumulative purchasing with creditors and ensuring it meets all the requirements of Council's policy *P420 Procurement and Disposal of Land and Assets* and its internal financial controls procedures?

The implementation of online purchase ordering in 2014 enabled Council to enhance its operational efficiency when placing orders and purchasing goods and services. It is important to ensure that any operational efficiencies gained are done so whilst maintaining the required level of internal controls and scrutiny.

Benefits of a decentralised online purchasing system include the removal of manual records and disseminating preparation of purchase orders and approving payments over a number of authorised officers. However, by increasing the number of employees with financial authority, an environment can be created where employees work in isolation without knowledge of what is in the best interests of Council as a whole.

Council's procurement structure as stated in Council policy P420 details that for purchases in excess of:

- $20,000 a *"Request for Expression of Interest"* (REOI) or Request for Quotation (RFQ) is required; and
- $50,000 a *"Request for Tender"* (RFT) is required.

P420 also states *"The value of the purchase will be calculated as follows:*

- Single one-off purchase – the total of the amount, or estimated amount of the purchase (excluding GST);
- Multiple purchases – the gross value, or the estimated gross value of the purchases (excluding GST); or
- Ongoing purchases over a period of time – the annual gross value, or the estimated annual gross value of the purchases (excluding GST);
- Purchasing including a trade-in/changeover – the gross changeover value being the gross value of the item *being purchased minus the value of the trade-in/changeover."*

Council has a comprehensive Prequalified Contractor Register (refer Attachment 1 of this report). This register ensures that contractors providing services onsite meet Council's requirements in regards to:

- Work, health and safety
- Holding appropriate and current insurances
- Being adequately accredited and/or licenced.

A number of improvements have been identified that are required to expand Council's management of purchases beyond that of just prequalification including:

- Pricing comparisons or catalogue items
- Overall rating of the supplier (council wide). This rating is required to factor in items such as:
    - Was the supplier compliant with Council instruction and procedures?
    - Did the supplier deliver on time?
    - Were the costs reliable and consistent to the supplier's word?
    - Did the supplier actively work with Council to obtain value for money?
    - In dealing with the supplier, were they polite and respectful?

Progress has been made into the ability of the 'purchasing module' within Council's enterprise system, Authority to provide the features listed above and also apply limitations on staff to only be able to raise purchase orders from prequalified or preferred suppliers. Unfortunately, the ability of Council's enterprise system Authority to provide these features is not available at this time, so further investigation has started in to the use of an online procurement portal.

## DISCUSSION

A review of cumulative spends by creditor from 1 July 2018 to 14 March 2019 highlights a number of cumulative spends that has warranted further consideration.

There are a number of internal financial control matters that arise when considering why staff purchase from a particular supplier. These include convenience and conflict of interests (refer Attachment 2 for conflict of interest checklist).

With decentralisation of purchasing and the number of Authorised Officers within Council able to make purchasing decisions, it is important to review cumulative and general spending habits and patterns to ensure value for money is obtained and Council is meeting its administrative procedures and procurement policy. When employees act alone in regard to making purchases, they may not benefit from Council's corporate discounts, plans or agreements and place unnecessary burden on Council's limited resources.

The benefits of procuring goods and services in an open and transparent market was demonstrated last year by the completion of a formal tender process for the supply and delivery of mobile bins. Prior to the formal procurement process, Council ordered bin supplies ad-hoc with the supplier and consequently payed recommended retail prices. By going to the market, the same supplier from whom the bins were purchased out of contract was the successful tenderer, however Council was able to secure a better price. It is anticipated Council will save approximately $10,000 over a two year period. Cumulative spend analysis enables identification of other similar items that can be added to Council's forward procurement plan.

There are a number of suppliers who Council are spending considerable amounts with in a financial year. In light of the procurement benefits generated from formally procuring mobile bins, the following items have been identified as priority procurements.

Table One: Priority Procurements

| Goods and/or Services | Approach | Anticipated date |
|---|---|---|
| Grave site excavation | Open market – local providers encouraged to apply | 2020 FY |
| Tree and stump removal | Open market – local providers encouraged to apply | 2020 FY |
| Corporate Wardrobe | Service review to determine requirements followed by open market approach if required (LGA panel and local providers) | 2020 FY |

| | | |
|---|---|---|
| Landfill monitoring | Open market approach | 2021 FY |
| Banking facilities | Open market approach – will take considerable pre-investigation work to ensure best outcome for all internal/external stakeholders involved | 2021 FY |
| Kerbing and footpath construction | Open market – local providers encouraged to apply | 2021 FY |
| Spraying | Open market – local providers encouraged to apply | 2021 FY |
| Stationery | Open market – local providers encouraged to apply. Need to consider online purchasing portals for all areas of Council to efficiently purchase | 2021 FY |
| Street and roadwork signs | Open market approach / LGA panel | 2021 FY |
| Security services | Open market – local providers encouraged to apply | 2022 FY |
| Labour hire | Open market – local providers encouraged to apply. Will take considerable pre-investigation work to ensure best outcome for all stakeholders | 2022 FY |
| IT equipment and copiers | Open market – local providers encouraged to apply | 2022 FY |

It is noted that investigations have found that some staff are engaging the services of contractors who are not listed on the prequalified contractor register. Due to the prequalified register being held separate to Council’s corporate wide facility, it is difficult to prevent this prior to it occurring. The ideal control is to have Council’s enterprise software system working so as to limit/mitigate the ability of staff to generation purchase orders with non-prequalified contractors. This functionality is at the forefront of requirements during the online procurement portal investigations.

## CONCLUSION

Cumulative spend analysis is an important part of ensuring that Council procures in an open and transparent manner in line with Council’s administrative procedures and procurement policy.

The procurement forward plan is being expanded to encapsulate the items listed at Table One of this report to ensure Council acts within its procurement policies, better practice and has the opportunity to derive both financial and non-financial benefits.

In order to operate efficiently and effectively, investigations will continue for an online procurement solution that reduces the gaps identified in relation to engaging prequalified contractors, rating suppliers, providing data analysis and reporting and offering pricing comparisons.

## ATTACHMENTS

1. Prequalified Contractor Register 2017 - 2019 - week commencing 08/04/2019 ⇩
2. Conflict of Interest Checklist ⇩

## Prequalified Contractors List as of 08/04/2019

| Classification | Description / Further Details | Contractor Name | Status | Rating | Supplier No |
|---|---|---|---|---|---|
| Air Conditioning/Refrigeration | Refrigeration and air conditioning repairs and installation | Gordon Refrigeration Pty Ltd | Current | N/A | 210 |
| | Airconditioning and refrigeration repairs | Mac's Refrigeration | Current | N/A | 2771 |
| Astestos ID/Removal | Asbestos Removal | AAA Asbestos Solutions | Expired | N/A | 5158 |
| | Asbestos Removal, Sampling, Surveys, Soil Remediation, Emergency Cleanups, Inspections, Demolition | South East Asbestos Pty Ltd | Current | N/A | 3981 |
| | Asbestos Removal & Demolition | JWNH Enterprises Pty Ltd T/A Th | Current | N/A | 6055 |
| Building Maintenance | Aluminium fabrication and glazing | Viridian | Current | N/A | 223 |
| | Installation and inspection of roof safety systems | Correct Safety Pty Ltd | Current | N/A | 5076 |
| | Security Services | Heemskerk Security & Shredall Security | Current | N/A | 1392 |
| | Contract AF17/184; Cleaning, hygiene and waste management services | Menzies International (Aust) Pty Ltd | Expired | N/A | 5368 |
| | Security & Locksmith & Guards | Wilson Security & Locksmith Service | Current | N/A | 2723 |
| | Joinery manufacturers | M S Hein & Sons | Current | N/A | 1009 |
| | Cleaning Services | Apec Cleaning Service | Current | N/A | 1978 |
| | Window cleaning, gutter cleaning, solar panel cleaning, bee extermination, audio visual sales service and | MA & ML Verrall | Current | N/A | 5194 |
| | Glass & glazing, aluminium products, repairs and maintenance | Mount Glass & Glazing Pty Ltd | Current | N/A | 558 |
| | Restoration and installation of sculptures, monuments and buildings | Ivo Tadic | Current | N/A | 1813 |
| | Ceiling, wall linings, external façade systems, carpentry, demolition, external cladding | MG Plasterers Pty Ltd | Current | N/A | 2289 |
| | Plumbing, Gas, Maintenance, Sheet metal, Roof work | HR & LM Zaadstra Pty Ltd | Current | N/A | 1990 |
| | Plastering | Luke Odgers | Expired | N/A | 5760 |
| | Wall and floor tiling and associated tasks | Danny Stephenson Tiling | Current | N/A | 4295 |
| | Gutter vacuum cleaning, tank cleaning, high | Blue Lake Jet Vac | Current | N/A | 5919 |
| | Primarily window cleaning but also pressure | South East Professional Window | Current | N/A | 2159 |
| | Carpet cleaning services | Cleaneasy | Current | N/A | 3581 |
| | Carpentry and General Maintenance | Cole Construction and Carpentry | Current | N/A | 6126 |
| | Supply/installation operable walls, glass wa | Hufcor Pty Ltd | Current | N/A | (blank) |
| Concreting | Kerbing, concrete, paving | KRF Kerbing | Current | N/A | 5229 |

| | | | | | |
|---|---|---|---|---|---|
| **Excavation/Trenching** | **Earthmoving works** | Heenan Earthmoving | Current | **N/A** | 708 |
| | **Earthworks, backhoes with rock breaker and auger attached** | Budget Backhoes & Earthworks | Current | **N/A** | 4981 |
| | **Excavation** | MTG Excavations Pty Ltd | Current | **N/A** | 301 |
| **Fencing** | **Fencing** | Do It Yourself Fencing | Current | **N/A** | 557 |
| | **Rural fencing, new and repairs. Post hole digging and driving** | Shane Glynn Fencing | Current | **N/A** | 3742 |
| | **Supply of Tubular Fencing** | Bluedog Fences Australia | Current | **N/A** | 5587 |
| **General Building** | **Engineering design and manufacture of structural steel, handrails, balustrade and other steel and metalwork** | DMK Engineering Pty Ltd | Current | **N/A** | 2633 |
| | **General Building** | EC & C Nieto Homebuilders | Expired | **N/A** | 5158 |
| | **Installation of folding wall/door systems and maintenance** | Lotus Folding Walls & Doors | Current | **N/A** | 5644 |
| | **Installation & services of all brand roller doors, gates etc. All steel/cladding work** | Thomson Bilt | Current | **N/A** | 4632 |
| | **Steel frame manufacturing and erection** | Parham Construction Pty Ltd | Current | **N/A** | 5088 |
| | **Carpentry** | Ben Jones Carpentry & Construction | Expired | **N/A** | 5926 |
| | **General engineering services, Inspector of Pressure Equipment, vessels and air receivers (internal and external)** | Dalkar Engineering | Expired | **N/A** | 1040 |
| | **Plumbing / Roofing / Fire Protection / Sheetmetal** | Metal Worx Pty Ltd | Current | **N/A** | 1607 |
| | **Builder - concrete, paving, stone and brickwork** | Merchys Building & Construction | Current | **N/A** | 3997 |
| | **Solid Plastering, Plasterboard Fixing, Flushing, Rendering, Cornice Quoin Work, Salt Damp Repairs** | Gilbert Plastering | Current | **N/A** | 5403 |
| | **Building and Building Repair Work** | Steplen Construction Pty Ltd | Current | **N/A** | 901 |
| | **Play Equipment, Shade Structures, Outdoor Fitness, Surfacing, Outdoor Furniture and Shelters, Play Auditing and Maintenance** | Forpark Australia SA/NT | Current | **N/A** | 3687 |
| | **General Engineering Services** | Krueger Engineering Pty Ltd | Current | **N/A** | 3704 |
| | **General engineering and sheetmetal work** | Andrew Bruhn Sheetmetal Pty Ltd | Current | **N/A** | 29 |
| | **Aluminium/stainless steel welding, sheet metal work, custom fabrication for cars/trucks** | BKM Custom Fabrication Pty Ltd | Current | **N/A** | 4131 |
| | **Commercial, Industrial & Domestic, Concreting, Concrete Pump Hire** | JNL Construction Pty Ltd | Current | **N/A** | 5026 |
| | **General Engineering** | JA & BM McKee Engineering | Expired | **N/A** | 2270 |
| | **Fibreglass Repairs** | Starky's Fibreglass Repairs | Current | **N/A** | 5918 |
| | **Brick layer, contractor, tiler, stonemason** | Keven A Lynch | Current | **N/A** | 2281 |
| **General Electrician** | **Electrical** | Mustart Electrical | Current | **N/A** | 5521 |
| | | Kameron Lamb Electrical Pty Ltd | Current | **N/A** | 5219 |

| | | | | | |
|---|---|---|---|---|---|
| | | Klaassens Contractors | Current | **N/A** | 3234 |
| | | RW & DD Gabriel Electrical Contractors Pty Ltd | Current | **N/A** | 1050 |
| | **Electrical contractors including communicatios, solar etc.** | Laser Electrical Mount Gambier | Current | **N/A** | 5407 |
| | **Electrical contractors** | Stuckey Electrical Contractors | Current | **N/A** | 289 |
| | **Building services, electrical install and maintenance** | Godrik Construction Pty Ltd T/as Friswell Electrical sA | Current | **N/A** | 5390 |
| | **Electrical Work** | BKT Contracting | Current | **N/A** | 5841 |
| **Landscaping** | **Irrigation Designer and Installer** | JB Irrigation | Current | **N/A** | 3860 |
| | **Native plant nursery and planting service** | Mimosa Farm Trees | Current | **N/A** | 74 |
| | **Turf Supplier** | Blue Lake Turf Supplies | Current | **N/A** | 3660 |
| | **Landscaping & Garden Maintenance** | The Complete Home Care Company | Current | **N/A** | 2840 |
| | **Gardening** | Bedford Phoenix Inc | Current | **N/A** | 3767 |
| | **Mechanical vegetation mulching** | Clearpath Vegetation Solutions | Current | **N/A** | 5925 |
| **Line Marking** | **Road/Line Marking and associated works** | Action Line Marking (SA) Pty Ltd | Current | **N/A** | 4984 |
| **Minor Civil Works** | **Civil earthworks** | W F C Contracting Co | Current | **B** | 270 |
| | **Civil Contractors** | GT Bobcat Pty Ltd | Current | **B** | 179 |
| | **All civil construction works and management** | Gambier Earth Movers Pty Ltd | Current | **B** | 10 |
| | **Civil Construction - Grader, Bobcat, Truck & Trailer, Excavator** | PJS Earthmoving Pty Ltd | Current | **N/A** | 5697 |
| | **Civil Construction** | Walker and Gray Earthworks Pty Ltd | Current | **N/A** | 198 |
| | **Concrete, Bitumen, Sawing & Drilling** | Clean Cut Industrial Services | Current | **N/A** | 553 |
| | **Civil and Landscaping** | Think Civil Pty Ltd | Current | **N/A** | 6154 |
| **Mowing/Slashing** | **Grounds Maintenance** | I & D Contracting | Current | **N/A** | 5766 |
| **Other** | **Catering** | Finns Fine Food | Expired | **N/A** | 3145 |
| | **Photography** | Frank Monger Photography | Current | **N/A** | 175 |
| | | Tanya Ewen Photographer | Expired | **N/A** | 5416 |
| | | Kinship Productions | Expired | **N/A** | 5143 |
| | **Radio Communications** | Gambier Electronics Pty Ltd | Current | **N/A** | 247 |
| | **Specialist audiovisual consultation services, arts and cultural project management** | Illuminart Productions Pty Ltd | Expired | **N/A** | 5298 |
| **Other** | **Supply and Installation of Floorcoverings** | Somerfields Carpets | Current | **N/A** | 778 |

| | | | | | |
|---|---|---|---|---|---|
| | **Surveying services** | Alexander & Symonds Pty Ltd | Current | **N/A** | 22 |
| | **Traffic Management** | Altus Traffic Management | Current | **N/A** | 3426 |
| | **Video Production** | Media Depot | Current | **N/A** | 5897 |
| | **Video/survey/photos/drone/UAV/GIS/sc an** | LC Aerial Pty Ltd | Current | **N/A** | 4998 |
| | **Supply of Lubricants** | Mogas Regional Pty Ltd | Current | **N/A** | 3490 |
| | **Various services and assistance** | Independent Learning Centre | Current | **N/A** | 5343 |
| | **Vehicle accident and recovery services** | Independent Towing | Current | **N/A** | 340 |
| | **Environmental biological management (revegetation/rehabilitation/ecological)** | ABOC Sustainable Systems | Current | **N/A** | 4064 |
| | **Architectural services, building design, construction supervision, master planning** | Brett Julian Architect | Current | **N/A** | 5391 |
| | **Audio visual, stage lighting, PA systems** | Total Electronic Contracting Pty Ltd | Current | **N/A** | 4240 |
| | **On-ground environmental works** | Conservation Volunteers Australia | Expired | **N/A** | 1413 |
| | **Service/maintenance of air compressors** | Blue Lake Air Compressors | Current | **N/A** | 5471 |
| | **Indoor Plant Hire and Maintenance** | Bolwarra Evergreen | Current | **N/A** | 2334 |
| | **Irrigation Sales and Service** | Watersolve Irrigation | Current | **N/A** | 5688 |
| | **Washroom Hygiene** | Fresh and Clean | Current | **N/A** | 3239 |
| | **Public Immunisation Services for Children and Adults** | South East Regional Community Health Service | Current | **N/A** | 798 |
| | **Repair and maintenance of swimming pool wood boiler** | MW Heating Limited | Current | **N/A** | 5241 |
| | **Water Bores, Clean Out Bores, Drainage Bores, Pump Repairs and Installation** | Sims Drilling | Current | **N/A** | 263 |
| | **Drain cleaning, hydro excavation, confined space entry, surface cleaning and CCTV services** | RSP Environmental Services | Current | **N/A** | 5413 |
| | **Service, sales, repairs, calibrations and installations for a wide range of weighing equipment** | SE Weighing Services Pty Ltd | Current | **N/A** | 1970 |
| | **Photocopiers - Sales and Service** | Pine Ridge Copiers | Current | **N/A** | 2859 |
| | **PA Hire** | Steve Mullan Sound and Lighting | Expired | **N/A** | 2038 |
| | **Business Office Equipment Sales and Service** | Green Triangle Electronics | Current | **N/A** | 211 |
| | **Stationery/Printing** | Exchange Printers | Current | **N/A** | 161 |
| | **Irrigation/Drilling/Pump Repairs & Sales** | Peter Jennings Pumps Pty Ltd | Current | **N/A** | 354 |
| | **Upholstery** | MacKenzie Upholstery | Current | **N/A** | 2599 |
| | **Weighbridge software and hardware** | ACCU Weigh Pty Ltd | Current | **N/A** | 5721 |
| | **Sales and service of compressed air equipment** | KPA Industrial | Current | **N/A** | 732 |

| | | | | | |
|---|---|---|---|---|---|
| | **Computing technology support** | Pittard Enterprises Pty Ltd T/as TDRS | Current | **N/A** | 5775 |
| | **Servicing & testing of products/systems** | A Noble & Son Ltd | Current | **N/A** | 887 |
| | **Residential, Commercial, Engineering & Indu** | Designs By Solly | Current | **N/A** | 5783 |
| | **Building Design** | Cooper Building Design | Current | **N/A** | 5782 |
| | **Sales, Service, Repairs, Installation of Comm** | EspressoWorx & Electrical Servic | Current | **N/A** | 3613 |
| | **Industrial Labour Hire** | Programmed Skilled Workforce Limited | Current | **N/A** | 5786 |
| | **Artist** | Psychotti Art | Current | **N/A** | 5801 |
| | | Art by EJ Zyla | Current | **N/A** | 5829 |
| | **Information, data and remote monitoring in Industrial and agricultural sectors** | Integrated Irrigation | Current | **N/A** | 5810 |
| | **Waste management, landfill design, groundwater monitoring, landfill gas monitoring, construction support, civil engineering, site contamination and remediation** | AECOM Australia Pty Ltd | Current | **N/A** | 5173 |
| | **Art Therapy and Mixed Media Art** | RinRinka Art Heart & Healing | Current | **N/A** | 4796 |
| | **Glitter tattoos for kids** | Lorraine Harris | Current | **N/A** | 5228 |
| | **Photo booth** | Pamalah Pty Ltd | Current | **N/A** | 5866 |
| | **Manufacture of themed areas** | ShowTrek Productions | Current | **N/A** | 3945 |
| | **Energy Monitoring** | Buddy Platform Limited | Expired | **N/A** | 5875 |
| | **Electric Motors** | SE Electric Motors | Current | **N/A** | 3168 |
| | **Art Installation** | Victoria University (Skunk Control) | Expired | **N/A** | 5950 |
| | **Graphic Design, print brokerage, branding, w** | Julia Reader | Current | **N/A** | 4926 |
| | **Electric overhead travelling crane repairs, se** | S & S Cranes (Aust) Pty Ltd | Current | **N/A** | 3061 |
| | **Sharps waste collections** | Veolia Environmental Services (A | Current | **N/A** | 4660 |
| | **GPS Tracking Systems** | IntelliTrac | Current | **N/A** | 6024 |
| | **Shade Structures & Sails, Waterproof Umbre** | Soulsby Sails Pty Ltd T/As Shadef | Current | **N/A** | 6054 |
| | **Photography, professional writing, social me** | Kate Hill | Current | **N/A** | 6037 |
| | **Hire Items** | SE Marquees Weddings & Events | Current | **N/A** | 5161 |
| **Painting** | **Painting and decorating** | Pridal Services Pty Ltd | Current | **N/A** | 5389 |
| | **Sign Writing** | Hyland Fox Signs | Current | **N/A** | 392 |
| | **Signage, stationery, promotional products and design** | The Sign Depot Mount Gambier Pty Ltd | Current | **N/A** | 5276 |
| | **Painter and Decorator** | Ray de Wit Painting Contractors Pty Ltd | Current | **N/A** | 3855 |
| | **Painting and Linemarking** | G Weyers Painting Service | Current | **N/A** | 2244 |

| | | | | | |
|---|---|---|---|---|---|
| | **Painting** | Wayne Elliott | Current | **N/A** | 2383 |
| **Pest Control** | **Pest control services** | All Bugs Pest Control | Current | **N/A** | 26 |
| | **Environmentally friendly pest control and inspection** | Spiderman SE Eco Pest Management | Current | **N/A** | 5415 |
| **Plant Hire** | **Plant & Machinery Dry/Wet Hire** | Civihire | Current | **N/A** | 5386 |
| | **Engineering, Crane Hire, Scissor Lift Hire** | Sims Engineering and Blue Lake Cranes | Current | **N/A** | 3389 |
| | **Crane Hire, Rigging, Transport & Float Hire** | Williams Crane Hire Pty Ltd | Current | **N/A** | 1740 |
| **Plumbing** | **Plumbing** | Maloney Plumbing Pty Ltd | Current | **N/A** | 3297 |
| | | Hirth Plumbing Solahart | Current | **N/A** | 274 |
| | **Plumbing - specialising in mains (cctv inspections)** | Raymond Koczak Plumbing Services Pty Ltd | Current | **N/A** | 769 |
| | **Plumbing** | A & K Geddes Plumbing | Current | **A** | 4209 |
| | **Plumbing, Gasfitting, Roofing** | Tye's Plumbing Service Pty Ltd | Current | **N/A** | 371 |
| | **Plumbing, Pool Repairs, Gas Works** | Pfeiler Plumb 'N' Gas | Current | **N/A** | 244 |
| | **Plumbing and Gasfitting** | Rathjen's Plumbing | Current | **N/A** | 2463 |
| **Professional Services** | **Health Consultancy** | Kirk Health Solutions | Current | **N/A** | 4885 |
| | **Legal Services** | Kelledy Jones Lawyers | Current | **N/A** | 4444 |
| | | Wallmans Lawyers | Current | **N/A** | 2996 |
| | | Norman Waterhouse Lawyers | Current | **N/A** | 257 |
| | | Mellor Olsson Lawyers | Current | **N/A** | 442 |
| | **Surveying** | Cameron Lock Surveying | Current | **N/A** | 5184 |
| | **Town planning consulting services** | Frank Brennan Consulting Services | Current | **N/A** | 5582 |
| | **Engineering, road, airfield, rail and water network systems** | Downer Infrastructure | Current | **N/A** | 5399 |
| | **Training Services** | Maybo Australia | Current | **N/A** | 5059 |
| | **Heritage architect, urban design, architectural design and contract administration services** | Habitable Places | Current | **N/A** | 818 |
| | **Architectural design services** | Chapman Herbert Architects | Expired | **N/A** | 130 |
| | **Consulting** | KPPM Strategy | Current | **N/A** | 4937 |
| | | SGL Consulting Group (Australia) Pty Ltd | Current | **N/A** | 2679 |
| | | XLR8 Consulting | Current | **N/A** | 5996 |
| | **Specialist engineering consultancy** | Southfront | Current | **N/A** | 5376 |
| | **Recruitment, labour hire, training, WHS Consultancy, project management services** | Gramac Corporate Pty Ltd | Current | **N/A** | 3080 |

| | | | | | |
|---|---|---|---|---|---|
| | **Investment Attraction and International Engagement** | Rodry Consulting | Current | **N/A** | 5664 |
| | **Provision of Environmental Health Services** | Envirand Pty Ltd | Expired | **N/A** | 5663 |
| | **Engineering surveying** | Independent Surveying Pty Ltd | Current | **N/A** | 5406 |
| **Professional Services** | **Structural, civil and environmental engineering design and inspection** | Tonkin Consulting | Current | N/A | 2024 |
| | **Interpreting and Translating Services (Chinese/English)** | Furui Exchange | Current | N/A | 5696 |
| | **Architectural, Disability Access Training, Audits and Action Plans, Energy Audits, Solar/Wind Power Generation Design and Project Management** | EnvironArc Design Pty Ltd | Current | N/A | 5400 |
| | **Chartered Accountants** | Dean Newbery & Partners | Current | N/A | 4482 |
| | **IT Consulting Services** | Control Track Pty Ltd | Current | N/A | 5654 |
| | **Building Surveying Services** | Dave Vandborg Building Surveyor | Current | N/A | 5772 |
| | **Information Technology and Telecommunic** | Gumlea IT Solutions | Expired | N/A | 5954 |
| | **Management Consulting** | BRM Holdich | Current | N/A | 5226 |
| | **Mental Health First Aid Training** | Joan4Training | Current | N/A | 5982 |
| | **Building Design / Construction / Project Ma** | TIA Consulting Pty Ltd | Current | N/A | 5989 |
| | **Underground service detection** | Pine Lime Designs | Current | N/A | 5988 |
| | **Landscape Architectural / Urban Design Con** | JPE Design Studio Pty Ltd | Current | N/A | 6002 |
| | **Freelance Writing** | Gretel Sneath | Current | N/A | 2389 |
| | **Marketing and promotional consultancy** | ingWord | Expired | N/A | 5921 |
| | **Support to Environmental Health Officers** | Aquatics Information | Current | N/A | 4833 |
| | **Community Development Consultancy Servi** | Epic Proposals | Current | N/A | 6155 |
| **Road Construction** | **Crack Sealing of Roads** | SuperSealing | Current | N/A | 4327 |
| **Tree Trimming** | **Tree felling & tree works, excavator, bobcat works** | All Trees All Stumps | Current | B | 3232 |
| | **Vegetation services** | Tree Works Australia Pty Ltd | Current | N/A | 5419 |
| | **Slashing / Tree Trimming** | South East Mini Quip | Current | N/A | 640 |
| | **Arboricultural Consultancy** | Arborman Tree Solutions Pty Ltd | Current | A | 1326 |
| | **Qualified Arborists** | Treeworx South East | Current | N/A | 5753 |
| **Waste Management** | **Waste Disposal - Liquid** | Don Stewart Waste Disposal | Current | N/A | 1320 |
| | **Industrial vacuum, pressure cleaning, septic pump out** | Envirogen Industrial Services (Aust) Pty Ltd | Current | N/A | 4270 |
| **Weed Control** | **Lawn and Park Spraying** | SE Spraying & Wecare Lawn Spraying Services | Current | N/A | 4922 |

| | | | | | |
|---|---|---|---|---|---|
| **Welding** | **Plastic Welding** | Russells Repairs | Current | N/A | 5629 |
| | **Trailer manufacturing and repairs, welding etc.** | Diverse Transport Fabrications | Current | N/A | 5398 |
| | **Stainless steel, aluminium and mild steel we** | Dyson Fabrications Pty Ltd | Current | N/A | 6011 |

# Conflict of Interest Checklist

Use this series of questions to identify possible conflict of interest.

1. Am I, a relative of mine or a member of my household likely to be directly affected by this matter or decision in any of the following ways that may result in betterment or worsening of finances or assets:
   - Gain or loss in any way that can be measured in monetary terms;
   - Owning property directly affected;
   - Owning shares or holding a position in an entity that is likely to be directly affected;
   - Owed money by an entity that is likely to be directly affected;
   - Employed by an entity that is likely to be directly affected;
   - Received any gifts (monetary or otherwise) from an entity that is likely to be directly affected?
2. Am I, a relative of mine or a member of my household employed by an entity that is likely to be directly affected?
3. Have I, a relative of mine or a member of my household previously dealt with this matter in any other capacity?
4. Have I, a relative of mine or a member of my household been involved in any court or tribunal process in relation to the matter?

## 5.2 2018/2019 BDO AND AUSCERT CYBER SECURITY SURVEY - REPORT NO. AR19/21468

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/21468** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Pamela Lee, General Manager Council Business Services** |
| **Authoriser:** | **Graeme Maxwell, Chief Executive Officer** |
| **Summary:** | **The 2018/2019 BDO and AusCERT Cyber Security Survey is provided for information and awareness of cyber security. This report also provides an update on Council's measures to manage the risk associated with cyber security.** |
| **Community Plan Reference:** | **Goal 1: Our People**<br>**Goal 3: Our Diverse Economy** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/21468 titled '2018/2019 BDO and AusCERT Cyber Security Survey' as presented on 15 May 2019 be noted.

## BACKGROUND

Cyber risk is a relevant and present risk aligned to the adoption of and development in technology. For this reason, the need for organisations including councils, to be able to detect, respond and recover from a cyber incident are more important than ever before. The cyber landscape is continually changing.

The accounting and advisory firm DBO recently issued its 2018/2029 BDO and AusCERT Cyber Security Survey, the results support that one of the biggest hurdles is being overcome with a genuine uplift in leadership awareness of cyber security and improved reporting to decision makers.

Cybercrime is a criminal activity carried out using a computer over the internet and/or technology enabled environment (e.g. a closed / restricted technology environment e.g. extranet, intranet).

*"Cybercrime comes in many forms with the most common types being identify and information theft, fraud, scams and attempting to access information on a computer or internet enabled device. As individuals and organisations, including governments transact more online, cybercrime has become more prevalent. It is important to be aware of the common types of fraud and scams to ensure the benefits of digital technology and online transacting while staying safe online."* Source: Commonwealth Bank of Australia's Phillippa Watson, Executive General Manager, Direct Channels.

The Survey notes the impacts of cyber-attacks are shifting. While organisations are reporting less business disruption, the potential for reputation damage is on the increase. Regulatory changes have brought cyber resilience into the public eye more. Intangible risks are challenging to recover from and impossible to insure against.

Being able to detect a cyber-attack or incident is an initial step, however it is only beneficial if a response is swift and targeted. An increased focus on awareness and reducing the impact of a cyber incident is needed.

## DISCUSSION

South Australian councils were offered the opportunity through the Local Government Risk Service's (LGRS) Cyber Risk Program to apply for grant funding to undertake a cyber security assessment through an LGRS appointed third Party, CQR. Council was successful in late 2018 with its grant applications for the LGRS grant funding. CQR is currently undertaking a cyber and data security assessment involving:

- Base line security questionnaire
- Router / firewall configuration review
- Windows server configuration review
- External penetration testing
- Report.

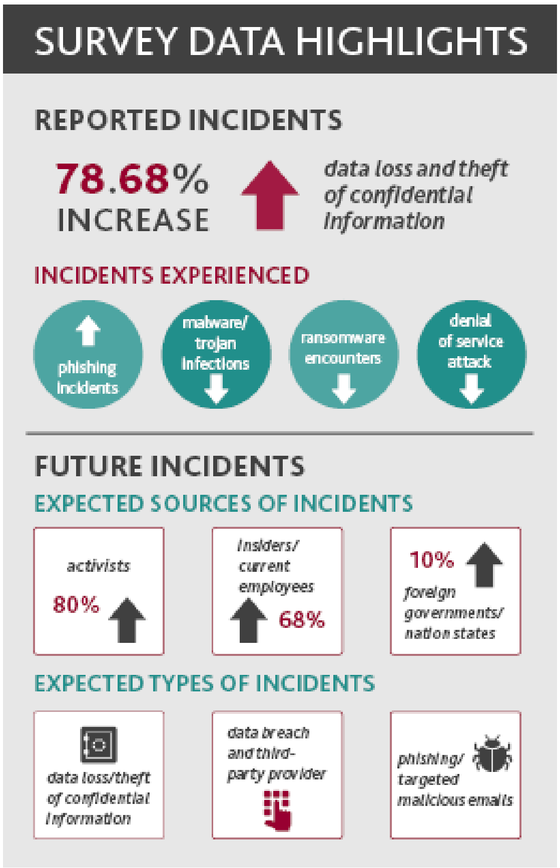
A report will be provided to the Audit Committee following the report being received and an action plan developed to address any findings and recommendations.

Council works closely with its service providers (managed services environment, local technology support serve and telecommunications providers) to identify and mitigate risks to our information and technology environments.

To provide background information regarding cyber security and cybercrime a copy of the 2018/2019 BDO and AusCERT Cyber Security Survey is attached to this report. Close to 500 organisations across Australia and New Zealand from a variety of sectors responded to the BDO and AusCERT Cyber Security Survey. Of the respondents, 74.4% were based in Australia, 20% in New Zealand and 5.6% were based internationally. Respondents included CEOs and directors (40%) and IT/security managers, analysts and engineers (59%) and internal auditors (1%) from organisations that ranged in size from less than $500,000 annual revenue through to more than $1 billion. Key highlights from the survey report include:

- Increased cyber awareness across respondent organisations, with management getting more involved
- Enhanced cyber maturity and improved security posture, likely as a result of compliance with regulatory changes
- More work is needed to manage the impact of incidents, particularly developing breach response plans and adopting cyber insurance.

The following infographic provides survey data highlights.



SURVEY DATA HIGHLIGHTS

REPORTED INCIDENTS

78.68% INCREASE ↑ data loss and theft of confidential information

INCIDENTS EXPERIENCED

↑ phishing incidents

malware/ trojan infections ↓

ransomware encounters ↓

denial of service attack ↓

FUTURE INCIDENTS

EXPECTED SOURCES OF INCIDENTS

activists 80% ↑

insiders/ current employees ↑ 68%

10% ↑ foreign governments/ nation states

EXPECTED TYPES OF INCIDENTS

data loss/theft of confidential information

data breach and third-party provider

phishing/ targeted malicious emails

**Summary observations from the survey**

- **Key Leadership is increasingly aware of cyber risk**

  Survey respondents demonstrated a clear increase in cyber security awareness in 2018. This shift in attitude has come directly from the top, indicating that there is a true increase in leadership awareness of cyber security and improved reporting to these senior levels.

  Where the Board/Council Elected Members and Executive Leadership Team have greater oversight and understanding of their organisation's cyber security risks, greater support and implementation of proactive cyber security controls is reported.

- **Increasing data breaches or just mandatory reporting?**

  Data loss/theft of confidential information incidents rose by 78.7% in 2018 compared to 2017. This significant increase could be related to the implementation of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB) in Australia in early 2018. The Act's requirements for mandatory reporting has seen investment in preparedness measures across many respondent organisations.

Despite this, the survey highlighted that organisations are not focusing enough on response or incident management procedures. These components, along with cyber insurance, should form part of a comprehensive cyber security resilience program, as they allow organisations to more effectively minimise the impact of breaches, while ensuring a rapid investigation into the cause and effect.

The Privacy Amendment (Notifiable Data Breaches (NDB)) Act 2017 (Cth) amends the Commonwealth Privacy Act 1988 (Cth) (Privacy Act) to introduce mandatory 'eligible data breach' notification provisions for entities regulated by the Privacy Act. The NDB applied from 22 February 2018 to all agencies and organisations with existing personal information security obligations under the Privacy Act. It was established by the passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017.

There is no information privacy law in South Australia that covers State Government, Local Government or South Australian Universities. South Australia State Government agencies are required to comply with the Information Privacy Principles Instruction (IPPI). Local Government authorities and South Australian Universities are not covered by either the Commonwealth Privacy Act or the IPPI.

Council's:

- Privacy Policy (P155) states Council's position in regard to the protection of individuals' privacy
- Records Management Policy (R155) states Council's framework for Council to effectively fulfil its obligations and statutory requirements under the State Records Act 1997.

All Council policies are available on its website. Induction training covers the obligations under these policies for Elected Members and staff. Reminders and refresher training is also provided to staff on the obligations under the policies.

- **Hacktivist attacks expected to be nearly twice as common in 2019**

When asked about the types of attackers that would be most prevalent in 2019, respondents indicated that activists/hacktivists would be nearly twice as likely to be sources of cyber security incidents as the previous year.

Organisations could be underestimating the prevalence of cyber security criminals and insiders, and overestimating the frequency of attacks launched by other sources. This could be symptomatic of a limited understanding of the relevant cyber security threat risk landscape.

- **The continued rise of phishing**

Phishing is a cybercrime in which a target or targets are compromised by clicking on hyperlinks in an email or text message. These links take the user to a fake internet site, purporting to be legitimate site, where they are lured into entering sensitive data such as personal information, banking credentials, credit card details and passwords.

Trend data from the BDO – AusCERT Cyber Security Survey results since 2016 outlines a consistent rise in phishing incidents. In fact, it remains the most common incident experienced. Adversaries continue to target the human psyche, our inquisitiveness and general position of trust. Humans are continuing to prove to be a weak link in the layers of defence.

Organisations are slowly implementing phishing awareness training across their workforce, but educating all employees about the dangers of phishing is a slow process. While education continues to improve, we expect phishing to remain the most popular attack vector.

Council's managed services provider has implemented software to detect and mitigate the incidence of phishing. Council's iServices team also provide information to raise staff awareness of the need to be vigilant when messages/links from unknown sources arrive in either email or text form on Council electronic devices (PCs, mobile phones).

## CONCLUSION

The effects of cybercrime are universal and impact individuals and organisations financially, emotionally and their reputation. Council takes precautions and has controls in place to protect and mitigate against the risk of cybercrime.

Council and its systems and technology managed services provider(s) assess the threat to Council and Council's data, information and systems and take measures to mitigate and manage security threats on an ongoing basis. Some of the measures include:

- Protecting passwords including mandatory changing of passwords and password complexity testing
- Protecting social media and email accounts
- Using anti-virus software and regularly updating the version and/or product
- Using password protected environments including Extranet (Elected Members), Intranet (staff), social media including 'Have Your Say'.

Council's success in securing an Local Government Risk Services (LGRS) Cyber Security Program grant in late 2018 has facilitated a cyber security assessment by an LGRS appointed service provider to review and test Council's systems and communications (including website and social media platforms) vulnerability. The report from this review is due by the end of June 2019.

## ATTACHMENTS

1. 2018/2019 BDO and AusCERT Cyber Security Survey ⇩

BDO

# 2018/2019 CYBER SECURITY SURVEY

AUSCERT

# FOREWORD

The cyber landscape is continually changing. New actors are entering the mix, the types of attack methods being used are evolving, regulatory obligations are shifting and organisations are looking at cyber security differently. The 2018/2019 BDO and AusCERT Cyber Security Survey Report highlights this more than any of our previous reports, as we draw upon three consecutive years of in-depth data to provide an insight to the cyber landscape in Australia and New Zealand.

This year the data paints a picture of an industry that is focused on prevention and compliance to regulatory changes, most notably the (Notifiable Data Breaches) Act 2017 (NDB) in Australia or the General Data Protection Regulation (GDPR). These changes have been a valuable mechanism to uplift cyber security maturity and instil a stronger focus on planning. With this has come higher spending on cyber security measures and a rise in confidence amongst respondents regarding their level of preparedness.

On the surface, all of these trends seem to position industry in a good place, but the reality is that more attention is needed on incident response. Even the best plans are of no help in the event of a cyber breach if they are not tested and continually reviewed and adjusted to remain relevant.

The continual rise of phishing, which is heavily reliant upon human interaction, only fuels this need for testing. A genuine business continuity risk exists for many Australian and New Zealand businesses and the key to overcoming it is education and testing of the learning process.

Interestingly, the report findings also pinpoint a significant increase in suspected attacks from foreign governments/ nation states, and a view by many respondents that hacktivist attacks will increase in the future.

These trends are reflective of what our global BDO Cyber Security team is witnessing worldwide. Our Cyber Threat Insights Report for the fourth quarter of 2018 highlighted a blurring of nation-state cyberattack groups with criminal cyberattack groups from their respective countries and other nations worldwide.

What is of particular note is that the impacts of cyber attacks are also shifting. While organisations are reporting less business disruption, the potential for reputation damage is on the rise. Regulatory changes have brought cyber resilience into the public eye and rarely a month goes by without the media reporting on a cyber breach and the impact it's had on an organisation's customers. Intangible risks like these are challenging to recover from and impossible to insure against.

This year's report delves into these topics and many more, providing you with a wealth of valuable benchmarking data and threat intelligence insights. By taking a proactive approach to learning more about the cyber landscape and how it could impact your business, you are taking a vital first step in instilling a culture of continual improvement and transparency about cyber security within your organisation.

Thank you to all the participants in this year's survey, and also to those who took part in our 2016 and 2017 surveys. Without your honest input and ongoing support, we couldn't ascertain the long term data trends that have shed light on many important issues in this year's report. We greatly appreciate the effort you put into supporting the survey and look forward to continuing the education journey with you into the future.

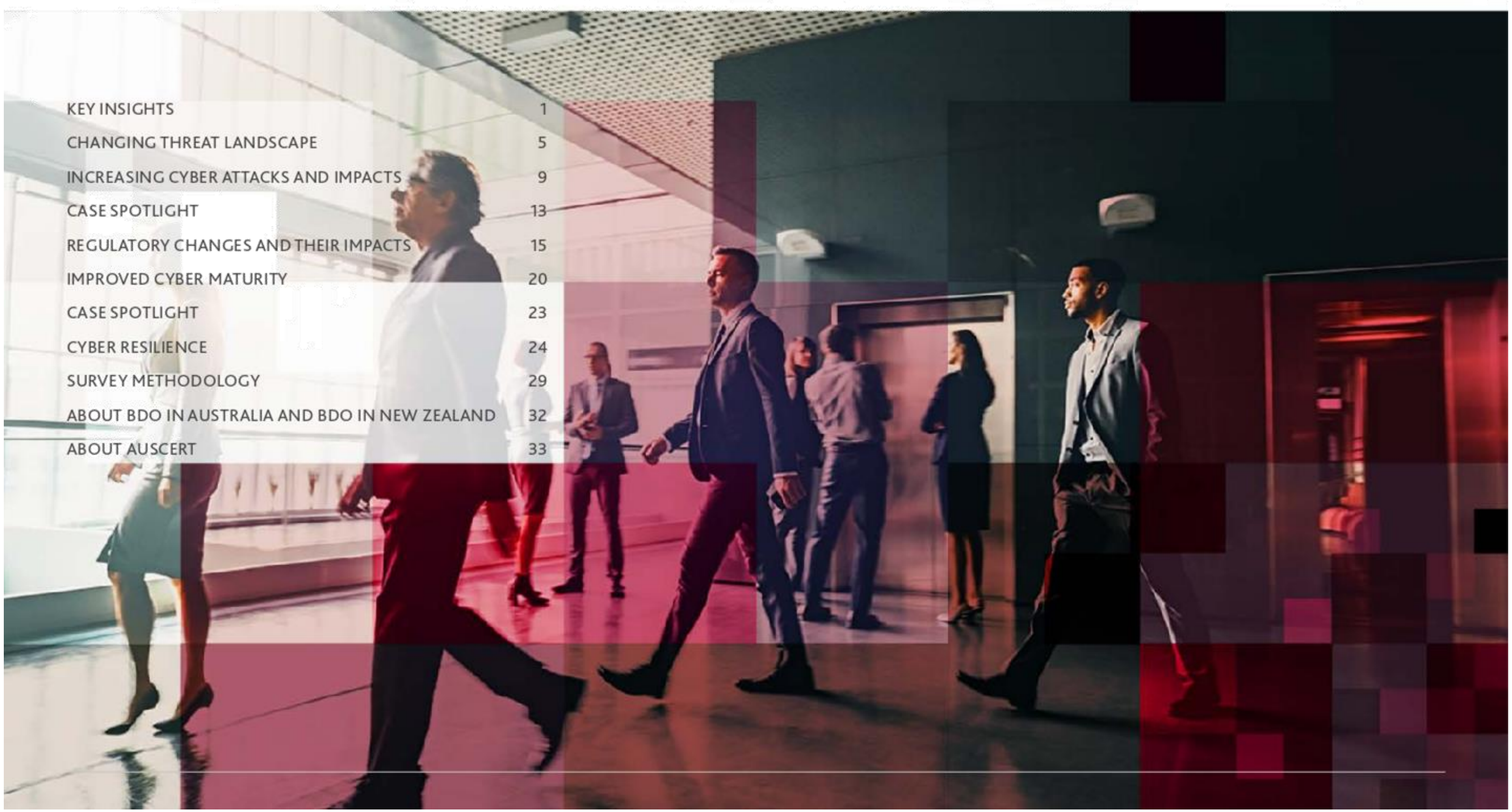
Leon Fouche
National Cyber Security Leader,
BDO

David Stockdale
Director,
AusCERT

Leon Fouche

D. P.

# CONTENTS



# KEY INSIGHTS

**At BDO, we strongly believe an organisation's approach to cyber security planning and management is set from the tone at the top. With this in mind, this year's results are music to our ears! A key theme running through the 2018 findings is that there has been a genuine uplift in leadership awareness of cyber security and improved reporting to these senior levels. It is action like this that allows organisations to strengthen their cyber security resilience.**

Many could argue this uplift in leadership engagement is simply the result of regulatory changes – the Notifiable Data Breaches Scheme and General Data Protection Regulation – and it would be hard to disagree entirely. What is clear though is that these changes are not the sole reason for Australian and New Zealand businesses taking a more proactive approach. High levels of respondent commitment to roll out activities such as cyber security awareness training and cyber security risk assessments demonstrates this.

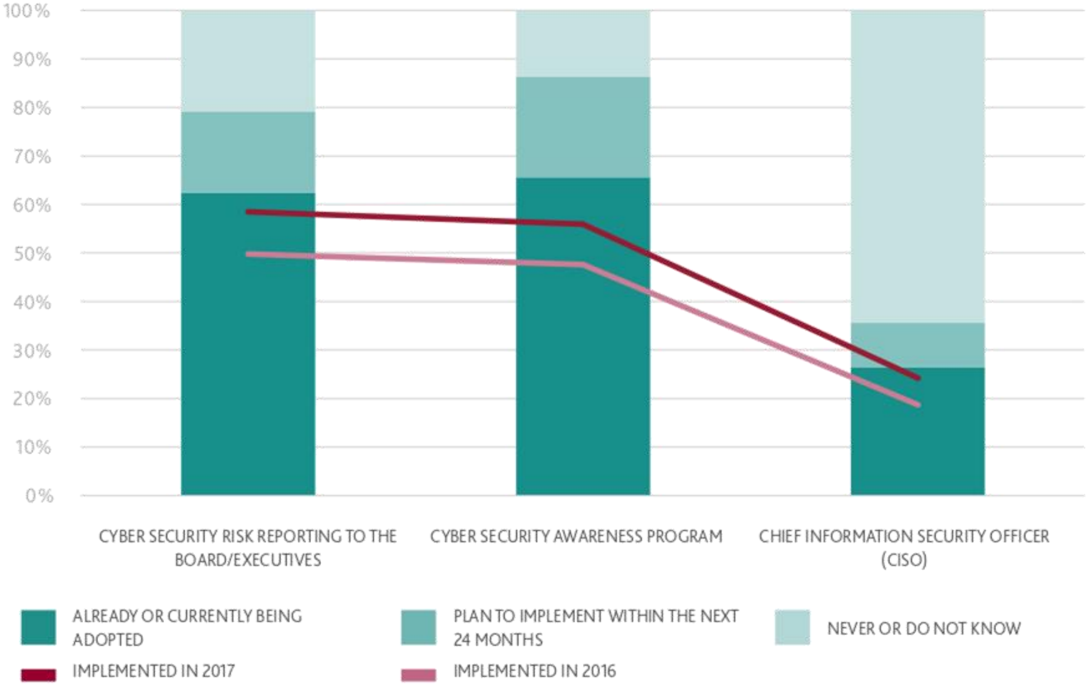
What is still missing though, is a stronger focus on reducing the impact of cyber incidents. The regulations and leadership support have clearly had a positive impact on helping respondents prevent a cyber attack, but many still appear vulnerable once an attack happens.

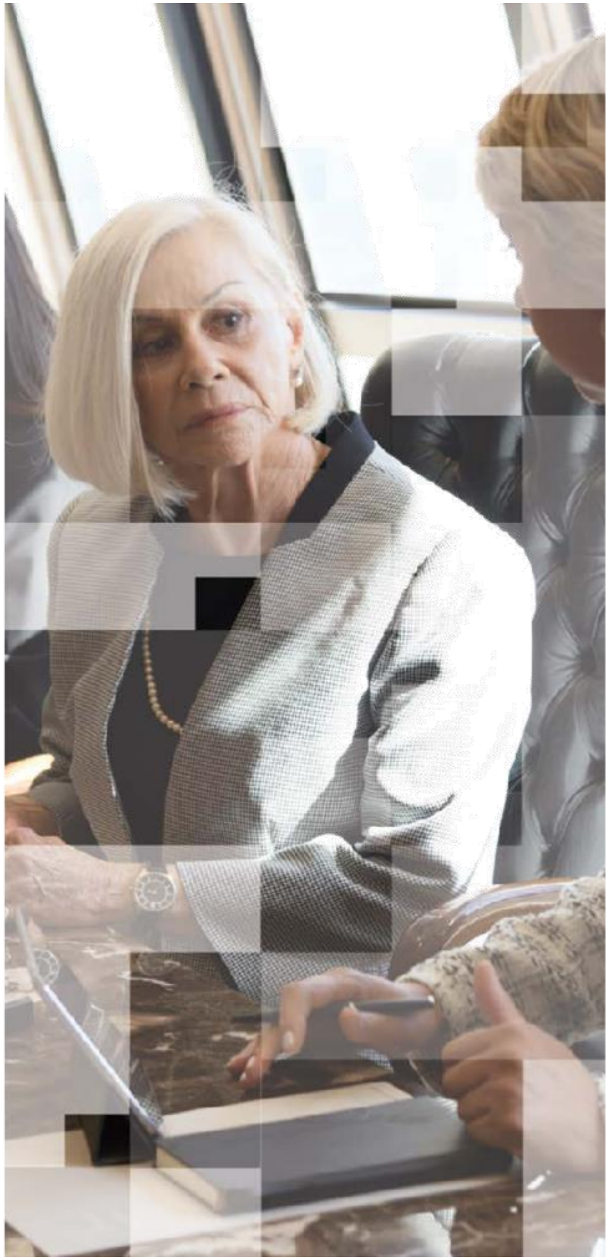
## LEADERSHIP IS INCREASINGLY AWARE OF CYBER RISK

In 2018, survey respondents demonstrated a clear increase in cyber security awareness. This shift in attitude has come directly from the top, with risk reporting to the Board and Executive Leadership Team (ELT) increasing. Where the Board and ELT have greater oversight and understanding of their organisation's cyber security risks, greater support and implementation of proactive cyber security controls is reported. These activities include cyber security training and awareness programs for staff within the organisation, establishing the requirement for cyber security risk assessments and standardising approaches to managing cyber security.

- **Increased cyber awareness across respondent organisations, with management getting more involved**
- **Enhanced cyber maturity and improved security posture, likely as a result of compliance with regulatory changes**
- **More work is needed to manage the impact of incidents, particularly developing breach response plans and adopting cyber insurance.**

CYBER RESILIENCE — LEADERSHIP AND TONE AT THE TOP





## CYBER RISK MANAGEMENT IS MATURING

Respondents have begun defining their risk management frameworks, but these exist in varying states of maturity. A BDO and Australian Institute of Company Directors study of Australian organisations in 2018 on Enterprise Risk Management[1] found that while the majority of organisations have partially defined risk thresholds and risk statements, only 6% have fully defined their risk posture.

In contrast, when we consider cyber security risk management, as opposed to the broader risk management definition, the data is more positive. This year's survey found that by 2020, 84.8% of respondents plan to implement regular cyber security risk assessments, while 86.4% of respondents expect to have a cyber security awareness program in place. This demonstrates that when the Board and ELT understand the risk landscape, they are willing to assign resources to address cyber security risk. We expect this sentiment to permeate further with respondents' risk management frameworks naturally being refined and maturing over time with a posture towards continual improvement.

## DATA PRIVACY REGULATIONS HAVE RAISED VISIBILITY OF CYBER RISK

A notable driver for change across industries in 2018 has been the implementation of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB) in Australia and the General Data Protection Regulation (GDPR) in Europe. With these new regulations, organisations face greater risk of significant financial (fines for non-compliance) and reputational damage associated with a data breach. These additional consequences, coupled with the immediate impact of data breaches, are leading to many respondents implementing preventative controls. This fact is reflected in the trend of increased IT security budgets for the third year running. In part due to this increase in budget, organisations appear more confident in setting and achieving their cyber security outcomes.

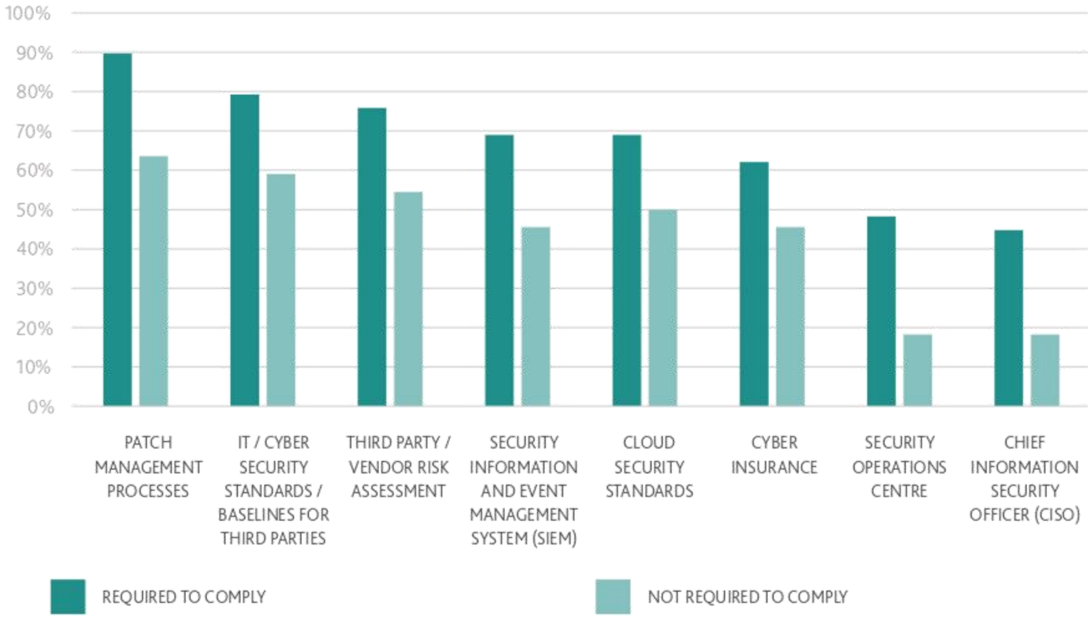
## TOO MUCH FOCUS ON PREVENTION, NOT ENOUGH ON RESPONSE

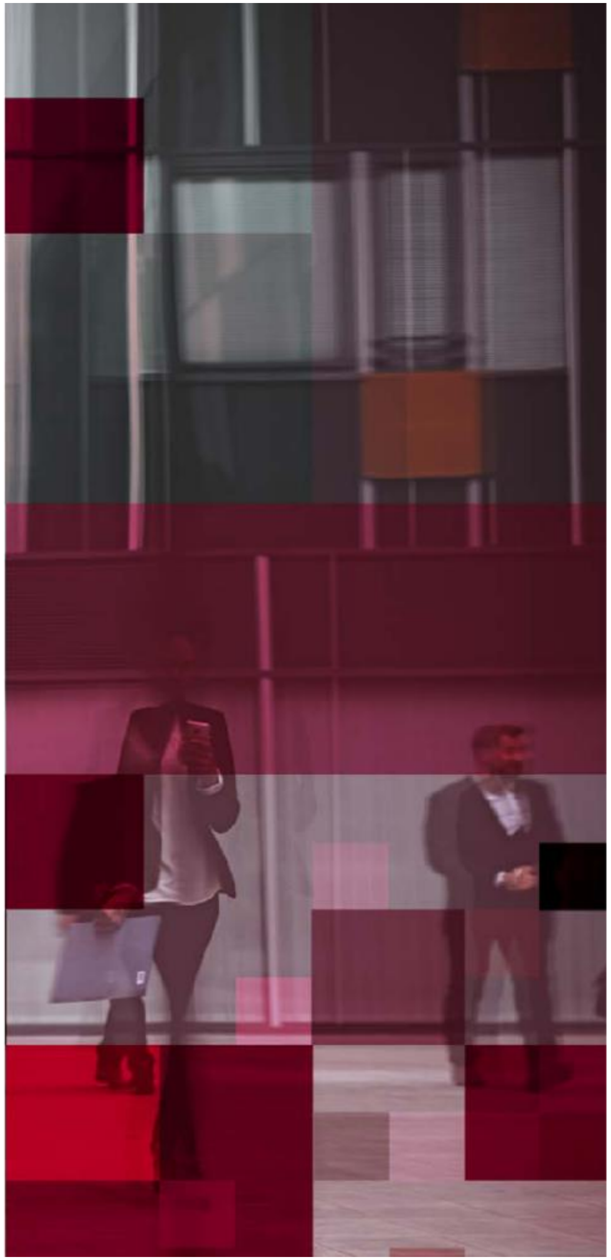
Even with this overall trend, further work is required to reduce the impact of cyber security incidents. In previous years, the BDO and AusCERT Cyber Security Survey has found that proper planning and preparation for cyber incidents resulted in greatly reduced impacts to the organisation following an incident. The importance of cyber resilience has been highlighted again in 2018.

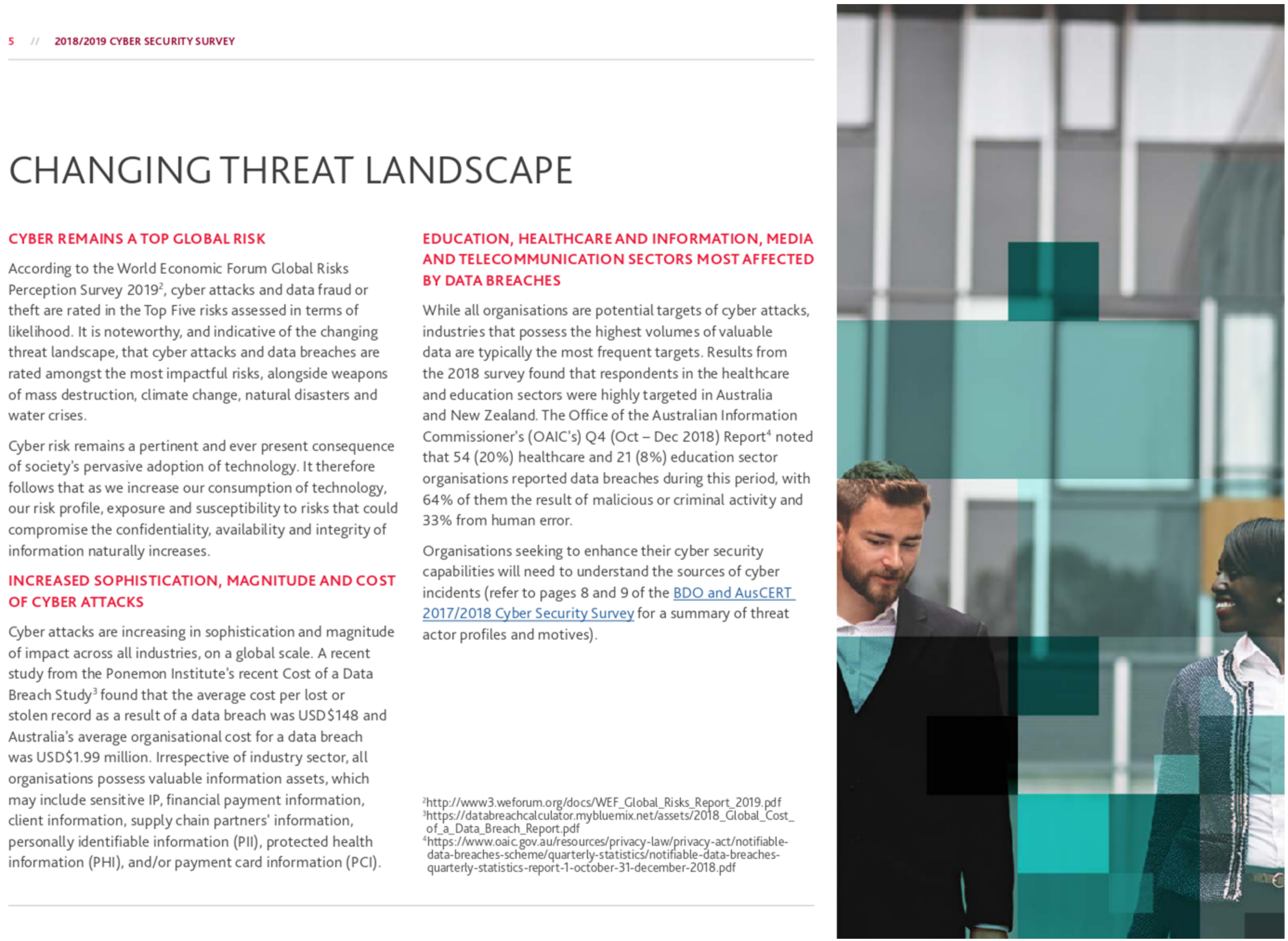
Where organisations are required to comply with NDB or GDPR, the adoption and maturity of security controls is significantly higher than those who are not required to comply. Despite this, the focus of this compliance is on preparedness, not response or incident management. We are hopeful that over the next 12 to 24 months, organisations will focus on implementing strategies to assist with reducing or lowering the impact of cyber security incidents, on the back of the work they've done to comply with the new regulations. Areas of focus should include the development of data breach response plans and the adoption of cyber insurance, as these controls can afford organisations the opportunity to minimise the impact of breaches, while ensuring rapid investigation can occur.

[1] https://aicd.companydirectors.com.au/advocacy/research/aicd-bdo-enterprise-risk-management-report-2018

HOW DATA BREACH COMPLIANCE REQUIREMENTS AFFECT ADOPTION OF SECURITY CONTROLS - 2018







# CHANGING THREAT LANDSCAPE

### CYBER REMAINS A TOP GLOBAL RISK

According to the World Economic Forum Global Risks Perception Survey 2019[2], cyber attacks and data fraud or theft are rated in the Top Five risks assessed in terms of likelihood. It is noteworthy, and indicative of the changing threat landscape, that cyber attacks and data breaches are rated amongst the most impactful risks, alongside weapons of mass destruction, climate change, natural disasters and water crises.

Cyber risk remains a pertinent and ever present consequence of society's pervasive adoption of technology. It therefore follows that as we increase our consumption of technology, our risk profile, exposure and susceptibility to risks that could compromise the confidentiality, availability and integrity of information naturally increases.

### INCREASED SOPHISTICATION, MAGNITUDE AND COST OF CYBER ATTACKS

Cyber attacks are increasing in sophistication and magnitude of impact across all industries, on a global scale. A recent study from the Ponemon Institute's recent Cost of a Data Breach Study[3] found that the average cost per lost or stolen record as a result of a data breach was USD$148 and Australia's average organisational cost for a data breach was USD$1.99 million. Irrespective of industry sector, all organisations possess valuable information assets, which may include sensitive IP, financial payment information, client information, supply chain partners' information, personally identifiable information (PII), protected health information (PHI), and/or payment card information (PCI).

### EDUCATION, HEALTHCARE AND INFORMATION, MEDIA AND TELECOMMUNICATION SECTORS MOST AFFECTED BY DATA BREACHES

While all organisations are potential targets of cyber attacks, industries that possess the highest volumes of valuable data are typically the most frequent targets. Results from the 2018 survey found that respondents in the healthcare and education sectors were highly targeted in Australia and New Zealand. The Office of the Australian Information Commissioner's (OAIC's) Q4 (Oct – Dec 2018) Report[4] noted that 54 (20%) healthcare and 21 (8%) education sector organisations reported data breaches during this period, with 64% of them the result of malicious or criminal activity and 33% from human error.

Organisations seeking to enhance their cyber security capabilities will need to understand the sources of cyber incidents (refer to pages 8 and 9 of the BDO and AusCERT 2017/2018 Cyber Security Survey for a summary of threat actor profiles and motives).

[2] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[3] https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
[4] https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-october-31-december-2018.pdf

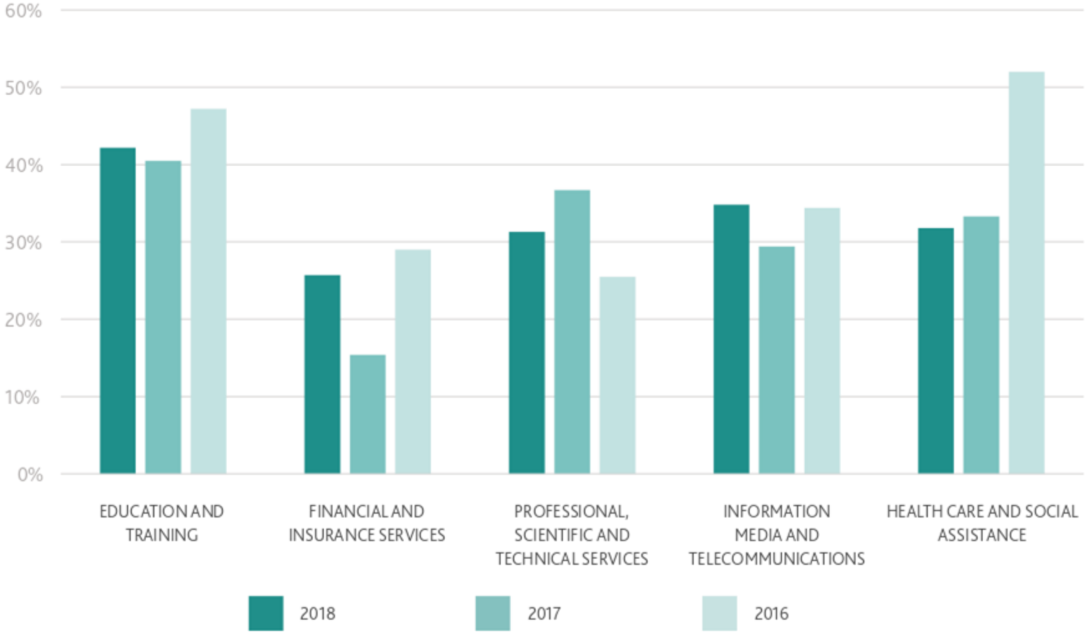
## CYBER CRIMINALS ARE THE MOST COMMON SOURCES OF CYBER ATTACKS

In 2018, respondent organisations overwhelmingly reported that cyber criminals were responsible for cyber attacks. Respondents also reported a significant increase in suspected attacks from foreign governments/nation states. Although there are clear differences in the motivations (and resources) between foreign government/nation state level groups and individuals or criminal groups, there is a degree of fluidity and commonality between the two classes of threat actor. In numerous cases, the same (or very similar) tools, techniques and procedures are used by different classes, perhaps because those are the best tools available. Consider the WannaCry malware link to North Korean state sponsored actors (see BDO 2017/2018 Cyber Threat Insights Report[5]).

## MANAGED SERVICE PROVIDERS ARE TARGETED FOR ACCESS TO THEIR CUSTOMERS' ENVIRONMENTS

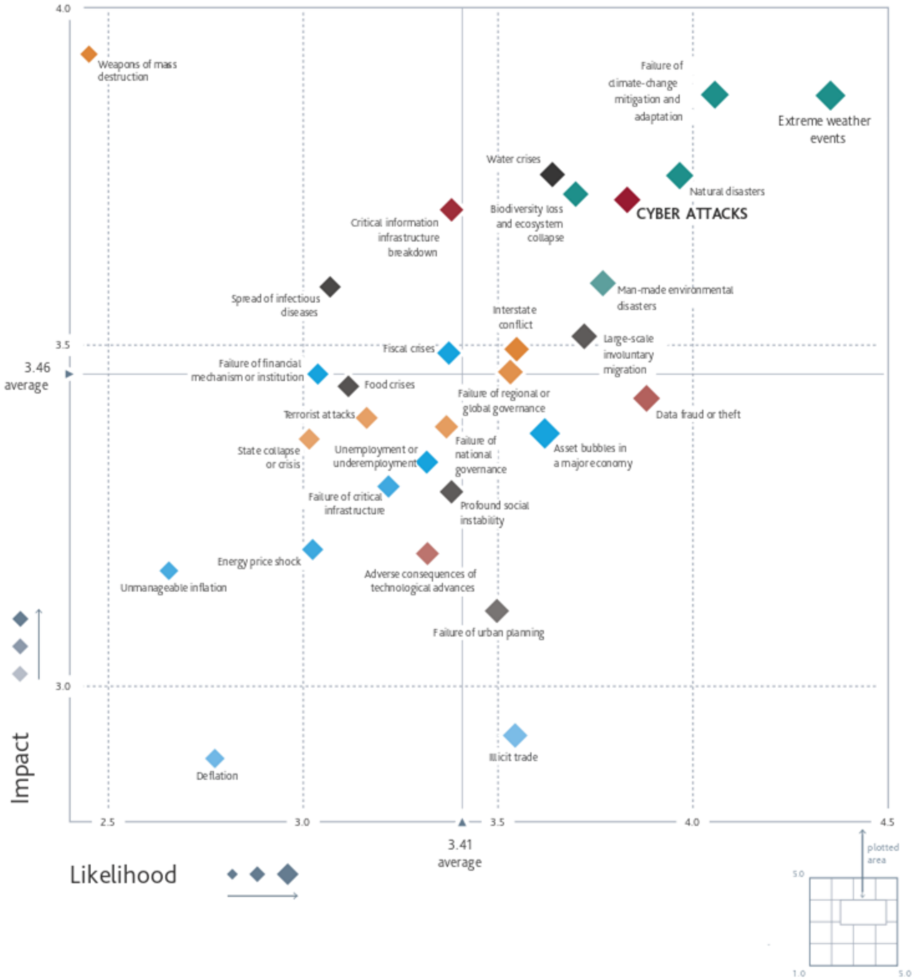
Managed Service Providers (MSPs) are engaged by organisations to manage their IT services and infrastructure. MSPs require remote access to their customers' systems to deliver these services, making MSPs attractive targets for state actors and cyber criminals. A notable example of this was the recently published campaign targeting MSPs worldwide, and which included Australian organisations, in a concerted effort to steal commercial secrets from the customers of MSPs for commercial advantage. It is important to note that the attributed threat actor's (APT10, also known as MenuPass, StonePanda or CloudHopper) activities in this campaign commenced as far back as 2014 and were comprehensively tracked and attributed in 2017 – however only recently had its impacts and the Australian Government's public response become well publicised.

### ORGANISATIONS THAT EXPERIENCED AN INCIDENT - 2016 TO 2018



[5] https://www.bdo.com.au/en-au/insights/cyber-security/publications/bdo-cyber-threat-insights-report-2017-2018

## THE GLOBAL RISKS LANDSCAPE 2019



Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Categories

◆ Economic

◆ Environmental

◆ Geopolitical

◆ Societal

◆ Technological

## HACKTIVIST ATTACKS EXPECTED TO BE NEARLY TWICE AS COMMON IN 2019

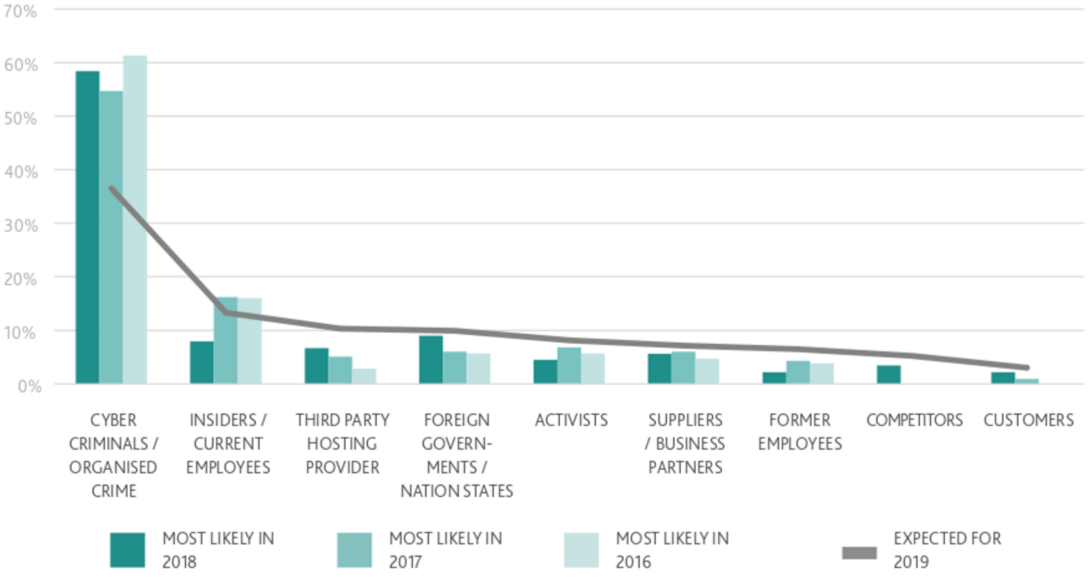
The adjacent graph shows the types of attackers respondents felt were most responsible for cyber attacks, compared to the attackers they expect to be most prevalent in 2019. Respondents perceive that cyber criminals will be perpetrating less attacks in 2019, but surprisingly they feel that activists/ hacktivists are going to be nearly twice as likely to be sources of cyber security incidents than the previous year.

Organisations may be underestimating the prevalence of cyber security criminals and insiders, and overestimating the frequency of attacks launched by other actors. This could be symptomatic of a limited understanding of the relevant cyber security threat risk landscape. In order to effectively defend against most likely cyber risks, organisations must have a clear understanding of who is targeting which assets, and how they are likely to do so.

## LIMITED PERCEPTION OF CYBER THREAT RISK LANDSCAPE

These findings indicate that respondents may be inaccurately assessing their relevant cyber security risk landscapes. When organisations perceive that different threat actors are targeting them compared to reality, security control investments are not commensurate with the real risk. This means organisations could be over or under protecting the wrong assets, from the wrong adversaries, in the wrong ways and for the wrong reasons. In general, this misinterpretation of the cyber threat landscape is likely symptomatic of limited comprehension of cyber risk more generally.

MOST LIKELY SOURCES OF INCIDENTS - 2018 vs 2019



# INCREASING CYBER ATTACKS AND IMPACTS

The 2018 survey data supports the common observation that adversaries are continually evolving their tactics and strategies. Cyber adversaries are rapidly evolving and adopting new tactics to better suit both their targets and the technology solutions they choose.

Data trends between 2017 and 2018 indicate that some exploits seem to be targeted for a period of time and possibly then become uneconomical for attackers to invest effort into as organisations' defence layers improve. The decline in ransomware and malware attacks from 2017 to 2018 demonstrates this. Conversely, some exploits have continued to grow year-on-year, such as phishing.

In 2018, the survey results have highlighted the following cyber attack trends:

- Phishing has consistently increased to become the most common incident experienced by survey respondents
- Adversaries are moving away from ransomware and malware exploits as there has been a significant fall in the number of attacks between 2017 and 2018. Looking at year-on-year, ransomware experienced a 44.27% drop in frequency. Ransomware, which involves unauthorised modification of information, can partially explain the more dramatic 70.90% drop in unauthorised modification of information incidents
- Data loss/theft of confidential information has risen rapidly since 2017. Respondents also reported an increase in the data breach via third party provider/supplier category
- Denial of service attacks have decreased from 2017
- In the 2018 survey we saw an increase in the number of attacks classified as 'None of the above', indicating that new incident types are occurring.

## THE CONTINUED RISE OF PHISHING

Our trend data from survey results since 2016 outlines a consistent rise in phishing incidents through to 2018. In fact, it remains the most common incident experienced. Adversaries continue to target the human psyche, our inquisitiveness and general position of trust. Humans are continuing to prove to be a weak link in the layers of defence.

We have seen many businesses slowly implementing phishing awareness training across their workforce, but educating all employees about the dangers of phishing is a slow process. While education continues to improve, we expect phishing to remain the most popular attack vector.

Phishing can also be considered a method through which other incidents can occur – for example, ransomware can be delivered through phishing, or credential compromise can be used to gain unauthorised access to information or perform Business Email Compromise (BEC) fraud.

Over the past 12 months, we have seen adversaries specifically target a number of industry sectors with BEC attacks. Organisations that manage the transfer of large sums of money have been specifically targeted, such as conveyancing firms.

## INCREASING DATA BREACH ATTACKS OR JUST MANDATORY REPORTING?

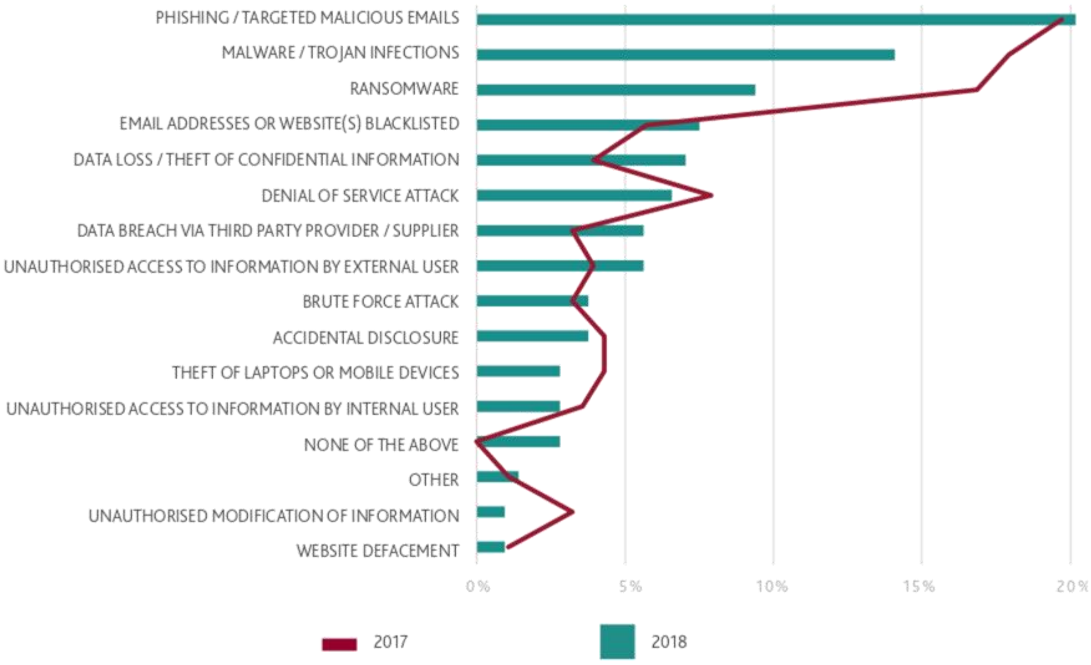
Data loss/theft of confidential information incidents rose by 78.68% in 2018 compared to 2017. Equally as alarming is the rise in data breaches experienced through third party providers and suppliers, which rose by 74.30%.

This increase in data may be related to implementation of the NDB Scheme by the Office of the Australian Information Commissioner in early 2018. The introduction of mandatory reporting could have contributed to respondents reporting a significant increase in these attacks between 2017 and 2018.

## LOOKING AHEAD...WHAT ARE RESPONDENTS EXPECTING?

When considering incident types experienced and future expectations, some interesting results came to the fore. Respondents are anticipating a significant increase in data loss/theft of confidential information in 2019, compared to what they actually experienced the prior year. Conversely, they expect to experience a sharp decrease in phishing incidents moving forward, yet this does not align with the trends we have observed over the past three years for this attack type. The expected reduction in malware and ransomware incidents in 2019 aligns with the trends presented in survey data.

INCIDENTS EXPERIENCED - 2017 vs 2018

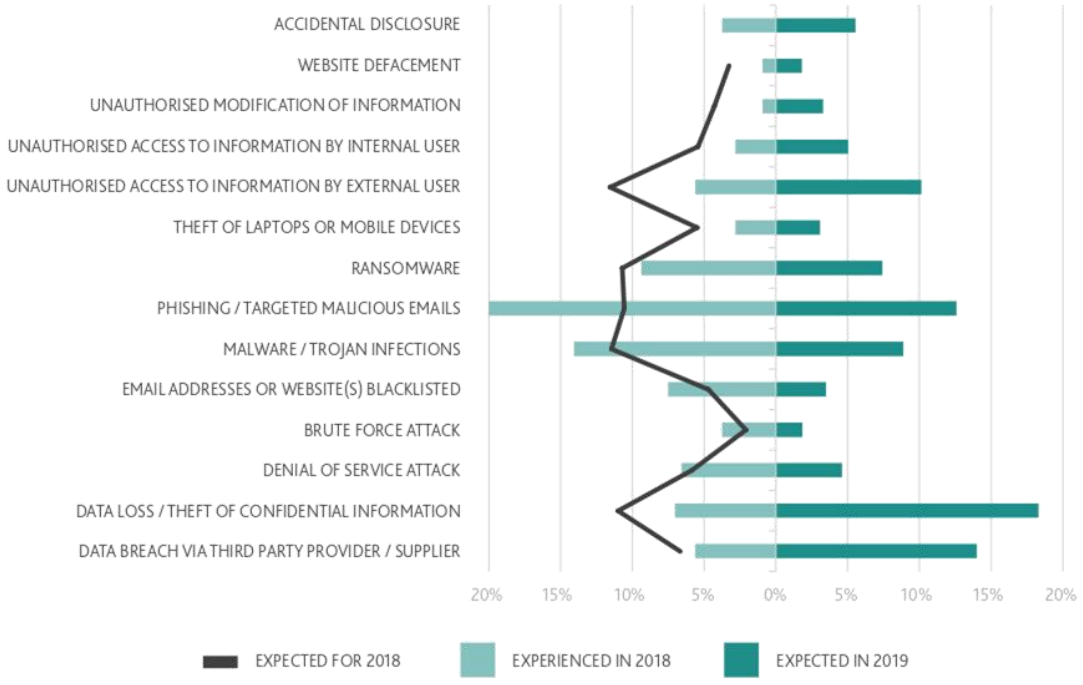


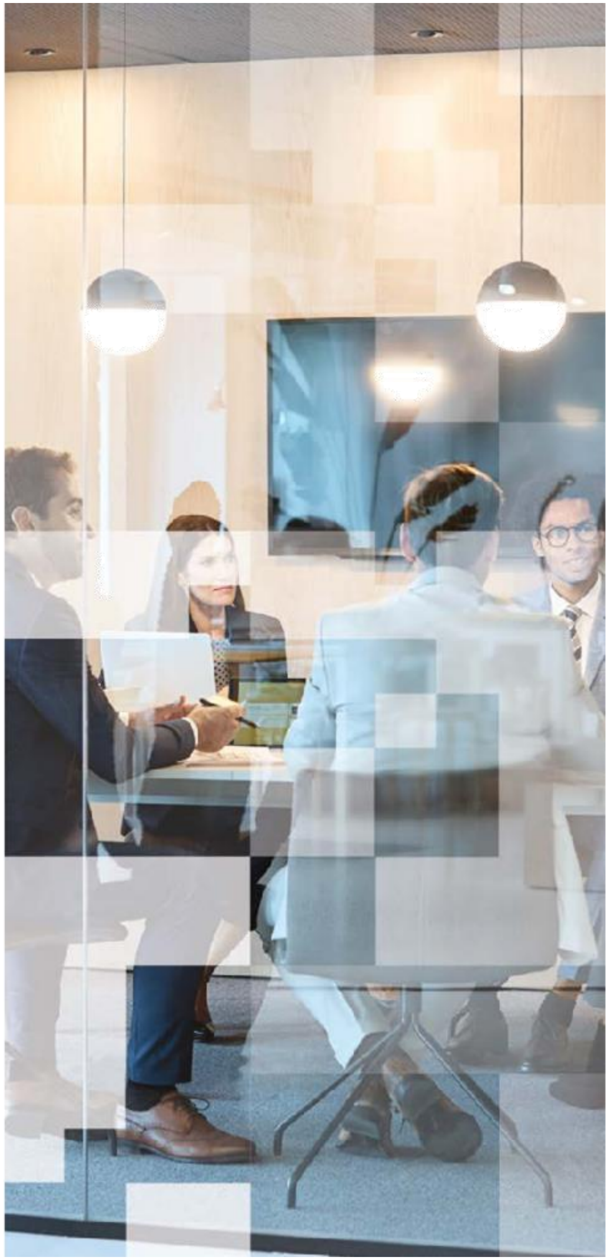
## INCREASE IN PHISHING ATTACKS AND APPLICABILITY OF INDICATORS OF COMPROMISE

AusCERT members have witnessed an increase in phishing, which is now more prominent than all other types of incidents. "Bullet proof" and lax processes within hosting providers are challenges for AusCERT and, as a result, AusCERT has invested in bespoke systems that integrate with its open source incident ticketing system, to facilitate tracking and faster recovery for its members suffering phishing attacks.

In AusCERT's established intel sharing groups (such as the CAUDIT ISAC for Australia and New Zealand higher education and research), the organisation targets its threat intelligence to suit members' utilisation patterns. This includes determining the type of threat indicators members are able to readily detect or prevent, such as email based indicators. For example, "email subject" is a readily detected and/or blocked indicator of compromise for most organisations, which has led to members utilising AusCERT's intelligence to configure their environments to increase their ability to prevent and/or detect phishing.

## INCIDENTS EXPERIENCED IN 2018 vs INCIDENTS EXPECTED IN 2019





## WHO EXPERIENCED AN INCIDENT

While the past three years of survey data show a downward trend in the number of respondent organisations experiencing a cyber incident, almost a third of all respondents in 2018 still experienced one. The reduction in the number of incidents may be due to greater defences and awareness being adopted by organisations, as the importance of cyber resilience has increased over the past two to three years.

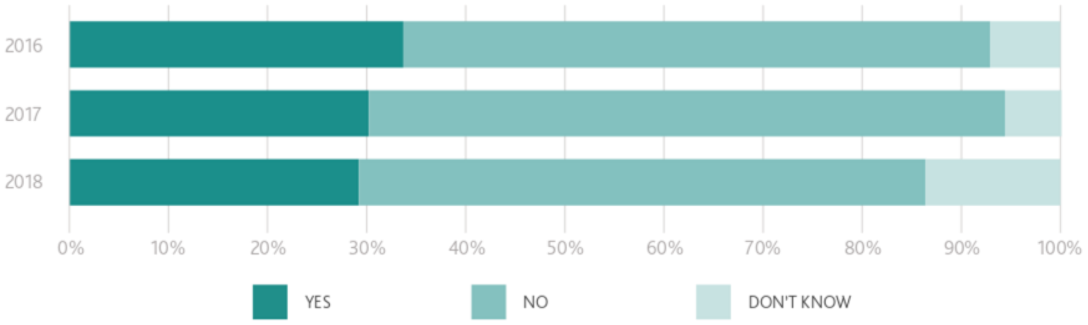
Interestingly, the 2018 survey saw a significant increase in the number of respondents who did not know whether an incident had occurred, an increase from 5.7% in 2017 to 13.6% in 2018. This change could be related to the decrease in the prevalence of ransomware, which by its very nature ensures the business knows they have been compromised.

## INCIDENT IMPACT

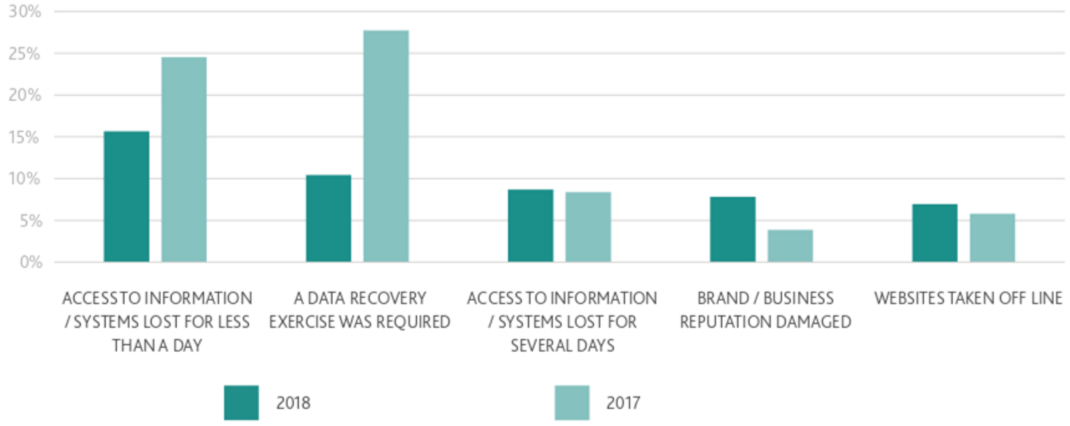
The impact of an incident on a business can vary considerably and data from 2017 to 2018 shows some stark changes in these impacts over just one year. There has been a considerable drop in both 'access to information/systems lost for less than one day' and 'a data recovery exercise was required'. One could argue this is the result of a drop in ransomware attacks, which generally require a data recovery process because data is encrypted and held to ransom by the cyber criminal/s.

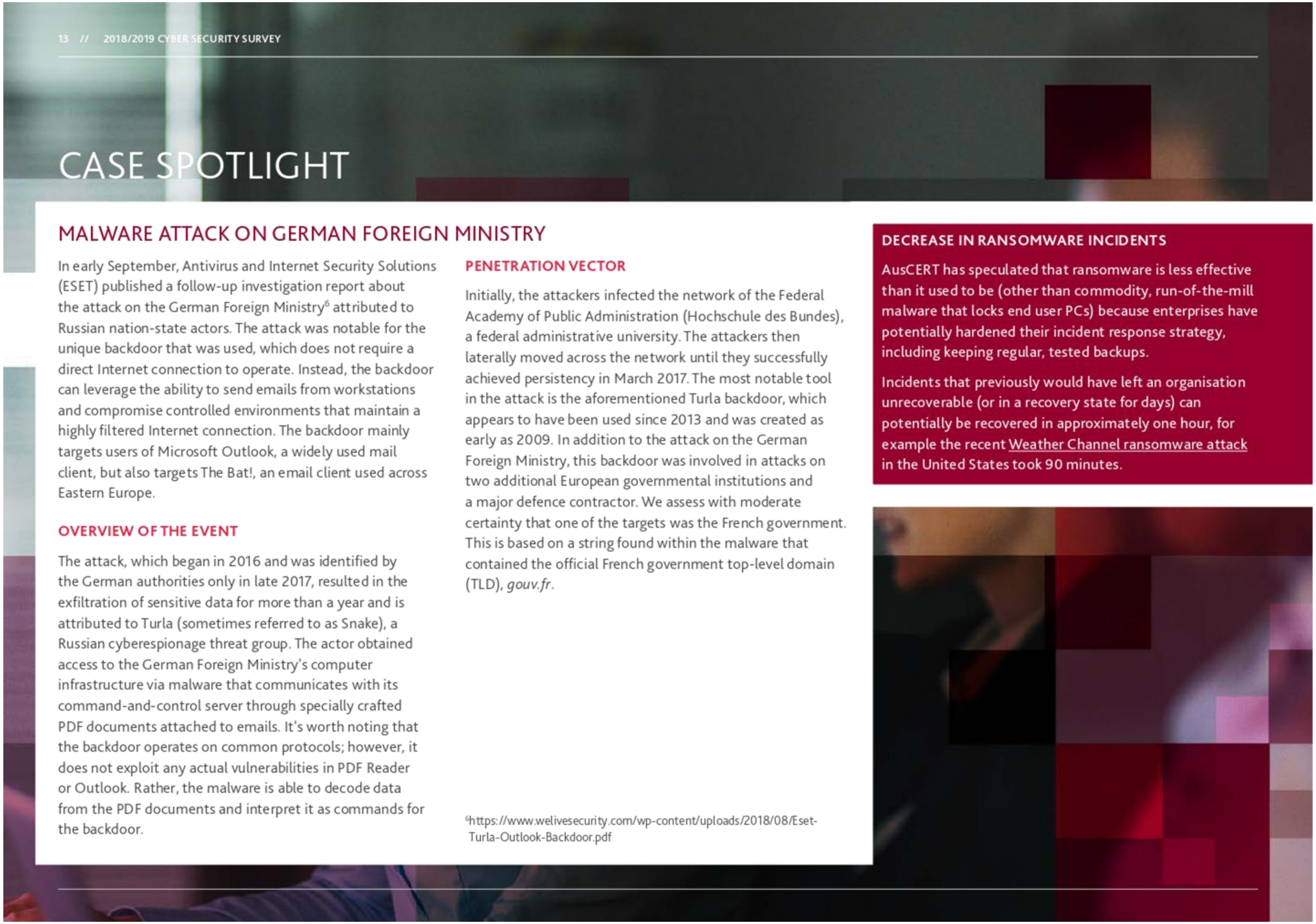
In contrast, this focus on preparedness has not filtered through to a reduction in the impact on an organisation's brand/reputation, nor their website. Both factors experienced an increase between 2017 and 2018. Business websites that have been taken offline also increased between the years.

## ORGANISATIONS THAT EXPERIENCED AN INCIDENT - 2016 TO 2018



## IMPACTS OF CYBER SECURITY INCIDENTS - 2017 vs 2018





# CASE SPOTLIGHT

## MALWARE ATTACK ON GERMAN FOREIGN MINISTRY

In early September, Antivirus and Internet Security Solutions (ESET) published a follow-up investigation report about the attack on the German Foreign Ministry[6] attributed to Russian nation-state actors. The attack was notable for the unique backdoor that was used, which does not require a direct Internet connection to operate. Instead, the backdoor can leverage the ability to send emails from workstations and compromise controlled environments that maintain a highly filtered Internet connection. The backdoor mainly targets users of Microsoft Outlook, a widely used mail client, but also targets The Bat!, an email client used across Eastern Europe.

### OVERVIEW OF THE EVENT

The attack, which began in 2016 and was identified by the German authorities only in late 2017, resulted in the exfiltration of sensitive data for more than a year and is attributed to Turla (sometimes referred to as Snake), a Russian cyberespionage threat group. The actor obtained access to the German Foreign Ministry's computer infrastructure via malware that communicates with its command-and-control server through specially crafted PDF documents attached to emails. It's worth noting that the backdoor operates on common protocols; however, it does not exploit any actual vulnerabilities in PDF Reader or Outlook. Rather, the malware is able to decode data from the PDF documents and interpret it as commands for the backdoor.

### PENETRATION VECTOR

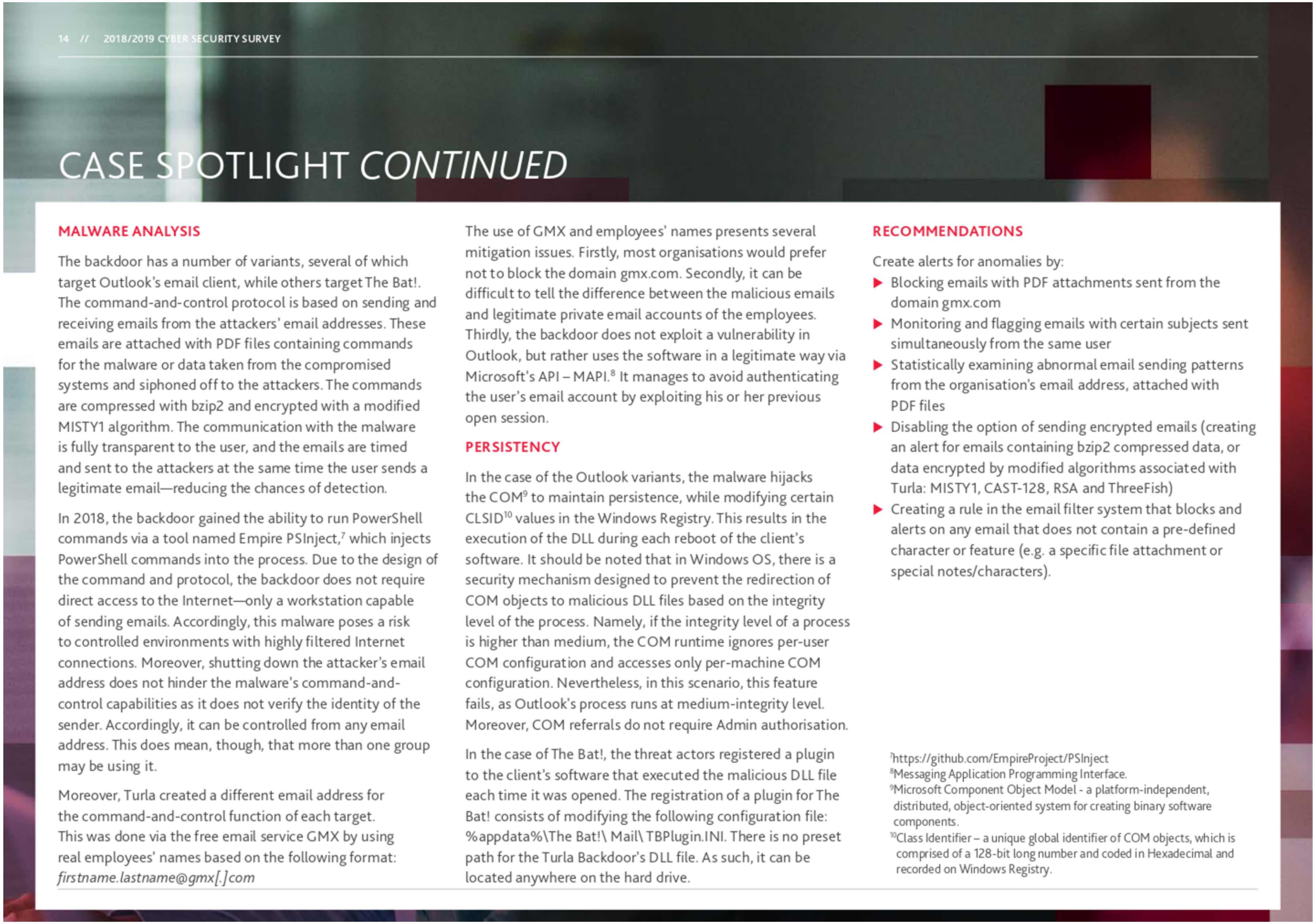
Initially, the attackers infected the network of the Federal Academy of Public Administration (Hochschule des Bundes), a federal administrative university. The attackers then laterally moved across the network until they successfully achieved persistency in March 2017. The most notable tool in the attack is the aforementioned Turla backdoor, which appears to have been used since 2013 and was created as early as 2009. In addition to the attack on the German Foreign Ministry, this backdoor was involved in attacks on two additional European governmental institutions and a major defence contractor. We assess with moderate certainty that one of the targets was the French government. This is based on a string found within the malware that contained the official French government top-level domain (TLD), *gouv.fr*.

[6] https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

### DECREASE IN RANSOMWARE INCIDENTS

AusCERT has speculated that ransomware is less effective than it used to be (other than commodity, run-of-the-mill malware that locks end user PCs) because enterprises have potentially hardened their incident response strategy, including keeping regular, tested backups.

Incidents that previously would have left an organisation unrecoverable (or in a recovery state for days) can potentially be recovered in approximately one hour, for example the recent Weather Channel ransomware attack in the United States took 90 minutes.



# CASE SPOTLIGHT *CONTINUED*

## MALWARE ANALYSIS

The backdoor has a number of variants, several of which target Outlook's email client, while others target The Bat!. The command-and-control protocol is based on sending and receiving emails from the attackers' email addresses. These emails are attached with PDF files containing commands for the malware or data taken from the compromised systems and siphoned off to the attackers. The commands are compressed with bzip2 and encrypted with a modified MISTY1 algorithm. The communication with the malware is fully transparent to the user, and the emails are timed and sent to the attackers at the same time the user sends a legitimate email—reducing the chances of detection.

In 2018, the backdoor gained the ability to run PowerShell commands via a tool named Empire PSInject,[7] which injects PowerShell commands into the process. Due to the design of the command and protocol, the backdoor does not require direct access to the Internet—only a workstation capable of sending emails. Accordingly, this malware poses a risk to controlled environments with highly filtered Internet connections. Moreover, shutting down the attacker's email address does not hinder the malware's command-and-control capabilities as it does not verify the identity of the sender. Accordingly, it can be controlled from any email address. This does mean, though, that more than one group may be using it.

Moreover, Turla created a different email address for the command-and-control function of each target. This was done via the free email service GMX by using real employees' names based on the following format: *firstname.lastname@gmx[.]com*

The use of GMX and employees' names presents several mitigation issues. Firstly, most organisations would prefer not to block the domain gmx.com. Secondly, it can be difficult to tell the difference between the malicious emails and legitimate private email accounts of the employees. Thirdly, the backdoor does not exploit a vulnerability in Outlook, but rather uses the software in a legitimate way via Microsoft's API – MAPI.[8] It manages to avoid authenticating the user's email account by exploiting his or her previous open session.

## PERSISTENCY

In the case of the Outlook variants, the malware hijacks the COM[9] to maintain persistence, while modifying certain CLSID[10] values in the Windows Registry. This results in the execution of the DLL during each reboot of the client's software. It should be noted that in Windows OS, there is a security mechanism designed to prevent the redirection of COM objects to malicious DLL files based on the integrity level of the process. Namely, if the integrity level of a process is higher than medium, the COM runtime ignores per-user COM configuration and accesses only per-machine COM configuration. Nevertheless, in this scenario, this feature fails, as Outlook's process runs at medium-integrity level. Moreover, COM referrals do not require Admin authorisation.

In the case of The Bat!, the threat actors registered a plugin to the client's software that executed the malicious DLL file each time it was opened. The registration of a plugin for The Bat! consists of modifying the following configuration file: %appdata%\The Bat!\ Mail\ TBPlugin.INI. There is no preset path for the Turla Backdoor's DLL file. As such, it can be located anywhere on the hard drive.

## RECOMMENDATIONS

Create alerts for anomalies by:

- Blocking emails with PDF attachments sent from the domain gmx.com
- Monitoring and flagging emails with certain subjects sent simultaneously from the same user
- Statistically examining abnormal email sending patterns from the organisation's email address, attached with PDF files
- Disabling the option of sending encrypted emails (creating an alert for emails containing bzip2 compressed data, or data encrypted by modified algorithms associated with Turla: MISTY1, CAST-128, RSA and ThreeFish)
- Creating a rule in the email filter system that blocks and alerts on any email that does not contain a pre-defined character or feature (e.g. a specific file attachment or special notes/characters).

[7] https://github.com/EmpireProject/PSInject
[8] Messaging Application Programming Interface.
[9] Microsoft Component Object Model - a platform-independent, distributed, object-oriented system for creating binary software components.
[10] Class Identifier – a unique global identifier of COM objects, which is comprised of a 128-bit long number and coded in Hexadecimal and recorded on Windows Registry.

# REGULATORY CHANGES AND THEIR IMPACTS

## PUBLIC DISCLOSURE OF DATA BREACHES WILL LIKELY INCREASE IN 2019

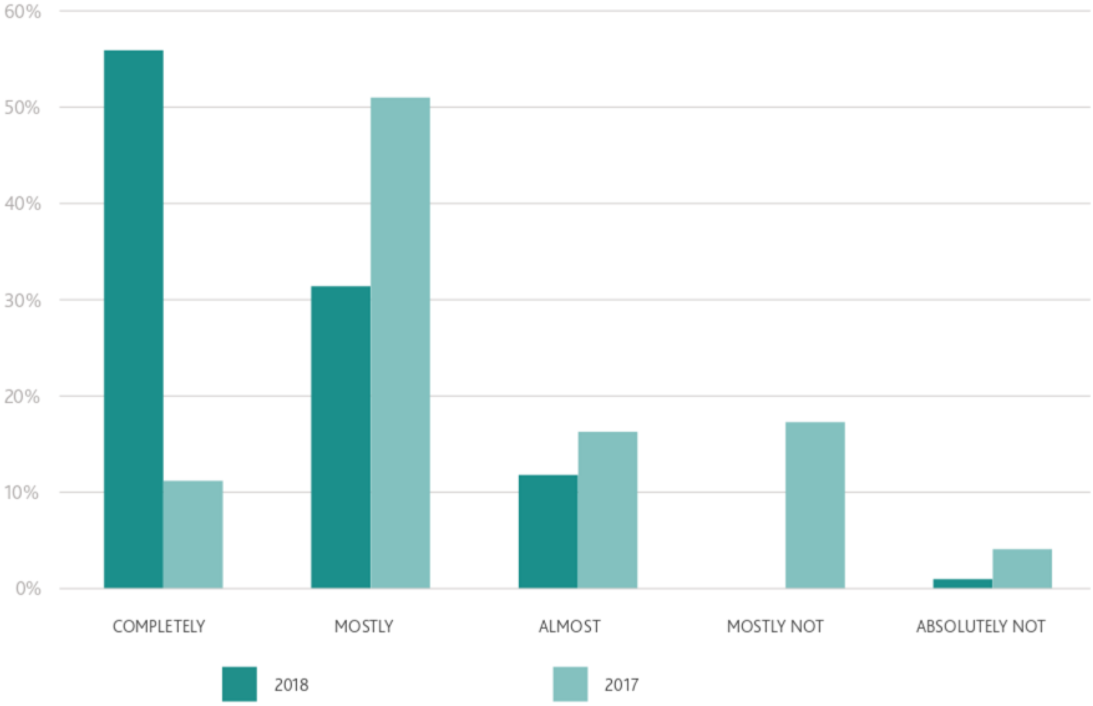
As governments become increasingly agile in responding to the ever-changing nature of cyber security threats, the regulatory landscape also continues to evolve. Naturally, with this increased focus on legislation regarding both cyber security and data privacy, the role of data breach detection, public disclosure and reporting has become significantly more prominent.

## HIGH CONFIDENCE IN MEETING NDB OBLIGATIONS

On 22 February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017 took effect in Australia. This legislation makes data breach notifications mandatory for organisations subject to the Privacy Act 1988 or with a turnover greater than $3 million per year. Furthermore, this scheme requires organisations to notify affected individuals at risk of serious harm by a data breach within 30 days of discovering the breach. There are significant financial penalties for non-compliance with this legislation of up to $420,000 for individuals and $2.1 million for organisations.

In the 2017 survey, we asked respondents to rate their confidence in meeting NDB compliance obligations. That survey also asked whether organisations who were required to comply with the scheme, had actually planned or implemented key controls necessary to prepare for it. We re-assessed respondents' preparedness for NDB in the 2018 survey and found that organisations were significantly more confident and prepared to meet their NDB obligations (55.9% completely confident in meeting NDB obligations in 2018, up from 11.2% in 2017).

CONFIDENCE IN MEETING NDB OBLIGATIONS - 2017 vs 2018



## ORGANISATIONS ARE READY TO COMPLY WITH THE NDB SCHEME

Correspondingly, respondent organisations have placed much greater emphasis on NDB preparation activities such as developing notification processes, response plans and other preparatory controls. Notwithstanding this beneficial uplift and apparent increased commitment to meeting NDB obligations, less than half of these organisations had actually tested their data breach response plans. Our experience is that the activity of exercising response plans commonly reveals simple, yet significant and often overlooked, gaps, allowing them to be adequately identified and remedied before they hinder actual data breach response efforts.

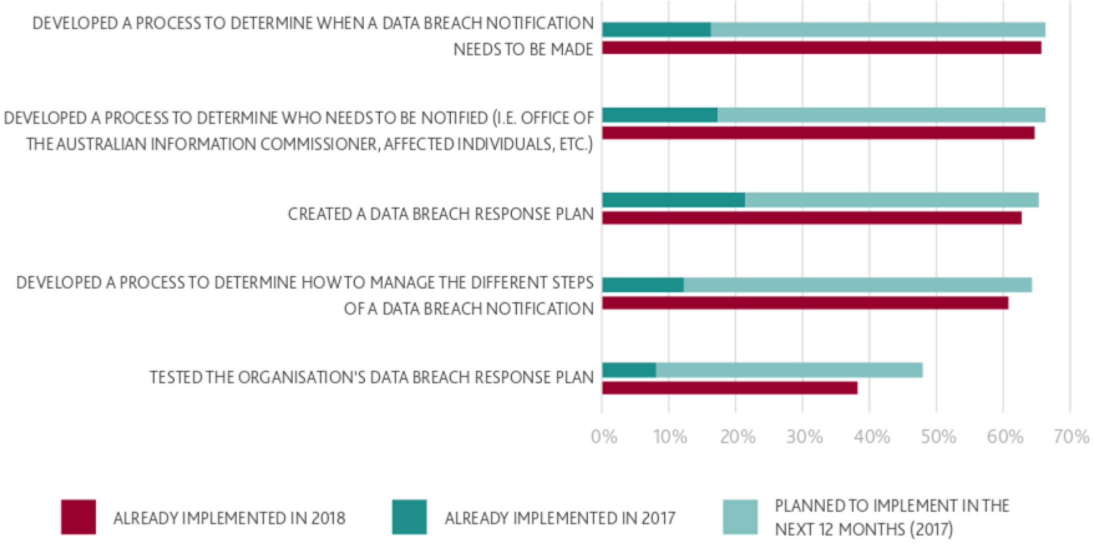
## UNCERTAINTY OF GDPR COMPLIANCE REQUIREMENTS

The GDPR introduced new requirements for data protection that took effect on 25 May 2018. The purpose of this legislation is to harmonise data protection regulations across the European Union (EU) and, as described by the OAIC, help "build legal certainty for businesses and enhance consumer trust in online services". GDPR seeks to protect all natural persons in the EU, whether they are citizens of a European country or not.

Some Australian organisations covered by the *Australian Privacy Act 1988 (Cth) (the Privacy Act)* (known as APP entities), may need to comply with the GDPR if they:

- Have an establishment in the EU (regardless of whether they process personal data in the EU)
- Do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU.

NDB PREPARATION ACTIVITIES - 2017 vs 2018



Similar to the Australian NDB scheme, there are significant financial sanctions applicable to organisations for non-compliance, including fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher).

While 18.8% of this year's respondents indicated they were required to comply with the GDPR, 38.8% responded that they did not know whether they were required to comply at all. This uncertainty is somewhat anticipated where a European data privacy regulation is imposed on organisations outside of the European Economic Area (EEA).

## LESS THAN HALF OF ORGANISATIONS REQUIRED TO COMPLY WITH GDPR CAN DEMONSTRATE COMPLIANCE

Of respondent organisations that identified the requirement to comply with the GDPR, less than 40% had implemented controls to meet their GDPR obligations. With the GDPR now enshrined in law, this indicates that the majority of organisations required to comply may not be capable of actually meeting their compliance requirements.

## DATA BREACH REPORTING BECOMING MORE FREQUENT

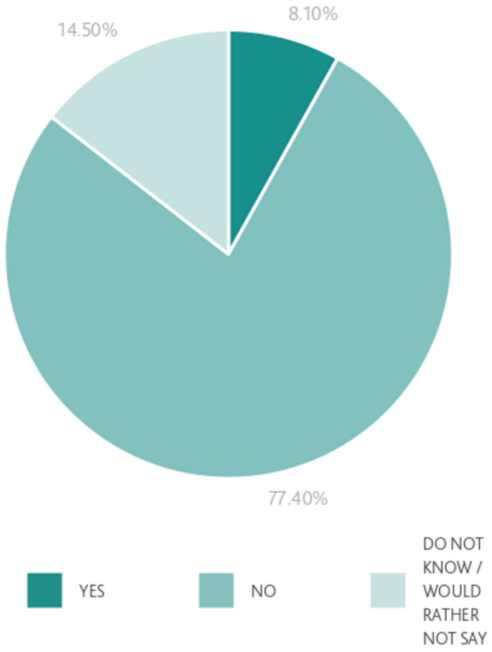
Since the NDB scheme commenced, there has been an increase in the number of data breach notifications made to the Office of the Australian Information Commissioner (OAIC) quarter-on-quarter, resulting in a total number of 812 data breach notifications for 2018[11].

As was seen in 2017, the OAIC's Q4 Report identified that the most common sectors making data breach notifications included health service providers (163), legal, accounting and management services (87), finance (119) and education (62). To a lesser extent, this also included business and professional associations (15), mining and manufacturing organisations (12) and charities (4). It is important to note that notifications made under the *My Health Records Act 2012* are not included in these figures, as they are subject to specific notification requirements set out in that Act.

## DATA BREACHES ARE RISING, REPORTING MAY NOT BE KEEPING UP

Examining the 2018 survey results reveals the rising frequency of data breach incidents. Of key interest is that almost 1 in 10 respondent organisations that have experienced a data breach in 2018 and are required to comply with the NDB scheme, have notified the OAIC. Given their prevalence and frequency, this may indicate that some notifiable data breaches have remained unreported. We also note that most occurrences of data breach incidents, with the exception of accidental disclosure, have increased significantly since 2017.

RESPONDENTS THAT HAVE MADE A BREACH NOTIFICATION TO THE OAIC - 2018



[11] https://www.oaic.gov.au/media-and-speeches/news/anniversary-of-notifiable-data-breaches-scheme

## CYBER CRIMINALS CHANGED TACTICS AND PREFER DATA BREACHES TO RANSOMWARE

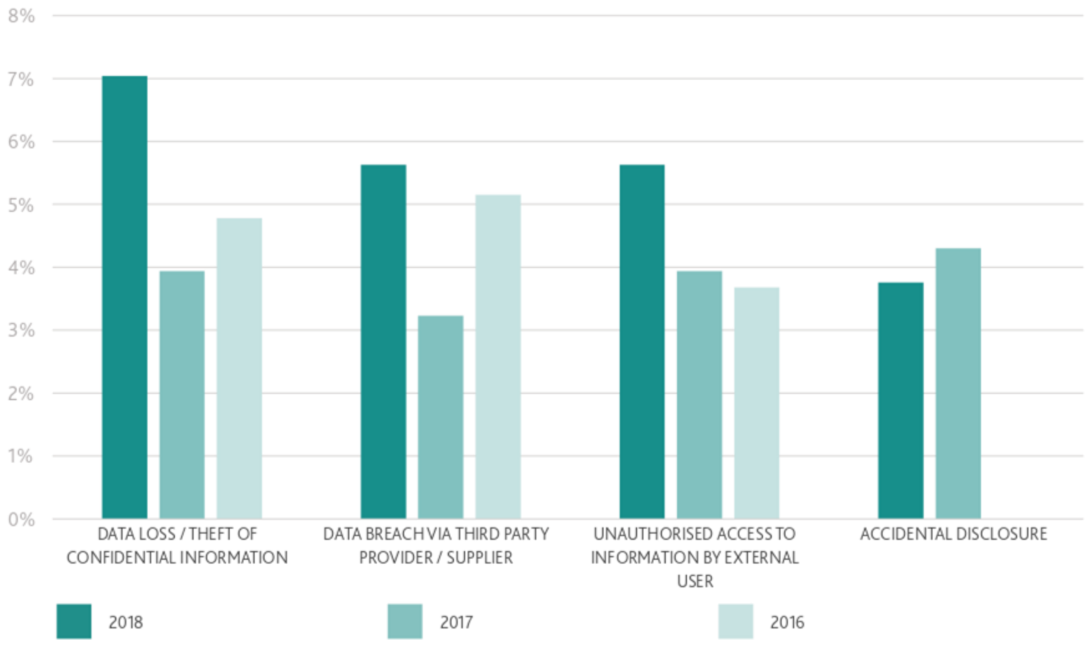
Our analysis of survey results from the past two years suggests that cyber criminals are changing their tactics, with contributing/causal factors that are two-fold:

- Cyber adversaries are changing tactics and realising the value of stolen identity and payment information (as distinct from the potential profits achievable through ransomware as seen in previous years)
- Regulatory changes requiring heightened visibility of data breach incidents have resulted in higher detection/reporting rates.

## MOST DATA BREACHES ARE DELIBERATE AND MALICIOUS

Analysing why data breaches occur, the 2018 survey found the majority of data breaches are reportedly caused by deliberate, malicious attacks. This aligns to the OAIC's latest Q4 NDB Report, which indicated that 64% of data breaches were caused by malicious or criminal attacks. Similarly, our 2018 survey found that one in three data breaches were caused by internal staff inadvertently disclosing information over email (i.e. by emailing the wrong recipient or by using the "Carbon Copy [CC]" feature instead of the "Blind Carbon Copy [BCC]" feature). This precisely mirrors the OAIC's reports, that 33% of data breaches were due to human error.

DATA LOSS FREQUENCY - 2017 vs 2018



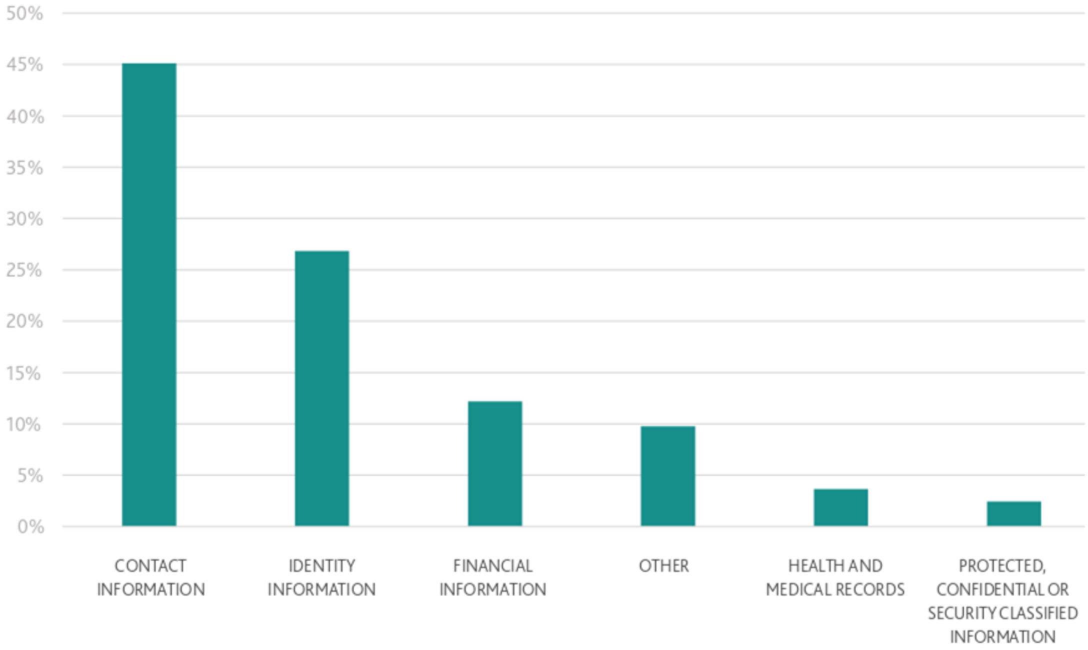
## ONE IN FOUR DATA BREACHES FACILITATE IDENTITY THEFT

The 2018 survey found the most commonly breached information type is contact information. Contact information include names (full or partial), physical addresses, telephone numbers, email addresses and usernames. Contact information was impacted in almost half of all data breaches. Alarmingly, more than one in four data breaches involved the compromise of identity information. This is information that can directly enable identity theft and fraud, allowing threat actors to (for example) take out financial loans under the victim's identity. This information includes artefacts such as passport details, birth certificates, drivers' licenses and tax file numbers.

## ONE IN TEN DATA BREACHES DIRECTLY ALLOW THEFT OF VICTIM'S FUNDS

More than one in ten data breaches reported in 2018 involved the direct compromise of financial information (including credit card details), in some cases allowing threat actors to directly and rapidly steal funds from the victim's financial institutions. In addition, 2.44% of data breaches involved security classified information, indicating that government information is not immune from data breaches, and it is being actively accessed and exfiltrated by cyber adversaries.

## CATEGORIES OF INFORMATION BREACHED - 2018



# IMPROVED CYBER MATURITY

## REDUCES THE LIKELIHOOD OF SUCCESSFUL ATTACKS

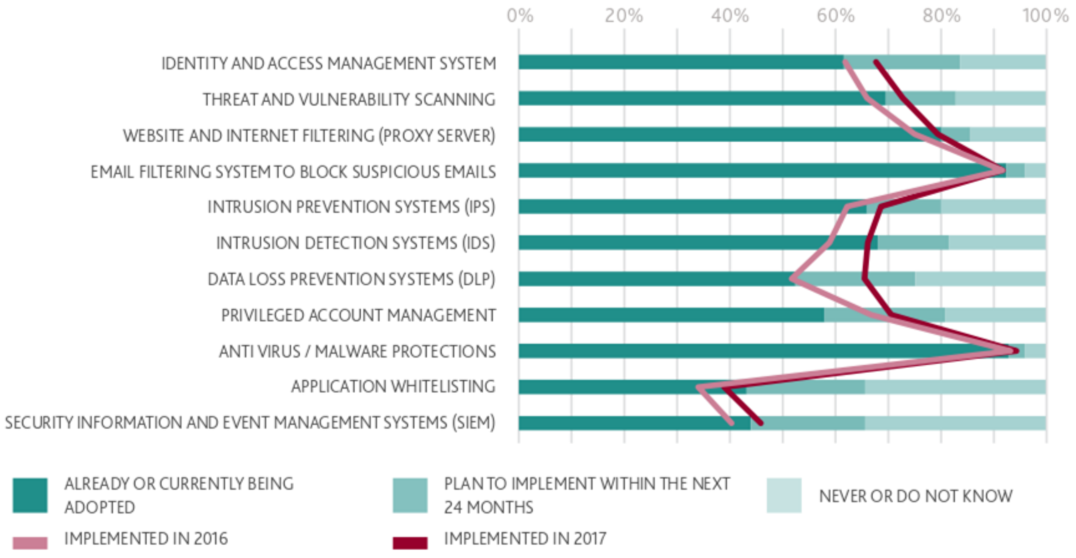
### INVESTMENTS IN CONTROLS HAVE CHANGED SIGNIFICANTLY

As seen with incidents, investments in controls have changed and shifted significantly since 2017. There are two likely primary drivers for this:

- Previously discussed significant changes in the regulatory environment, such as the NDB and the GDPR have arguably required organisations to maintain heightened visibility of cyber risk across their organisation, including into their own supply chains. This results in an increased investment in procedural and governance focused cyber security risk management practice
- Organisations are taking proactive steps to implement preventative, predictive, detective and reactive controls to meet the changing tactics, techniques and procedures (TTPs) that are being employed by cyber adversaries, across all classes of threat actor.

In light of the above, it's not surprising that we have witnessed a general shift away from investments in cyber security technology, and a honed investment lens towards those controls that could be more accurately considered procedural and governance based.

IMPLEMENTATION OF TECHNICAL CONTROLS - 2016 TO 2018

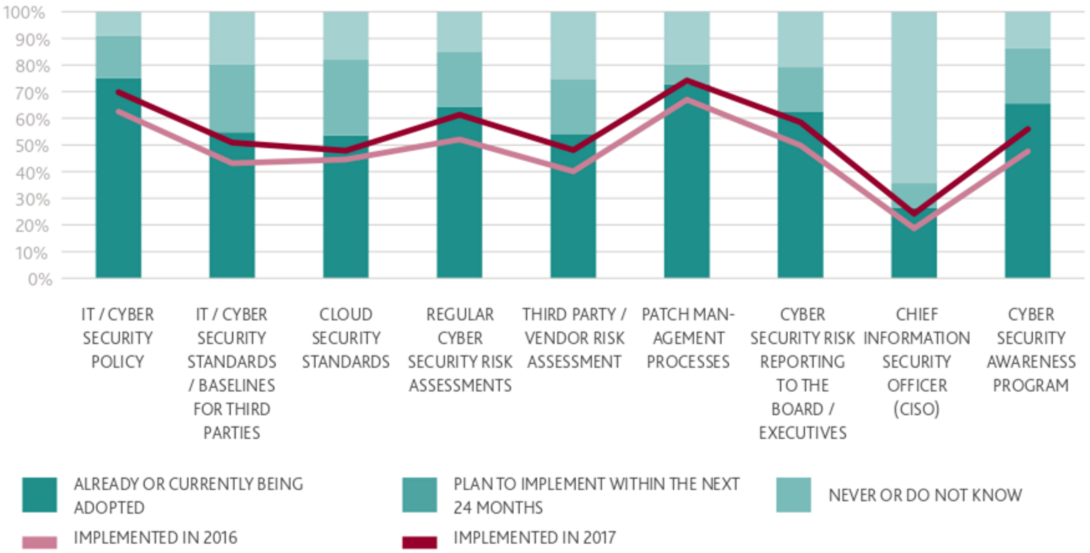


As we specifically examine the survey responses concerning the implementation of technical controls from 2016 to 2018, two downward trends and one upward trend are immediately noted:

- 65% of survey respondents indicated they had implemented a Data Loss Prevention system (DLP) in 2017, versus only approximately 52% in 2018, representing an approximate 20% year-on-year reduction
- 70% of survey respondents indicated they had implemented a privileged account management technical control in 2017, compared to approximately 58% in 2018, representing an approximate 17% year-on-year reduction
- 39% of survey respondents indicated they had implemented application whitelisting in 2017, whereas approximately 43% had put in place the same control the following year, representing an approximate 10% year-on-year improvement.

As an aside, we note that both privileged account management and application whitelisting are considered part of the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC)'s Strategies to Mitigate Cyber Security Incidents Essential Eight[12]. These prioritised mitigation strategies are designed to assist organisations in protecting their systems against a range of cyber threats.

IMPLEMENTATION OF PROCESSES AND STANDARDS - 2016 TO 2018



[12] https://acsc.gov.au/infosec/mitigationstrategies.htm

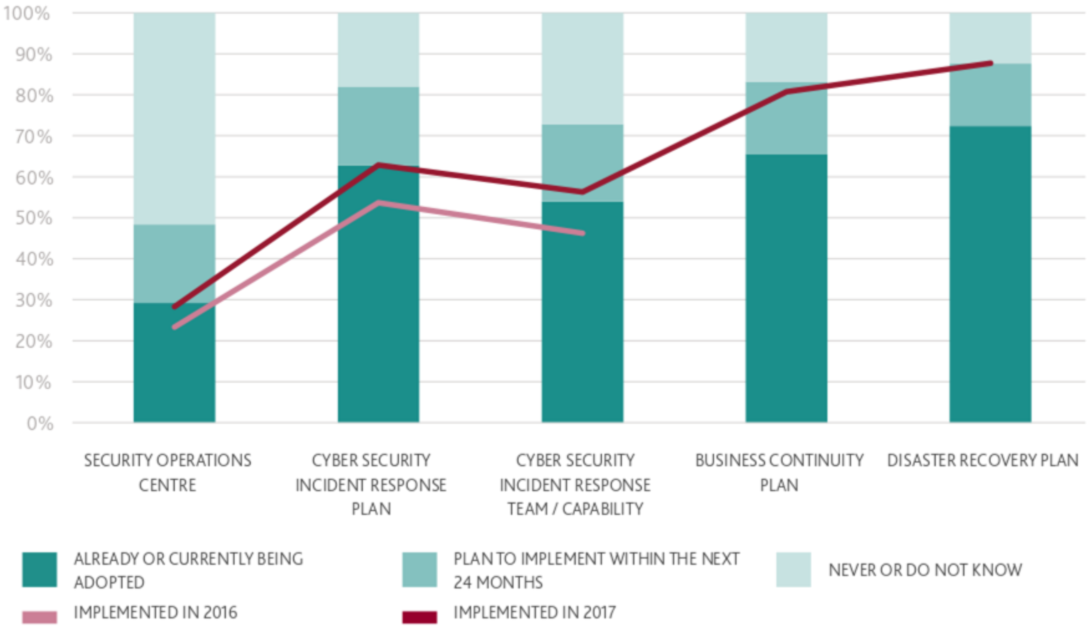
When we examine respondents' implementation of processes and standards from 2016 through to 2018, we observe further evidence of these shifts away from specific cyber security technologies and towards more general processes and standards.

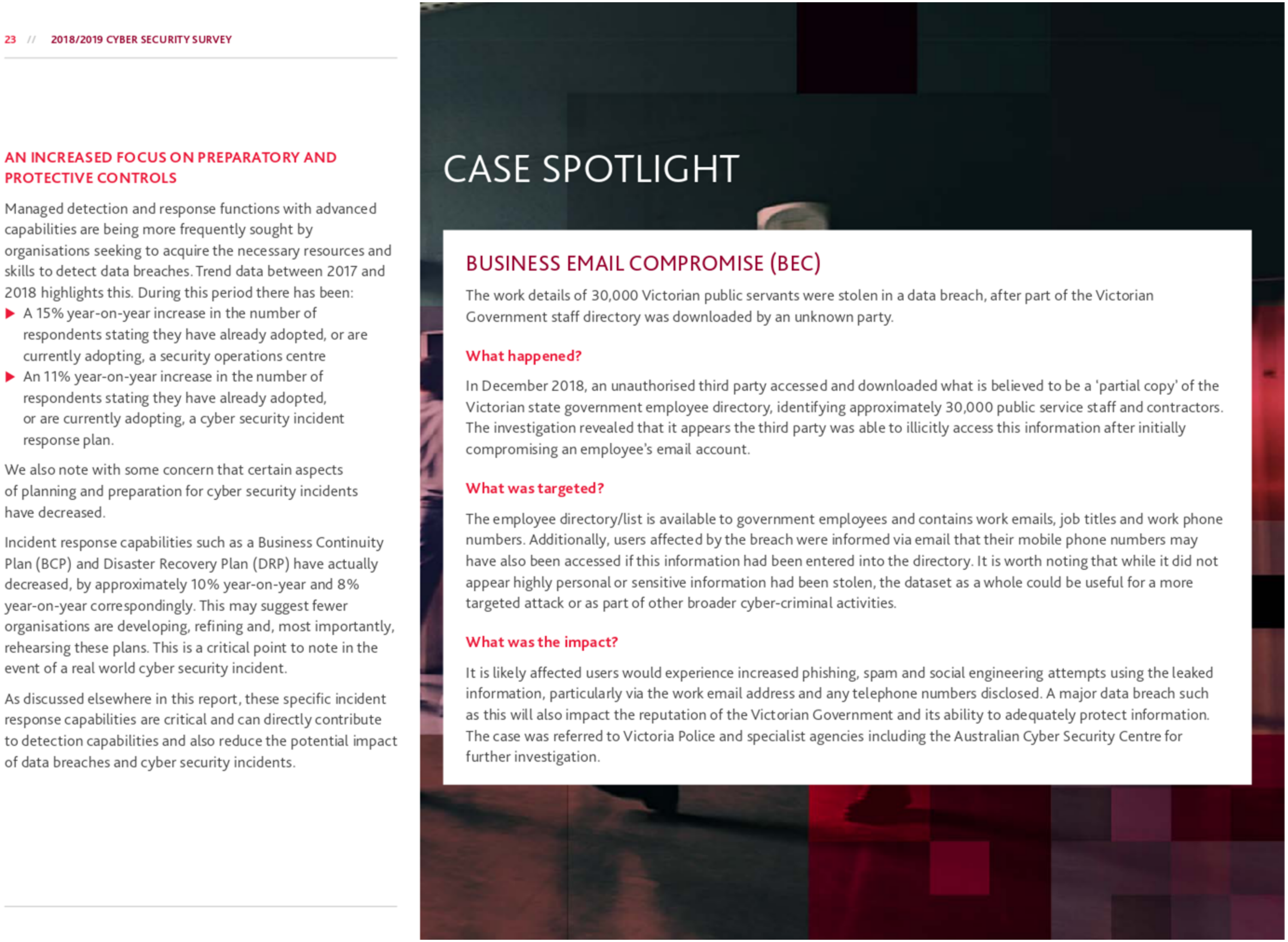
We note with positive interest that:

- Cyber security awareness programs have been adopted nearly 20% more often as compared to 2017
- There was a 12% year-on-year increase in both third party vendor risk assessments and cloud security standards as compared to 2017.

The benefits to organisations seeking to improve both their resilience and improve their maturity through the implementation of a cyber security awareness program cannot be understated. In short, if they lessen the likelihood of their organisation being breached, they will likely be more capable of meeting regulatory requirements and experience an uplift in the organisation's overall cyber security culture.

IMPLEMENTATION OF INCIDENT RESPONSE CAPABILITIES - 2016 TO 2018





### AN INCREASED FOCUS ON PREPARATORY AND PROTECTIVE CONTROLS

Managed detection and response functions with advanced capabilities are being more frequently sought by organisations seeking to acquire the necessary resources and skills to detect data breaches. Trend data between 2017 and 2018 highlights this. During this period there has been:

- A 15% year-on-year increase in the number of respondents stating they have already adopted, or are currently adopting, a security operations centre
- An 11% year-on-year increase in the number of respondents stating they have already adopted, or are currently adopting, a cyber security incident response plan.

We also note with some concern that certain aspects of planning and preparation for cyber security incidents have decreased.

Incident response capabilities such as a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) have actually decreased, by approximately 10% year-on-year and 8% year-on-year correspondingly. This may suggest fewer organisations are developing, refining and, most importantly, rehearsing these plans. This is a critical point to note in the event of a real world cyber security incident.

As discussed elsewhere in this report, these specific incident response capabilities are critical and can directly contribute to detection capabilities and also reduce the potential impact of data breaches and cyber security incidents.

## CASE SPOTLIGHT

### BUSINESS EMAIL COMPROMISE (BEC)

The work details of 30,000 Victorian public servants were stolen in a data breach, after part of the Victorian Government staff directory was downloaded by an unknown party.

**What happened?**

In December 2018, an unauthorised third party accessed and downloaded what is believed to be a 'partial copy' of the Victorian state government employee directory, identifying approximately 30,000 public service staff and contractors. The investigation revealed that it appears the third party was able to illicitly access this information after initially compromising an employee's email account.

**What was targeted?**

The employee directory/list is available to government employees and contains work emails, job titles and work phone numbers. Additionally, users affected by the breach were informed via email that their mobile phone numbers may have also been accessed if this information had been entered into the directory. It is worth noting that while it did not appear highly personal or sensitive information had been stolen, the dataset as a whole could be useful for a more targeted attack or as part of other broader cyber-criminal activities.

**What was the impact?**

It is likely affected users would experience increased phishing, spam and social engineering attempts using the leaked information, particularly via the work email address and any telephone numbers disclosed. A major data breach such as this will also impact the reputation of the Victorian Government and its ability to adequately protect information. The case was referred to Victoria Police and specialist agencies including the Australian Cyber Security Centre for further investigation.

# CYBER RESILIENCE

## MORE WORK REQUIRED TO REDUCE IMPACTS

### PRIOR PLANNING AND PREPARATION INCREASES DETECTION OF DATA BREACHES

The 2018 survey found that organisations with a cyber security incident response plan and capability detected and responded to more data breach incidents than those without. In 2018, organisations with planning and preparation were 3.5 times more likely to detect data breaches via third party suppliers and providers when compared to organisations without planning and preparation.

It is unlikely organisations experience more data breaches because they have established plans and preparations. Rather, those with incident response plans and preparations are likely reporting more data breaches than those without because of their improved capability to detect them. Following from this, a confronting prospect is to be considered; that data breaches are occurring more frequently, and detected less often, than many organisations realise.

### PRIOR PLANNING AND PREPARATION REDUCES INCIDENT IMPACTS

Prior planning and preparation allows organisations to adopt an ever forward-leaning posture in the face of cyber attacks. Where incidents occur, organisations that have planned and prepared ahead of time understand how to respond immediately and effectively. This capability to rapidly detect and analyse, contain, eradicate and recover from cyber security incidents is a key contributor to reducing their impacts.

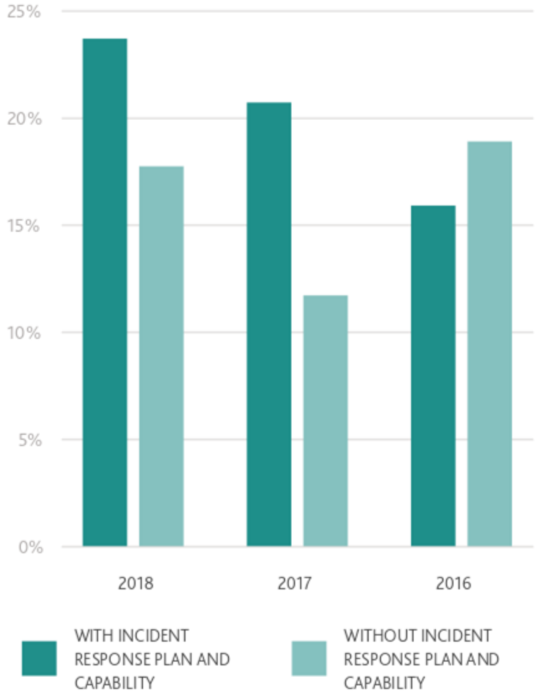
### INCIDENT RESPONSE PLANS AND CAPABILITIES REDUCE THE DISRUPTION, DURATION AND REPUTATIONAL DAMAGE OF CYBER SECURITY INCIDENTS

Across both 2017 and 2018, organisations with plans and preparations in place have experienced reduced incident impacts. These include:

- Less disruption and downtime
- Shorter incident durations
- Minimised reputational damage.

To be effective in not only preventing incidents, but reducing their impact and damage when they do occur, organisations need to be proactively establishing, rehearsing and optimising incident response plans and capabilities.

### DATA BREACH INCIDENTS DETECTED - WITH AND WITHOUT PLANNING AND PREPARATION - 2016 TO 2018



## DATA BREACHES HAVE LESS TANGIBLE IMPACTS THAT CANNOT BE INSURED

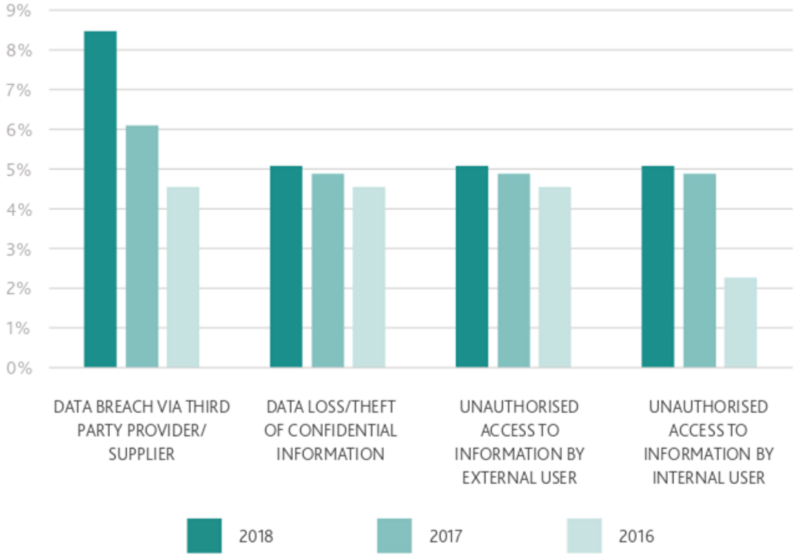
Directly linked to higher generation of profits, a brand's value is often considered one of its most important, yet intangible assets. The general makeup of an organisation's brand can be understood through the key contributors to its reputation – which include its perceived trust and strength. As a double-edged sword, the public's awareness of information security has generally increased, largely driven by high profile data breaches and global cyber security incidents with intense media coverage. As this awareness increases, it has also engendered a sense of public distrust. Numerous academic studies have cited distrust of information security as a hindrance to the adoption of services by consumers, which translates to an opportunity cost for organisations.

Information security and cyber security risk management is inextricably linked to the health of an organisation's reputation, and therefore brand (a powerful contributor to any organisation's bottom line). To strengthen the reputation is to support the brand – and to do so, organisations globally (and across all industries) have quickly recognised the returns on information security investments. The costs of a data breach, both direct and intangible, now often outweigh the cost of their mitigation.

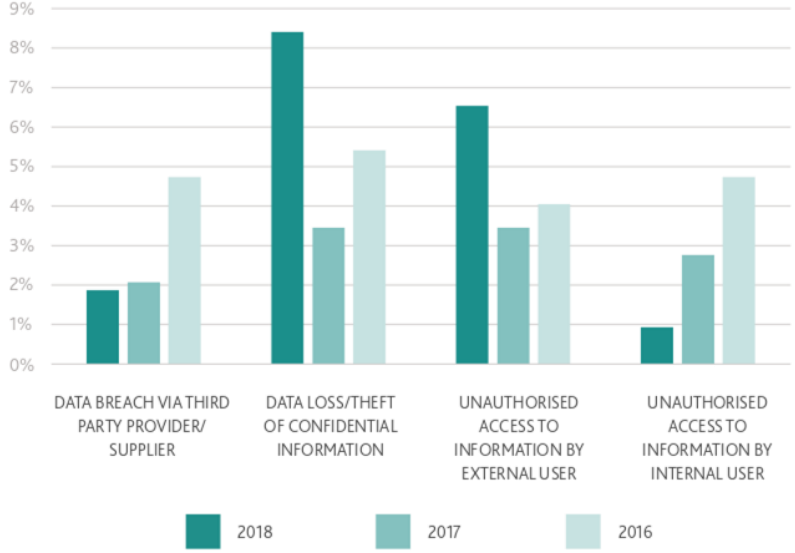
## REPUTATIONAL DAMAGE PUSHES THE BOTTOM LINE DOWNWARDS

The costs of an information security incident have, traditionally, been difficult to quantify. In recent times, numerous sources provide estimates and averages for the cost of data breaches specifically (most notably research work from Ponemon Institute's Cost of a Data Breach Study). Typically, these evaluations quantify the cost of a data breach in terms of 'cost per record'. Often, these estimates are based on simple calculations of the average direct costs attributed to responding to a data breach, such as third-party specialist advice, forensics, the cost of purchasing new systems, the cost of priority response from services providers, and the average size of the data breach. While these are simple estimations of the direct costs of cyber security incidents, wider reputational impacts can have even heavier (and traditionally more difficult to quantify) costs attributed to them.

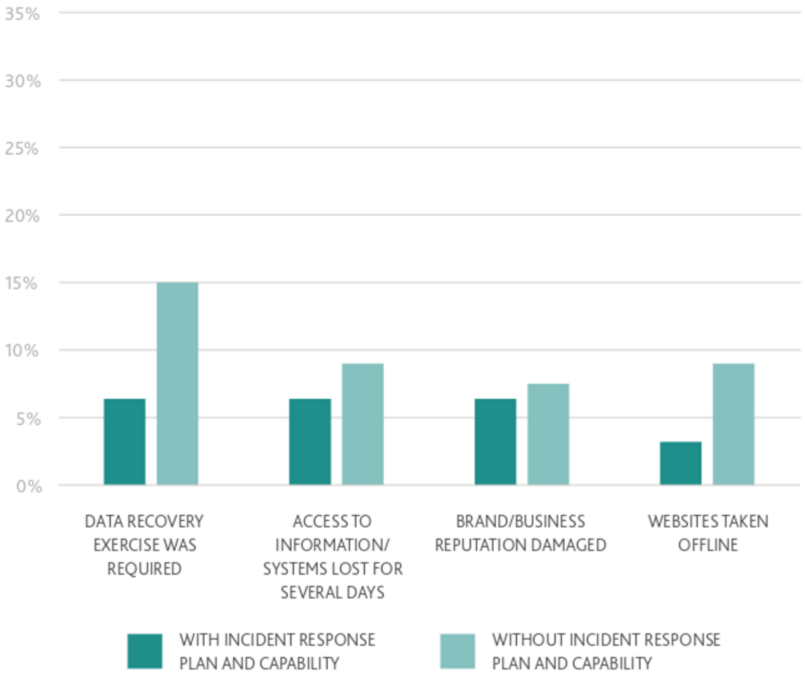
DATA BREACH INCIDENTS DETECTED - WITH PLANNING AND PREPARATION - 2016 TO 2018



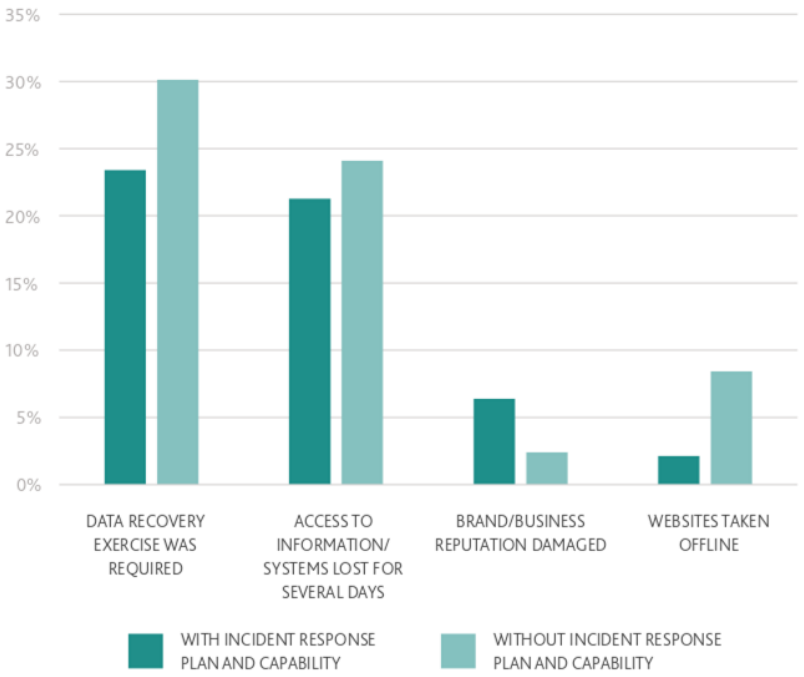
DATA BREACH INCIDENTS DETECTED - WITHOUT PLANNING AND PREPARATION - 2016 TO 2018



INCIDENT IMPACTS - 2018



INCIDENT IMPACTS - 2017



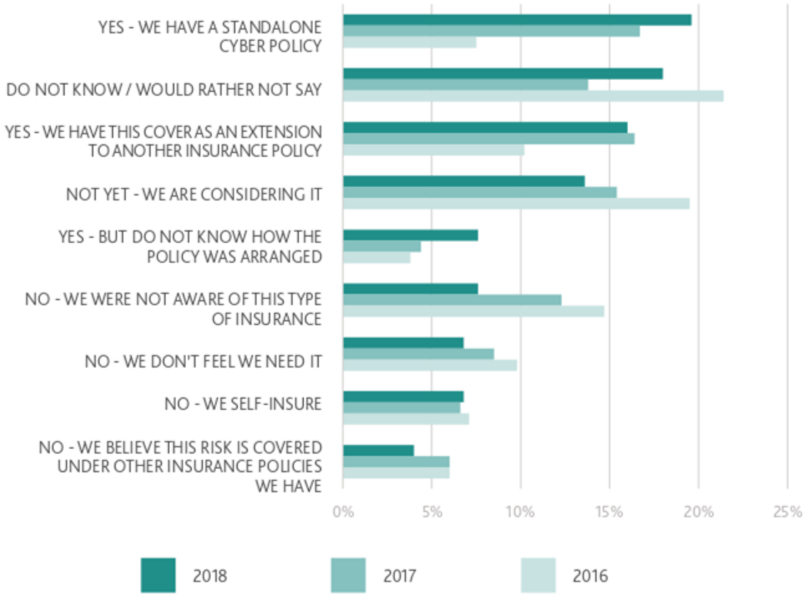
## INCREASING ADOPTION OF CYBER INSURANCE

The number of respondents indicating they have adopted cyber insurance has increased. Similarly, less organisations perceive that cyber risks are covered by other insurance policies.

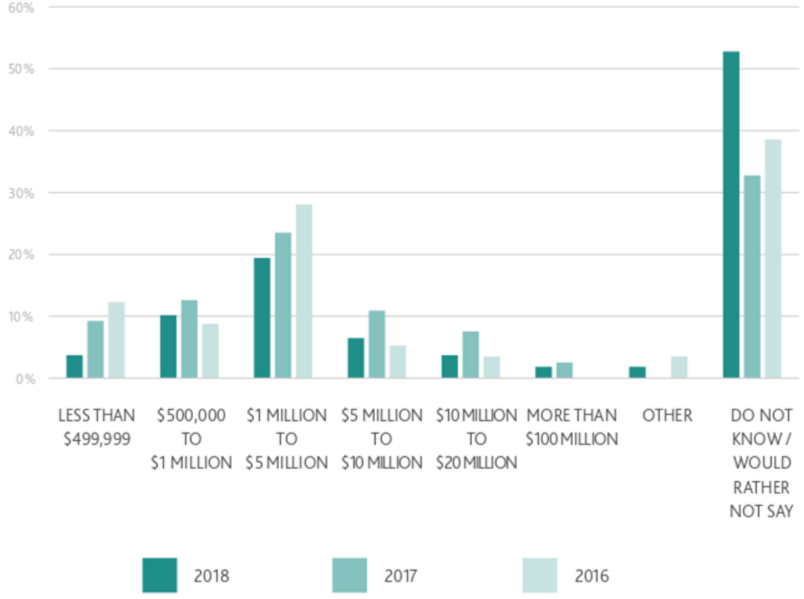
## UNCERTAINTY OF CYBER INSURANCE COSTS AND COVER

The 2018 results suggest organisations are becoming increasingly confident in the decision to adopt cyber insurance. Despite this, they also seem less certain on their premium costs and levels of cover compared to previous years. This could be indicative of an emerging awareness of and appreciation for cyber insurance, and its subsequent adoption without deeper levels of consultation.

### UPTAKE OF CYBER INSURANCE - 2017 vs 2018



### LEVEL OF CYBER INSURANCE COVER - 2017 vs 2018



# SURVEY METHODOLOGY

BDO and AusCERT deliver annual cyber security surveys to identify industry trends across private and public small to medium sized organisations across the Asia Pacific region.

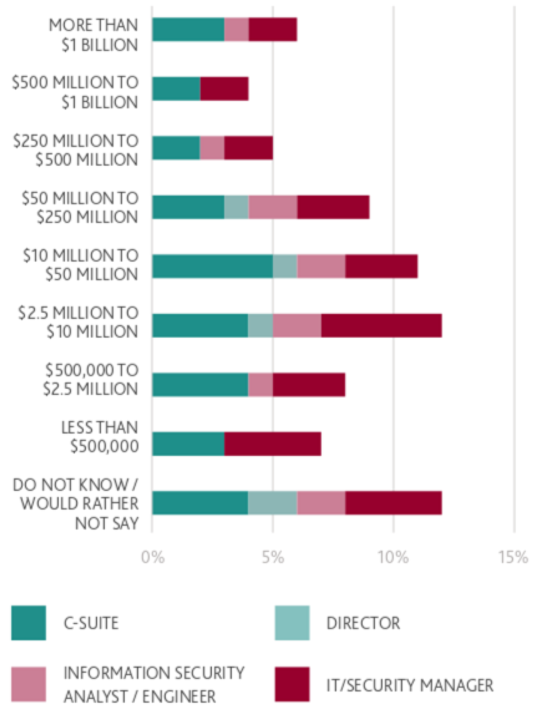
Prior to launching the BDO and AusCERT Cyber Security Survey in 2016, we found that most existing cyber security benchmarking data focused on multinational organisations in other global regions, making it difficult for Australian and New Zealand organisations to contextualise the findings and realise value through relevant, actionable insights. The data collected within this Survey Report provides a more relevant benchmark for organisations in Australia and New Zealand, who are not necessarily subject to the international legislations that have driven cyber security growth in the United States and Europe.

In 2018, we conducted the third annual BDO and AusCERT Cyber Security Survey. We received strong support from industry, with almost 500 respondents across a variety of industry sectors. Of these respondents, 74.4% were based in Australia, 20% were based in New Zealand, while 5.6% were based internationally.

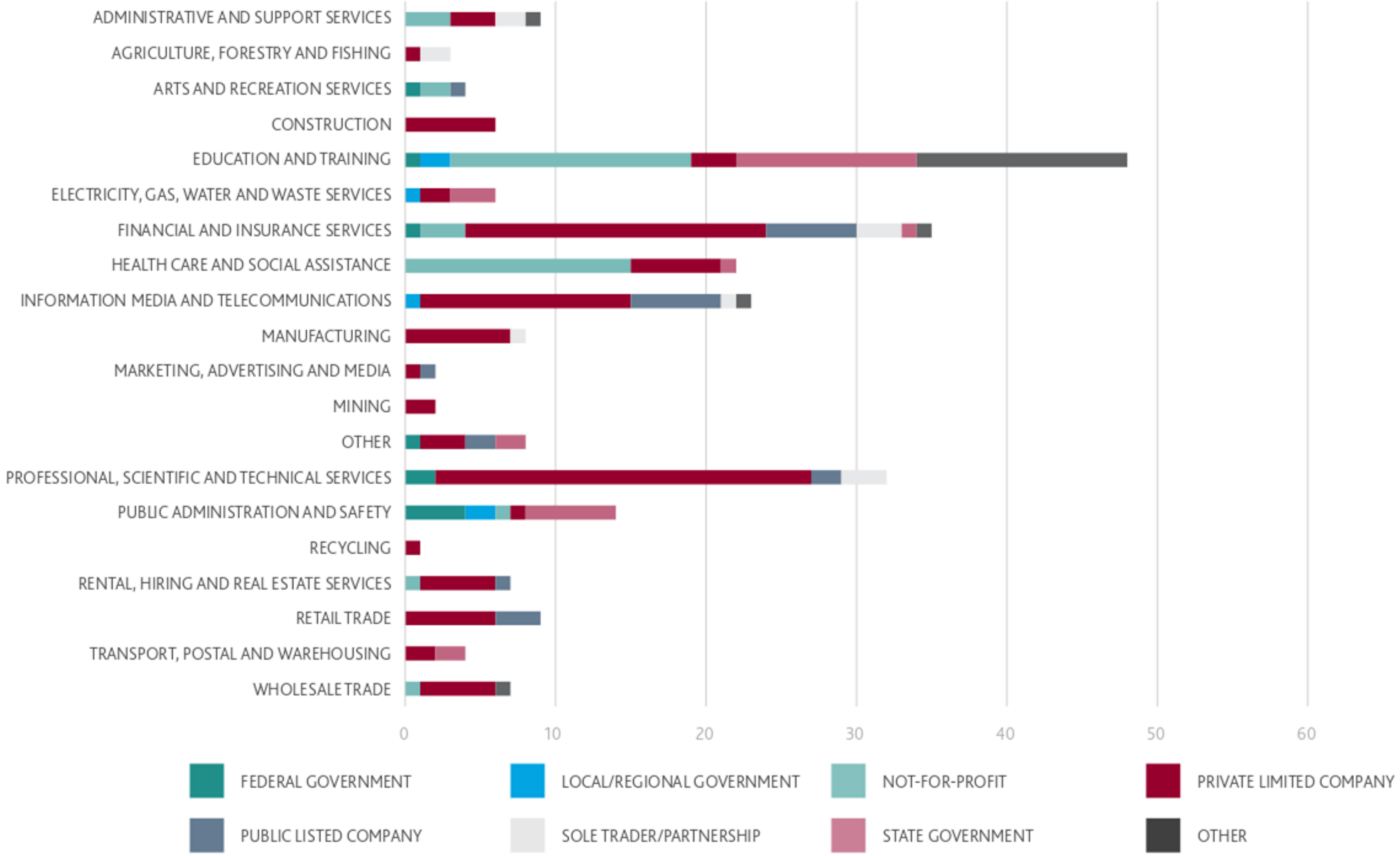
Our survey covered a wide variety of organisation types across a range of industry categories, now demonstrating a greater percentage of respondents from the education and financial sectors compared with previous years. The data set contained all industry sizes, but particularly focused on small and medium sized businesses. The individuals completing the survey were closely connected to cyber security and their organisation's risk management responsibilities:

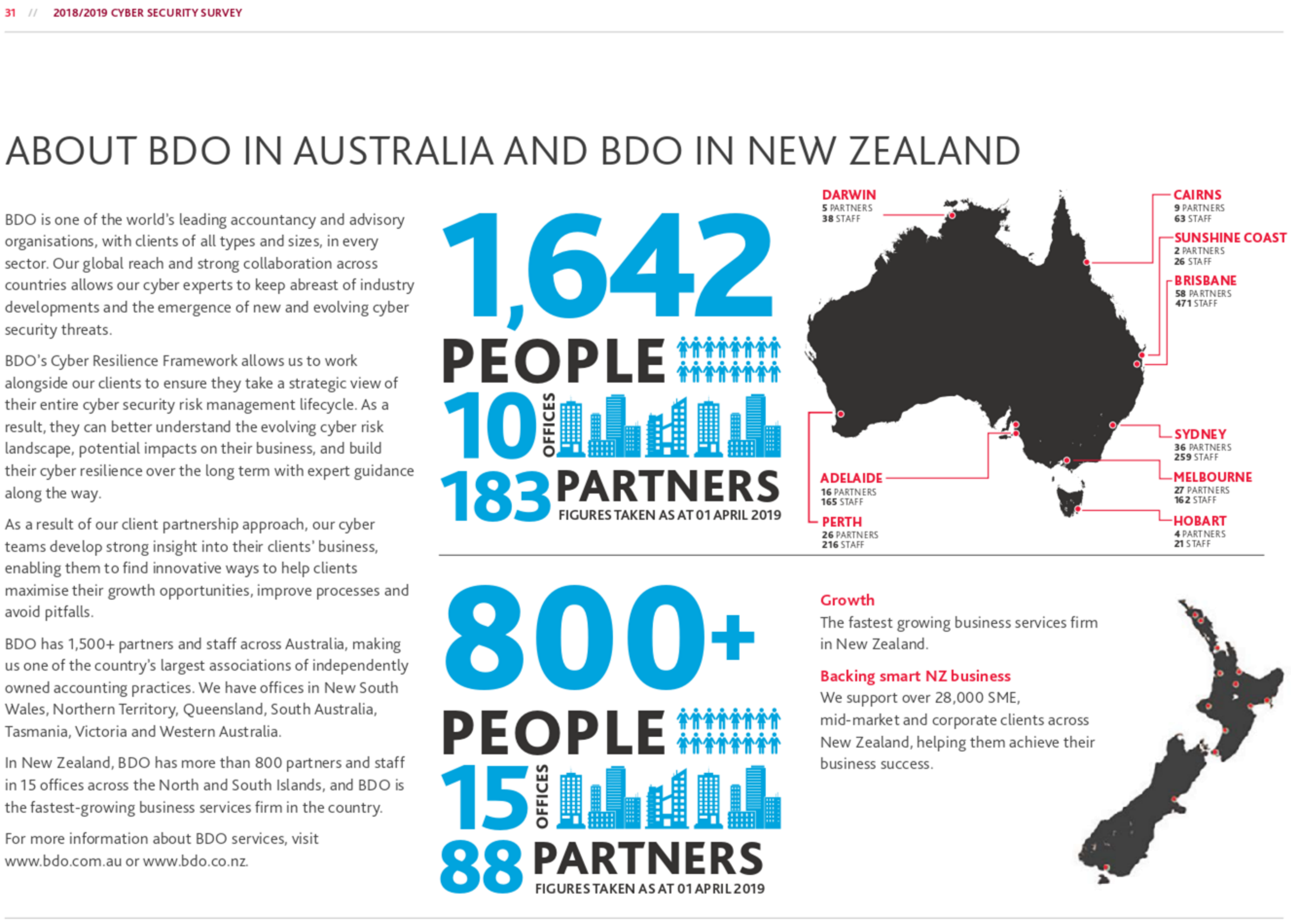
- 40.4% were C-level executives
- 28% were IT/Security Managers
- 7.6% were Security Analysts/Engineers
- 1% were Internal Auditors
- 23% were in other roles.

RESPONDENTS BY ORGANISATIONS' ANNUAL REVENUE



## RESPONDENTS BY ORGANISATION TYPE AND SECTOR





# ABOUT BDO IN AUSTRALIA AND BDO IN NEW ZEALAND

BDO is one of the world's leading accountancy and advisory organisations, with clients of all types and sizes, in every sector. Our global reach and strong collaboration across countries allows our cyber experts to keep abreast of industry developments and the emergence of new and evolving cyber security threats.

BDO's Cyber Resilience Framework allows us to work alongside our clients to ensure they take a strategic view of their entire cyber security risk management lifecycle. As a result, they can better understand the evolving cyber risk landscape, potential impacts on their business, and build their cyber resilience over the long term with expert guidance along the way.

As a result of our client partnership approach, our cyber teams develop strong insight into their clients' business, enabling them to find innovative ways to help clients maximise their growth opportunities, improve processes and avoid pitfalls.

BDO has 1,500+ partners and staff across Australia, making us one of the country's largest associations of independently owned accounting practices. We have offices in New South Wales, Northern Territory, Queensland, South Australia, Tasmania, Victoria and Western Australia.

In New Zealand, BDO has more than 800 partners and staff in 15 offices across the North and South Islands, and BDO is the fastest-growing business services firm in the country.

For more information about BDO services, visit www.bdo.com.au or www.bdo.co.nz.

1,642 PEOPLE
10 OFFICES
183 PARTNERS
FIGURES TAKEN AS AT 01 APRIL 2019

DARWIN
5 PARTNERS
38 STAFF

CAIRNS
9 PARTNERS
63 STAFF

SUNSHINE COAST
2 PARTNERS
26 STAFF

BRISBANE
58 PARTNERS
471 STAFF

SYDNEY
36 PARTNERS
259 STAFF

MELBOURNE
27 PARTNERS
162 STAFF

ADELAIDE
16 PARTNERS
165 STAFF

PERTH
26 PARTNERS
216 STAFF

HOBART
4 PARTNERS
21 STAFF

800+ PEOPLE
15 OFFICES
88 PARTNERS
FIGURES TAKEN AS AT 01 APRIL 2019

**Growth**

The fastest growing business services firm in New Zealand.

**Backing smart NZ business**

We support over 28,000 SME, mid-market and corporate clients across New Zealand, helping them achieve their business success.

# ABOUT AUSCERT

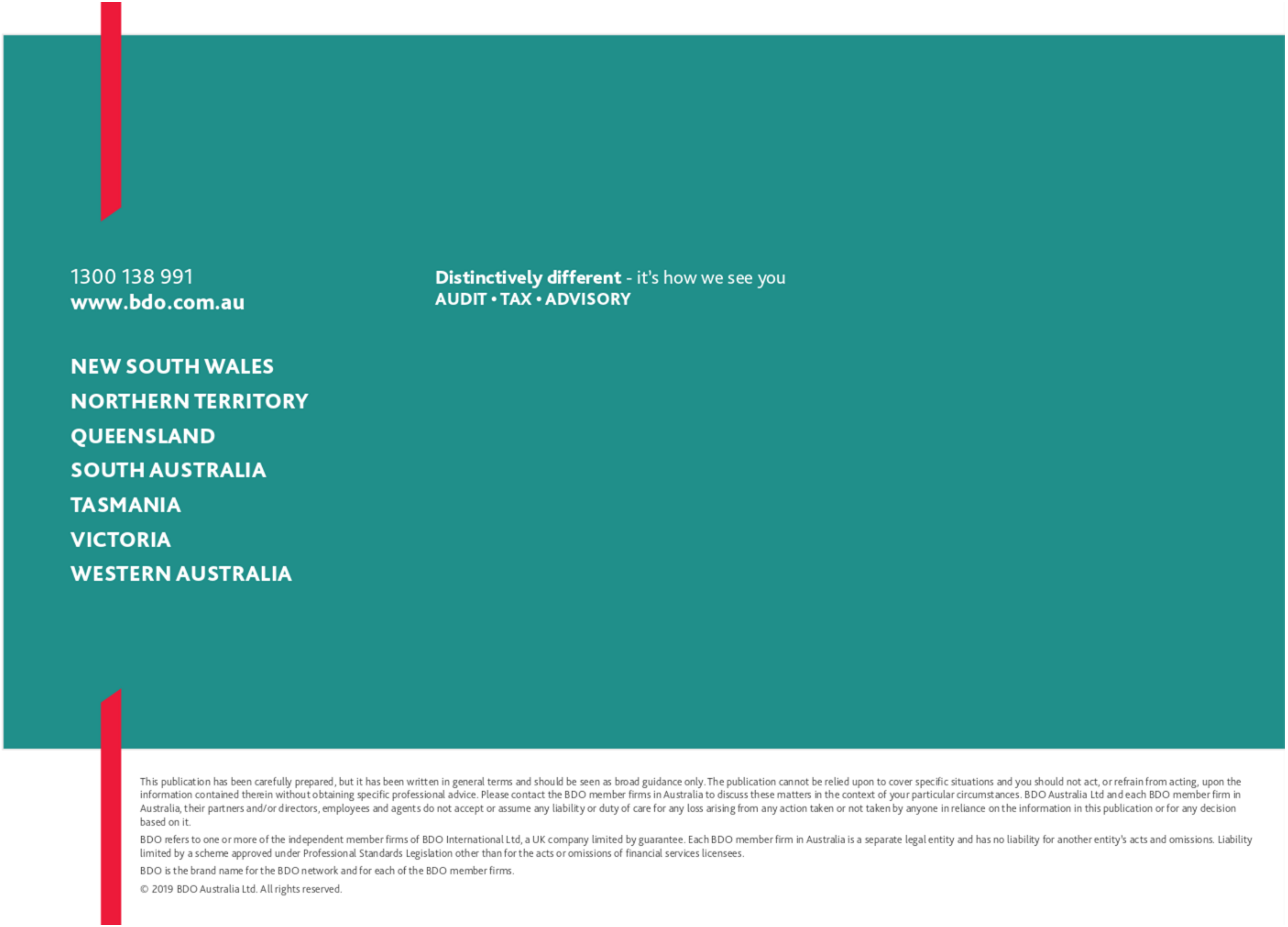
AusCERT (the Australian Cyber Emergency Response Team) is a membership-based, independent, not-for-profit security team, which is part of The University of Queensland.

AusCERT has a national focus across industry and government and has a national and global reach.

Established in 1993, AusCERT is one of the oldest cyber emergency response teams in the world. AusCERT services help organisations prevent, detect, respond and improve their resilience to cyber attacks.

For more information about AusCERT services, visit www.auscert.org.au.

AUSCERT



1300 138 991
**www.bdo.com.au**

**Distinctively different** - it's how we see you
**AUDIT • TAX • ADVISORY**

**NEW SOUTH WALES**
**NORTHERN TERRITORY**
**QUEENSLAND**
**SOUTH AUSTRALIA**
**TASMANIA**
**VICTORIA**
**WESTERN AUSTRALIA**

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations 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 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.

BDO refers to one or more of the independent member firms of BDO International Ltd, a UK company limited by guarantee. Each BDO member firm in Australia is a separate legal entity and has no liability for another entity's acts and omissions. Liability limited by a scheme approved under Professional Standards Legislation other than for the acts or omissions of financial services licensees.

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

## 5.3 ACCOUNTING STANDARDS UPDATE – REPORT NO. AR19/21548

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/21548** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Kahli Rolton, Management Accountant** |
| **Authoriser:** | **Pamela Lee, General Manager Council Business Services** |
| **Summary:** | **This report has been prepared for information to update the Audit Committee on the potential impact of upcoming changes to the Australian Accounting Standards that may impact Council's future reporting.** |
| **Community Plan Reference:** | **Goal 3: Our Diverse Economy** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/21548 titled 'Accounting Standards Update' as presented on 15 May 2019 be noted.

## BACKGROUND

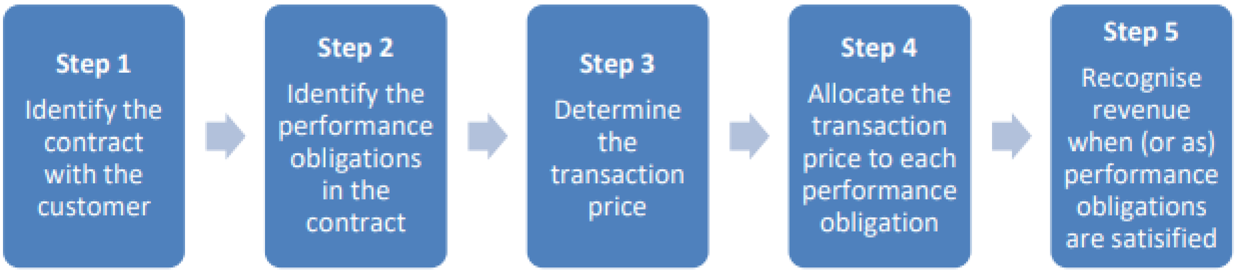
AASB 15 applies to all contracts with customers, except for contracts covered by other Standards, such as leases, insurance and financial instruments. AASB 15 was introduced to harmonise with international reporting requirements, overcome weaknesses in the previous revenue standards, deliver more accurate commercial financial reporting and a single revenue recognition model for investors to understand and compare the revenue of different companies.

AASB 15 stipulates how and when revenue is recorded, requiring entities to provide users of financial statements with more information and reporting disclosures. Its core principle is the recognition of revenue for the transfer of goods or services, at a value that reflects the consideration to which the entity expects to be entitled, in return for meeting performance obligations.

AASB 15 mandatorily applies to annual reporting periods beginning on or after 1 January 2018. As from 1 July 2019, councils are required to comply with the following Australian Accounting Standards (AASB):

### AASB 15 Revenue from Contracts with Customers

Currently, revenue transactions are often separated into components that are accounted for under different revenue standards and interpretations. This is no longer the case as AASB 15 provides a single framework for revenue recognition using a five-step model.



Step 1 Identify the contract with the customer

Step 2 Identify the performance obligations in the contract

Step 3 Determine the transaction price

Step 4 Allocate the transaction price to each performance obligation

Step 5 Recognise revenue when (or as) performance obligations are satisified

### AASB 16 Leases

Replacing the current standard AASB 117 Leases, the objective of AASB 16 is to improve transparency on financial leverage and capital employed by bringing all lease assets and liabilities onto the balance sheet.

### **AASB 1058 Income of Not-for-Profit Entities** (NFP)

AASB 1058 replaces most of the NFP income recognition requirements in AASB 1004 Contributions (AASB 1004). The main impacts of AASB 1058 are:

- The timing of income recognition will depend on whether there is any performance obligation or other liability. This will result in better matching of income and related expenses.
- NFP lessees will now recognise peppercorn leases as right-of-use assets at fair value.
- All NFP entities can elect to recognise volunteer services if they can be reliably measured.

Council is required to report on 2018/2019 comparatives regarding any change in accounting policy applied from 1 July 2019.

Copies of each accounting standard can be located at www.aasb.gov.au .

## DISCUSSION

An assessment on Council's existing accounting policies has not been completed to determine what impact (if any) there will be on existing accounting policies  as disclosed in Note 1 of Council's annual Financial Statements . In assessing whether AASB 15 will have an impact on the Council's current accounting policies, the proposed approach is to identify circumstances where the Council has:

- An agreement in place with external parties that creates an enforceable right and/or obligation on the Council; and
- The Council has promised to transfer a good and/or service that is deemed to be sufficiently specific.

A review of all Note 2 income transaction classes will be conducted to determine whether any accounting policies need to be amended to comply with the requirements per AASB 15.

AASB 16 provides guidance on how to assess whether a contract held by the Council may have a lease that will need to be accounted for in accordance with the new standard. For a contract to contain a lease under AASB 16, the standard requires that the customer (i.e. the Council) can satisfy both of the following:

- The right to obtain substantially all the economic benefit from the use of the asset; and,
- The right to direct the use of the asset.

Where a lease is identified to exist, a lessee is required to recognise the lease on the Balance Sheet through the following accounting entries:

- A ‘right of use’ asset considers the following initial cost components:
  - initial measurement of lease liability
  - Lease payment less any lease incentives received before commencement date
  - Initial direct cost
  - Estimate of costs to be incurred by dismantling /removing.
- A ‘right of use’ asset considers the following initial cost components:
  - Present value of lease payments that are not paid at the commencement date.

A review of Council’s lease register and information currently reported in the Annual Financial Statements will be undertaken to determine the changes required to the reporting and disclosure of leases to comply with the new requirements under AASB 16.

In considering the potential impact of changes to AASB 1058, the following areas will be considered further as part of the assessment to be undertaken:

- Grants
- Assets received below fair value
- Volunteer services; and
- Leases entered into that are below market rates.

As a general overview of AASB 1058, the standard follows the following general principles:

- Where grants are received to buy or construct a non-financial asset that require the unspent funds of the grant to be returned to the funding body, the unspent funds will likely result in a liability being recognised in the Balance Sheet. Grants received that have specific performance obligations (i.e. an agreement that is enforceable and there are services to be provided which are specific in nature), AASB 15 is the prevailing standard that applies in determining the correct accounting treatment. The change in accounting treatment would initially record a liability and then subsequently revenue as and when an obligation(s) has been satisfied.
- Ensuring assets which are acquired at significantly below their fair value (this includes peppercorn leases) to now be initially recorded at their fair value.
- Council may need to recognise the cost/value of volunteer services if the value can be reliably measured and the Council would have incurred the cost (i.e. engaged an external party) to deliver the services that the volunteer services relate to.
- Leases which are entered into below market value (i.e. a peppercorn lease), the right-of-use asset will be measured at its assessed fair value.

Once an assessment is completed, the results are to be consulted and agreed with Council's external auditor Galpins to ensure they will be satisfied with any proposed changes in accounting policies

## CONCLUSION

Council will review and apply where necessary a number of changes implemented by the Australian Accounting Standards Board. The Standards affected include:

- AASB 15 – Revenue from Contracts with Customers
- AASB 16 – Leases
- AASB 1058 – Income for Not-for-Profit Entities.

A report will be prepared and presented at the next Audit Committee meeting outlining the results of the completed assessments for Audit Committee Member's consideration and endorsement.

## ATTACHMENTS

Nil

## 5.4 INTERIM MANAGEMENT LETTER FINANCIAL YEAR 2018/2019 GALPINS - REPORT NO. AR19/21549

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/21549** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Jeroen Zwijnenburg, Manager Finance and Customer Service** |
| **Authoriser:** | **Pamela Lee, General Manager Council Business Services** |
| **Summary:** | **Galpins undertook the Interim Audit on 16 and 17 April 2019 for the 2019/2020 financial year. The findings and recommendations will be presented to the Audit Committee at the meeting on 15 May** |
| **Community Plan Reference:** | **Goal 3: Our Diverse Economy** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/21549 titled ‘Interim Management Letter Financial Year 2018/2019 Galpins’ as presented on 15 May 2019 be noted.

## BACKGROUND

Amendments to s129 of the Local Government Act 1999 (the Act) require auditors to provide an opinion regarding internal controls of councils. This opinion focuses on councils' obligations under s125 of the Local Government Act 1999:

> *"A council must ensure that appropriate policies, practices and procedures of internal control are implemented and maintained in order to assist the council to carry out its activities in an efficient and orderly manner to achieve its objectives, to ensure adherence to management policies, to safeguard the council's assets, and to secure (as far as possible) the accuracy and reliability of council records."*

In order to assist Council in addressing the requirements of s129, the external auditors reviewed a prioritised list of controls from the Local Government Finance Management Better Practice Model based on their initial audit risk assessment.

Council's auditors, Galpins, undertook the interim audit during their visit to Council on Tuesday 16 to Wednesday 17 April 2019.

## DISCUSSION

The scope of the interim audit included a review of internal controls the external auditors consider key controls to be in place for the purpose of addressing the requirements of s129.

The key core controls for the following key business cycles were identified as critical for the purpose of issuing a controls opinion this financial year:

- Purchasing and procurement/contracting
- Fixed assets
- General Ledger
- Accounts payable
- Credit cards
- Payroll
- Rates / rates rebates
- Banking
- Debtors
- Receipting.

A draft Interim Audit Management Letter was provided by the external auditors to Council on 6 May 2019. The Interim Management Letter was not finalised in time to be included with this report and will be presented to the Audit Committee at its meeting on 15 May 2019 by a member of the Galpins audit team.

Council's management response to the findings will focus on steps to mitigate the identified weaknesses.

## CONCLUSION

The draft Interim Management Letter indicates Council demonstrated a high level of compliance with the implementation of an internal control framework consistent with the principles within the Local Government Better Practice Model of internal financial controls.

In regards to the identified weaknesses Council's Administration is committed to implementing the required steps to address these findings in the draft Interim Management Letter.

A representative of Galpins will speak to this item.

**ATTACHMENTS**

Nil

## 5.5 PROCESS IMPROVEMENT - CUSTOMER EXPERIENCE TEAM IMPROVEMENT - REPORT NO. AR19/21550

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/21550** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Leanne Little, Team Leader Customer Service** |
| **Authoriser:** | **Pamela Lee, General Manager Council Business Services** |
| **Summary:** | **This report supporting the ongoing commitment by the Administration to process improvements provides an example of a recent process improvement by the Customer Experience Team involving manual payments received over the phone and involved the Customer Service (CX), Westpac Account Manager, Rates, Development and Finance Administration. This process improvement has also allowed CX to adopt new technology and delivered cost savings by way of administrative efficiencies and reduction in postage and printing.** |
| **Community Plan Reference:** | **Goal 1: Our People**<br>**Goal 2: Our Location**<br>**Goal 3: Our Diverse Economy** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/21550 titled ‘Process Improvement - Customer Experience Team Improvement’ as presented on 15 May 2019 be noted.
2. That examples of process improvements and service reviews from across Council be reported to the Audit Committee in accordance with the Audit Committee’s Work Program.

## BACKGROUND

Business processes are generally not as efficient as they could be. Most organisations rarely stop to re-evaluate their processes, they stick to what they started out with. While this isn't necessarily unhealthy, it does leave room for errors, mistakes, inefficiencies, ineffective allocation of resources, falling short of meeting the customers' expectations and the opportunity for improvement. This is where business process improvement (BPI) comes in.

In general terms, process improvement is a systematic approach to assisting an organisation in optimising its processes to achieve more efficient and effective processes and results.

The methodology was first documented in H. James Harrington's 1991 book Business Process Improvement. It is the methodology that both Process Redesign and Business Process Reengineering are based upon. Process improvement is considered by academics and practitioners to be part of the organisational development discipline; where by a series of actions are taken by a process owner to identify, analyse and improve existing business processes within an organisation to meet new standards, goals and other objectives, such as changes in customer expectations, changes in quality standards, reducing costs and/or accelerating schedules. Process improvements often follow a specific or defined methodology to increase the likelihood of success. Process improvement may include the restructuring of training programs to increase their effectiveness. Process improvement is also a method to introduce process changes to improve the quality of a product or service, to better match changing customer and consumer expectations or needs.

BPI, while not having a universally-accepted definition, is viewed as the analysis, review, and improvement of existing business processes. This is achieved by mapping the current process, identifying inefficiencies and improvements, redesigning the process which becomes the future state, benchmarking to initial metrics/measures, implementing improvements and monitoring the outcome. Typically, the main goal of BPI is one or more of the following:

- Goal 1: Reducing Process Time - Finding ways of carrying out the process faster or more efficiently. For example: eliminating useless non value steps to adopting new technology.
- Goal 2: Improving Output Quality - Creating an improved product with the same input of resources. This usually means finding steps within the process that negatively influence the end-product, resulting in defects, errors and rework.
- Goal 3: Cutting Out Waste - Discovering wasteful processes and cutting them out of the process. This may help achieve the first 2 goals or improve overall productivity. Staff can spend more time on the work that creates higher value for the organisation, generates high levels of customer experience and satisfaction and/or that is usually more satisfying from an employee perspective.

Council has been using a process improvement template since mid-2017 to identify, analyse, implement and monitor process improvements. The Process Improvement Plan template is used by staff to provide guidance when reviewing processes. The Process Improvement Plan template:

- Provides a robust and consistent approach to reviewing processes
- Ensures new staff/staff unfamiliar with process improvements have a template to guide them
- Identifies and engages process stakeholders
- Documents each process improvement
- Serves as a story board of each process improvement.

## DISCUSSION

A recent process improvement identified and developed by the Customer Experience Team with oversight and support from the Team Leader Customer Experience was undertaken on the Call Centre service provided where CX staff receive manual Payments over the phone. Key stakeholders were identified, involved in the review and trialing of the new workflow. This process involves CX Officers receiving payments over the telephone for:

- Development Applications
- New Bins
- Green Waste Service
- Property Searches
- Rates
- Infringements
- Mayors Christmas Appeal.

Prior to the process improvement, payments were taken over the phone, manually written onto paper based slip and handed to the cashier to process. Delays were experience with the previous process between receiving the card details and processing the payments. At times when a payment declined it required a physical call back to the customer.

Investigation of online payment platforms revealed our current banking provider was able to offer a Virtual Terminal payment solution which enabled CX Staff to utilise the internet and receive payments from any location within Council. In addition to this, authorisation status is immediate and the virtual payment offers the ability to email receipts directly to the customer, eliminating the requirement for printing and posting. Using internal workflows the receipt can be actioned to the Cashier for immediate processing.

The improved process was trialed in December 2018 and fully implemented in January 2019.

The Process Improvement Plan template for the Westpac Online Payway Service is included as Attachment 1 to this report.

## CONCLUSION

The Audit Committee have identified an interest in process improvements and service reviews to assist them to oversee efficiency and effectiveness.

Process improvement is the activity of identifying, analysing and improving existing business / administrative processes within the Council to optimisation customer service, efficiency, effectiveness and cost and to meet new requirements and/or standards; for example quality, turnaround times.

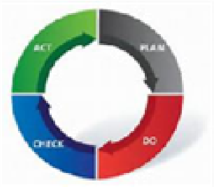
The Westpac Online Payway Service is provided as a recent example of a process improvement undertaken within Council.

## ATTACHMENTS

1. Process Improvement Plan - Westpac Online Payway Services ⇩

City of Mount Gambier

Values: Value 1, Value 2, Value 3, Value 4 and Value 5 TBC



# PROCESS IMPROVEMENT PLAN

## START WITH A PROFILE OF THE PROCESS AND/OR SERVICE

Name of process / service: Westpac Payway Online Payment Service

**Owner:** Leanne Little / Customer Experience Team

**Date of SWOT**: October 2018

**Date this review commenced**: 1/11/2018

**Date this review completed**: 1/11/2018

**Date improvements implemented**: December

Comments/ feedback on the review: A review of the current process for receiving payments over the phone required a procedure more administratively efficient. Customer Experience team are continuously looking for opportunities to gain efficiencies, save costs, utilize our It infrastructure more effectively and improve Customer Service.

**Feedback Received –**

***Issue 1*** - Senior Rates Officer provided feedback on utilizing this method when properties are in debt recovery and their ability to determine any payments made prior to escalating debt recovery.

***Solution*** 1 – In the first instance advise customer that we have a secure 1300 number on the back of the rates notice to use. If customer insists on paying, payment must be processed through the Authority system immediately to enable Rates Officers to see payments. If property is with debt recovery status, Rates Officer should be notified accordingly.

**Issue 2** – Finance Officer advised that on one occasion the daily bank amount has not matched equally to the Authority Terminal.

**Solution 2** – No administrative solution required. There was a delay in an authorization from Westpac which held over the amount of $57.05 until the next business day. This can happen using the merchant terminals at the counter also.

***Positive Feedback*** – Council utilized this payment option for receiving donations for the Mayors Christmas Appeal. Customer appreciated the ease of making donations this way. Payway also offers the ability to email a receipt immediately.

***Positive Feedback*** - Applying receipt to Development Application process has improved timeframe of moving application to next stage.

***Further Opportunity Identified***

This service offers the ability to provide a secure payment facility at any location, at any given time, providing there is access to internet.

This could be beneficial for many areas of Council including, Tourism, Events, and Community Engagement.

This could also form part of a solution for Business Continuity Analysis and Action for Council to continue business or at the very least extend operating times.

## 1. MEASURE CURRENT PROCESS OR SERVICE

### a. Process

- Customer phones and requests to make payment using Credit Card (payments may be for Green waste, Rates, Development Applications and Fines, Debtor Accounts, Mayors Christmas Apeal)
- CX Telephone Officer writes credit card details manually on slip and hands over to Cashier for processing.
- Cashier processes as a "moto" payment ***if approved***, processes through authority, prints receipt, creates postage label and places in the post. If declined Cashier phones Customer to clarify then reprocesses and completes process of printing receipt and posting.
- If relating to a Development Application, the receipt can not be applied to the DA until verified by the Cashier as approved. Slows down application process for Development Lodgements

Click here to enter text.

### b. Stakeholders

- External Customer, Rates Officers, CX Staff, Finance Staff, Westpac Account Manager

### c. Measure Current Process:

- Current manual process provides is no effective way of measuring how long the process actually takes. We have worked on an average transaction.
- If call centre operator is busy taking calls the manual process meant that it could be some time possibly hours after details were taken over the phone before payment was actually processed.
- Customer Credit Card details written down increases security risk of misuse

## 2. ANALYSE

### a. Reason for Improvement

- Gain efficiencies for Administration Staff
- Provide increased Customer Service with immediate payment confirmation
- Reduce Costs of postage by utilizing mail
- Reduce manual processes
- Increase security of Customer Information – Card details are not written down, immediate approval given no need to keep details.

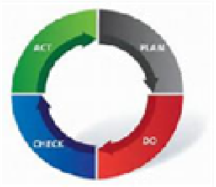
### b. Current Situation

- Current process is very manual.
- Can not give immediate approval / decline.
- Requires manual involvement of task between Call Centre and Cashier for every transaction.
- Expensive to print and mail receipts. Unable to email and electronically record receipt immediately
- Not administratively efficient.

### c. Analysis

- Appendix A illustrates the approximate costs associated with the current manual process.
- The figures ae based around the amount of manual telephone payments for the 2017/2018.
- Savings are based on completing the same amount of transactions but under the new process.
- A further review will be completed at EOFY for actual savings

Values: Value 1, Value 2, Value 3, Value 4 and Value 5 TBC



# PROCESS IMPROVEMENT PLAN

## 7. MONITOR AND CONTROL

Select measurements required for ongoing control and continue to measure process / service outcomes for conformance to implemented improvements.

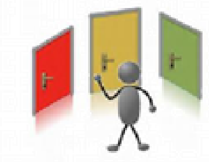
- Collection of data combined with reporting will monitor effectiveness.
- Collection of feedback and solutions to identify any problems along the way.

## PICTURE OF TEAM

- CX Staff
- Finance Officers – Bank Reconciliations
- Rates Officers – Bulk of Payments received by Council
- Development
- Future – Implementation to other Council sites.

## 3. OPTIONS

- Keep processing manual payments
- Implement New Process and Monitor for any further Improvement Opportunities
- Direct Customers to website where possible.



## 6. STANDARDISE

Develop or modify the process and/or procedures to reflect the new process / service, update the flowchart(s) and SWOT.

- Administration procedure has been created
- Training for all staff with Westpac Payway – Onsite by Westpac
- Develop Reconciliation procedures

## 5. IMPLEMENT

Implement and track changes and measures to ensure

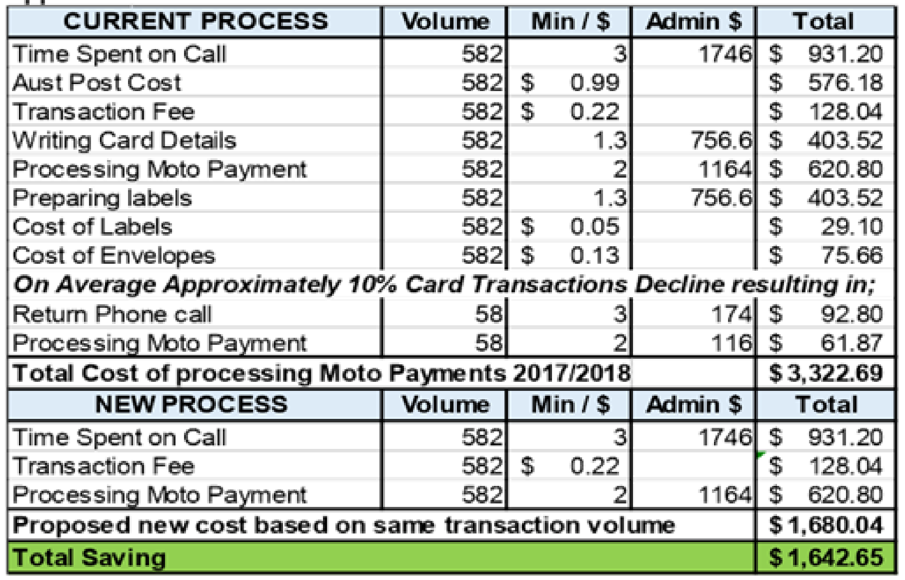
- Statistics to be recorded on type of transactions received by this method.
- Monitor effectiveness and evaluate feedback
- Continuously seek feedback from stake holders

## 4. SOLUTION

Identify best solution and confirm why.

- Proceed with Payway process.
- Increased efficiency and provide immediate approval and receipt for customer
- Significant cost saving on Administration, postage and printing
- Increased security of Customer Information.

Appendix A



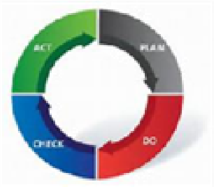
| CURRENT PROCESS | Volume | Min / $ | Admin $ | Total |
|---|---|---|---|---|
| Time Spent on Call | 582 | 3 | 1746 | $ 931.20 |
| Aust Post Cost | 582 | $ 0.99 | | $ 576.18 |
| Transaction Fee | 582 | $ 0.22 | | $ 128.04 |
| Writing Card Details | 582 | 1.3 | 756.6 | $ 403.52 |
| Processing Moto Payment | 582 | 2 | 1164 | $ 620.80 |
| Preparing labels | 582 | 1.3 | 756.6 | $ 403.52 |
| Cost of Labels | 582 | $ 0.05 | | $ 29.10 |
| Cost of Envelopes | 582 | $ 0.13 | | $ 75.66 |
| ***On Average Approximately 10% Card Transactions Decline resulting in;*** | | | | |
| Return Phone call | 58 | 3 | 174 | $ 92.80 |
| Processing Moto Payment | 58 | 2 | 116 | $ 61.87 |
| **Total Cost of processing Moto Payments 2017/2018** | | | | **$ 3,322.69** |
| **NEW PROCESS** | **Volume** | **Min / $** | **Admin $** | **Total** |
| Time Spent on Call | 582 | 3 | 1746 | $ 931.20 |
| Transaction Fee | 582 | $ 0.22 | | $ 128.04 |
| Processing Moto Payment | 582 | 2 | 1164 | $ 620.80 |
| **Proposed new cost based on same transaction volume** | | | | **$ 1,680.04** |
| **Total Saving** | | | | **$ 1,642.65** |

File Reference: AR17/43253
Process Improvement Plan A3 Template.docx
Date Template Created: 9 July 2017

PDCA: Plan-Do-Check-Act
PDCA stands for Plan-Do-Check-Act
It is a cyclical method for continuous improvement of processes.
PLAN
DO
CHECK
ACT

City of
Mount Gambier

Values: Value 1, Value 2, Value 3, Value 4 and Value 5 TBC



# PROCESS IMPROVEMENT PLAN

PDCA: Plan-Do-Check-Act
PDCA stands for Plan-Do-Check-Act
It is a cyclical method for continuous improvement of processes.
PLAN
DO
CHECK
ACT

## 5.6 AUDIT COMMITTEE REVIEW OF WORK PROGRAM – REPORT NO. AR19/21551

| | |
|---|---|
| **Committee:** | **Audit Committee** |
| **Meeting Date:** | **15 May 2019** |
| **Report No.:** | **AR19/21551** |
| **CM9 Reference:** | **AF11/863** |
| **Author:** | **Kahli Rolton, Management Accountant** |
| **Authoriser:** | **Pamela Lee, General Manager Council Business Services** |
| **Summary:** | **The Audit Committee reviews its work program annually. This report provides a draft Audit Committee Annual Work Program for 2019/2020.** |
| **Community Plan Reference:** | **Goal 1: Our People**<br>**Goal 2: Our Location**<br>**Goal 3: Our Diverse Economy**<br>**Goal 4: Our Climate, Natural Resources, Arts, Culture and Heritage** |

**REPORT RECOMMENDATION**

1. That Audit Committee Report No. AR19/21551 titled 'Audit Committee Review of Work Program' as presented on 15 May 2019 be noted.

2. That the Audit Committee adopts the Work Program as presented.

   OR

3. That the Audit Committee adopts the Work Program with the following changes:

   (a) …

## BACKGROUND

Section 126 of the Local Government Act 1999 covers the requirements of a council's audit committee including the
*(4) The functions of an audit committee as following:*

> *(a) reviewing annual financial statements to ensure that they present fairly the state of affairs of the council; and*
>
> *(ab) proposing, and providing information relevant to, a review of the council's strategic management plans or annual business plan; and*
> *(ac) proposing, and reviewing, the exercise of powers under section 130A; and*
>
> *(b) liaising with the council's auditor; and*
> *(c) reviewing the adequacy of the accounting, internal control, reporting and other financial management systems and practices of the council on a regular basis.*

The Local Government (Financial Management) Regulations 2011 Part 5 Audit Committees provides direction regarding membership of a Council's audit committee.

An independent audit committee is a fundamental component of good corporate governance. To ensure that the Audit Committee (the Committee) are executing their roles effectively as per the Audit Committee Terms of Reference (refer Attachment 1) and adding value wherever possible, the Annual Work Program provides structured guidance and focus for items the Committee is to consider and review. It is good practice to review the Annual Work Program at least annually to ensure currency and relevance of the program. The Work Program was last reviewed in February 2018.

## DISCUSSION

A revised Audit Committee Annual Work Program incorporating the meeting schedule for 2019 was last reviewed by the Committee at their meeting in February 2018 and adopted by Council at its meeting in March 2018.

The Committee's draft Work Program for 2019-2020 is provided as Attachment 2 to this report for the Audit Committee's consideration and to encourage input from members regarding areas of focus. Any alterations made to the Program can be easily identified in blue font at Attachment 2 to this report.

## CONCLUSION

The draft Annual Work Program is provided for the Committee's consideration and input.

## ATTACHMENTS

1. TERMS OF REFERENCE FOR COUNCIL'S AUDIT COMMITTEE - 10 December 2018 ⇩
2. Draft Audit Committee Annual Work Program - reviewed May 2019 ⇩

## 1 Membership

1.1 Members of the Committee are appointed by Council.

1.2 The Committee will consist of at least one independent member with at least one additional member from the Elected Members of Council, consistent with any Regulations[1]. The size of the committee shall be three (3) members.

The Mayor is an ex officio member of the Committee.

1.3 Independent member(s)[2] of the Committee must meet at least one of the following minimum requirements for membership:

- Have recent and relevant financial qualifications and/or experience in a relevant financial role
- Working knowledge of risk management
- Working knowledge of internal controls
- Experience with internal and/or external auditing.

1.3 Only members of the Committee are entitled to vote (move and second) in Committee meetings. Members of Council's staff may attend any meeting as observers and be responsible for preparing papers for the Committee. In accordance with the principles of open, transparent and informed decision making, Committee meetings must be conducted in a place open to the public. The agenda and minutes of the Committee meetings, subject to any items that are discussed in confidence under Section 90 of the Local Government Act 1999 and subsequently retained as confidential under Section 91 of the Act, are also required to be made available to the public.

1.4 Council's external auditors shall be invited to attend a minimum of two (2) meetings of the Committee each financial year. Attendance is at the external auditor's discretion.

1.5 Appointments to the Committee shall be for a period of at least two years, reviewed at a common appointment date every two years. The common appointment date for existing appointees is 31 December. Appointees may be reappointed by Council.

1.6 Resignation of appointment must be in writing.

1.7 Members of the Committee, including the Presiding Member are appointed by Council.

## 2 Administrative Resources

The Chief Executive Officer shall provide sufficient administrative resources to the Committee to enable it to adequately carry out its functions. This includes, but is not limited to:

- Adequate meeting space
- Adequate human resources to prepare agendas, reports minutes

[1] Section 126(2) provides that an audit committee may include persons who are not members of Council.

[2] A person would not be considered independent if he or she was an Elected Member of that Council. Subject to any codes of conduct adopted by Council, this does not preclude an Elected Member or an employee of a Council from being a member of an audit committee of another Council.

- Connectivity for video conference, skype, internet connection, if required, etc.

## 3 Quorum

The quorum necessary for the transaction of the Committee's business shall be 50% of the number of members [3] of the Committee plus one. A duly convened meeting of the Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in or exercisable by the Committee.

## 4 Frequency of Meetings

The Committee shall meet at least four times a year at appropriate times in the reporting and audit cycle and otherwise as required.

## 5 Notice of Meetings

5.1 Ordinary meetings of the Committee will be held at times and places as determined by the Committee. A special meeting of the Committee may be called in accordance with the Act.

5.2 Notice of each meeting confirming the venue, time and date, together with an agenda of items to be discussed and supporting papers shall be forwarded to each member of the Committee and known observers, no later than three (3) clear days before the date of the meeting.

## 6 Minutes of Meetings

6.1 The Chief Executive Officer shall ensure that the proceedings and resolutions of all meetings of the Committee, including recording the names of those present and in attendance are minuted and that the minutes otherwise comply with the requirements of the Local Government (Procedure at Meetings) Regulations 2013.

6.2 Minutes of the Committee meetings shall be circulated within seven (7) days after a meeting to all members of the Committee and made available to the public.

## 7 Role of the Committee

### 7.1 Financial reporting and management

The Committee shall:

7.1.1 Monitor the integrity of the financial statements of the Council, including in its annual report, reviewing significant financial reporting issues and judgements which they contain.

7.1.2 Review and challenge where necessary:

7.1.2.1 The consistency of, and/or any changes to accounting policies.

7.1.2.2 The methods used to account for significant or unusual transactions where different approaches are possible.

[3] Where calculating 50% results in a fraction, the fraction is dropped. For example, 3 divided by 1 equals 1.5; drop the fraction of 0.5 and the result is 1.

7.1.2.3 The compliance with appropriate accounting standards and use of appropriate estimates and judgements, taking into account the views of the external auditors.

7.1.2.4 The clarity of disclosure in the Council's financial reports and the context in which statements are made; and

7.1.2.5 All material information presented with the financial statements, such as the operating and financial review and the corporate governance statement (insofar as it relates to the audit and risk management).

7.1.3 Monitor the budgeting process and the process of review of actuals versus budget.

7.1.4 Monitor that budgets are aligned to the Strategic Management Plans.

### 7.2 Internal Controls and Risk Management Systems

The Committee shall:

7.2.1 Monitor the effectiveness of the Council's internal controls and risk management systems; and

7.2.2 Review and recommend the approval, where appropriate, of statements to be included in the annual report concerning internal controls and risk management.[4]

### 7.3 Whistle blowing

The Committee shall review the Council's arrangements for its employees to raise concerns, in confidence, about possible wrongdoing in financial reporting or other matters. The Committee shall ensure these arrangements allow independent investigation of such matters and appropriate follow-up action.

### 7.4 Internal audit where Council does not have a separate internal audit function

The Committee shall:

7.4.1 Monitor and review the effectiveness of the Council's internal audit function in the context of the Council's overall risk management system.

7.4.2 Consider and make recommendation on the program of the internal audit function and the adequacy of its resources and access to information to enable it to perform its function effectively and in accordance with the relevant professional standards.

7.4.3 Review all reports on the Council's operations from the external auditors[5].

[4] It is important that the audit committee understand the business of the Council to appreciate the risks it manages on a daily basis, and to ensure that there are appropriate management plans to manage and mitigate this business risk. This will include insurance matters, financial reporting, legal and regulatory compliance, business continuity, and statutory compliance. This can be facilitated by discussions with the external auditors and by presentations by management on how business risks are identified and managed.

[5] Note that the reports to the audit committee need not be the detailed reports that are presented to management for their review. Ordinarily a high level review report is all that is required detailing the work undertaken, the findings and management response.

7.4.4 Review and monitor management's responsiveness to the findings and recommendations of the external auditors; and

7.4.5 Where appropriate, meet the auditor without management being present, to discuss any issues arising from the internal audits carried out. In addition, the external Auditor shall be given the right of direct access to the Mayor of the Council and to the Presiding Member of the Committee.

### 7.5 External audit

The Committee shall:

7.5.1 Develop and implement a policy on the supply of the statutory audit and non-audit services by the external auditor, taking into account any relevant ethical guidance on the matter.

7.5.2 Consider and make recommendations to the Council, in relation to the appointment, re-appointment and removal of the Council's external auditor.

The Committee shall oversee the selection process for new external auditor and if an auditor resigns the Committee shall investigate the issues leading to this and decide whether any action is required.

7.5.3 Oversee Council's relationship with the external auditors including, but not limited to:

7.5.3.1 Recommending the approval of the external auditor's remuneration, whether fees for audit or non-audit services, and recommending whether the level of fees is appropriate to enable an adequate audit to be conducted.

7.5.3.2 Recommending the approval of the external auditor's terms of engagement, including any engagement letter issued at the commencement of each audit and the scope of the audit.

7.5.3.3 Assessing the external auditor's independence and objectivity taking into account relevant professional and regulatory requirements and the extent of Council's relationship with the external auditors, including the provision of any non-audit services.

7.5.3.4 Satisfying itself that there are no relationships (such as family, employment, investment, financial or business) between the external auditor and the Council (other than in the ordinary course of business).

7.5.3.5 Monitoring the external auditor's compliance with legislative requirements on the rotation of audit partners, and

7.5.3.6 Assessing the external auditor's qualifications, expertise and resources and the effectiveness of the audit process (which shall include a report from the external auditors on the Committee's own internal quality procedures).

7.5.3.7 Action(s) to follow up on matters raised by the external auditors.

7.5.4 Meet as needed with the external auditor. The Committee shall meet the external auditor at least once a year (without management being present if requested) to discuss the external auditor's report and any issues arising from the audit.

7.5.5 Review and make recommendations on the annual audit plan, and in particular its consistency with the scope of the external audit engagement.

7.5.6 Review the findings of the audit with the auditor. This shall include, but not be limited to, the following:

- A discussion of any major issues which arose during the external audit
- Any accounting and audit judgements, and
- Levels of errors identified during the external audit.

The Committee shall also review the overall effectiveness of the external auditor.

7.5.7 Review any representation letter(s) requested by the auditor before they are signed by management[6].

7.5.8 Review the management letter and management's response to the external auditor's findings and recommendations.

## 8 Reporting responsibilities

The Committee shall make whatever recommendations to Council it deems appropriate on any area within these Terms of Reference where in its view action or improvement is needed.

## 9 Other matters

The Committee shall:

9.1 Have access to reasonable resources in order to carry out its duties[7].

9.2 Be provided with appropriate and timely training, both in the form of an induction program for new members and on an ongoing basis for all members.

9.3 Give due consideration to laws and regulations of the Local Government Act, 1999, including all amendments and revisions.

9.4 Oversee any investigation of activities within these Terms of Reference.

[6] Note that these representation letters are a standard practice of any audit and provide the external auditors confirmation from management, (in particular the Chief Executive Officer) that, amongst other matters, accounting standards have been consistently applied, that all matters that need to be disclosed have been so disclosed and that the valuation of assets has been consistently applied.

[7] Subject to any budget allocation being approved by Council.

9.5 At least once per year, review its own performance.

9.6 At least once every two years review its terms of reference, to ensure it is operating at maximum effectiveness and recommend changes it considers necessary to the Council for approval.

Sitting Fees for Audit Committee Members are set by Council.

Audit Committee Meeting: 17 December 2018
Last reviewed by the Audit Committee:: 19 December 2017
Scheduled for adopted by Council: 15 January 2019

| **Report** | **Frequency** | **Timing** | | | | **Requirement**<br>• LG Act 1999,<br>• LG (Financial Management) Regulations 2011<br>• Audit Committee TOR | **Reference** |
|---|---|---|---|---|---|---|---|
| | | **February** | **April/May** | **September** | **November** | | |
| Review Annual Work Program | Annually | | 🟦 | | | TOR | 7.5.5 and 9.5 |
| Review Terms of Reference | Annually | 🟦 | | | | TOR | 9.5 |
| Internal Controls, Risks and Improvement plans (including cumulative spend and procedure) | Quarterly | 🟦 | 🟦 | 🟦 | 🟦 | Regulations<br>TOR | S 41(b)<br>7.2.1 |
| Infrastructure and Asset Management Plans and Asset Management Strategy | Annually | | 🟦 | | | TOR | 7.1.4 |
| Long Term Financial Plan | Annually | | 🟦 | | | Regulations | S 126(4)(ab) |
| Annual Business Plan and Budget (including assumptions) | Annually | | 🟦 | | | LG Act | S 126(4)(ab) |
| External Audit - Interim Review and Management Letter | Annually | | 🟦 | | | TOR | 7.5 |
| Confidential meeting with External Auditors | Annually | | | 🟦 | | LG Act<br>TOR | S 126(4)(b)<br>7.5 |
| External Auditor – Statutory External Audit and Report on Financial Results | Annually | | | 🟦 | | Regulations<br>TOR | Reg. 10<br>7.5 |
| Annual Financial Results / Statements including authorisation by Presiding Member | Annually | | | | 🟦 | LG Act<br>TOR | S 126(4)(a)<br>7.1 |
| Quarterly Budget Review | 3 times pa | 🟦 | 🟦 | | 🟦 | LG Act and TOR | S126<br>7.1.3 |
| Crisis Management Arrangements including: Emergency Management | Biennially | | | | 🟦 | TOR | 7.2.1 |
| Annual Report | Annually | | | | 🟦 | TOR | 7.1.1 and 7.2.2 |
| Policy Reviews<br>• Budget Framework Policy B300<br>• Fraud and Corruption Prevention Policy<br>• Treasury Management Policy | Refer Policies | | | | 🟦 | <br>TOR<br>TOR<br>TOR | <br>7.1.2.1<br>7.2 and 7.3<br>7.1.2.1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| T150<br>- Whistleblowing Protection Policy W150 | | | | | 🟦 | TOR | 7.3 |
| Audit Committee Self-Assessment | Annually | | | | 🟦 | TOR | 9.5 |
| Review of External Auditors' performance and overall effectiveness | Annually | | | | 🟦 | TOR | 7.5.3 and 7.5.6 |
| Annual Report to Council by the Presiding Member of the Audit Committee | Annually | | | | 🟦 | To be included in TOR when next updated | |
| Presentations will be scheduled at the request of the Audit Committee and/or to accompany reports / agenda items where relevant | | | | | | | |

## 6 URGENT MOTIONS WITHOUT NOTICE

## 7 MEETING CLOSE