

DirectorTech

Strategy + Risk + Governance



High-level advice on untangling business technology from the Centre for Internet Safety at the University of Canberra.

Issue 002, December 2017

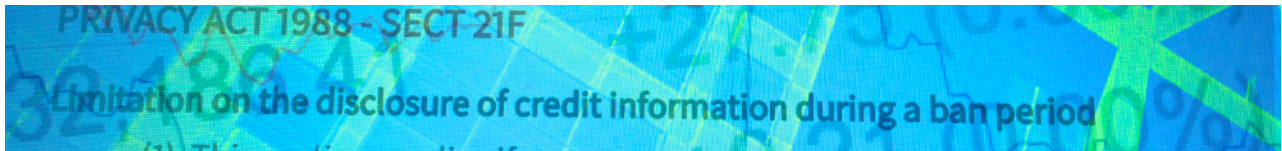
DirectorTech 002

002.001	
Getting started with data governance	3
002.002	
How the robots wrecked advertising	7
002.003	
Strategic implications of automation	11
002.004	
The ethics of automation	15
002.005	
The workplace law of social media	19
002.006	
How do you put a price on cyber risk?	24
002.A1	
About the Contributors	27
002.A2	
About DirectorTech	29

002.001

Getting started with data governance

*Even just thinking about setting up a data governance program can seem overwhelming. It's hard to know where to start. **Kate Carruthers** has some of the answers.*



Every day there are more reasons for setting up a data governance program. The General Data Protection Regime (GDPR) legislation from the European Union, for example, or the Australian Government's looming Mandatory Data Breach Notification regime

They all add to the regulatory pressure to get on top of data governance. Further, with the growth of big data and analytics, it is increasingly important to manage data as an asset.

However, there are some simple measures that will give any organisation a solid foundation for your data governance program.

A good way to start is to get a clear strategic focus and alignment, develop metrics that matter in your organisation, and develop a value proposition that key stakeholders can support. To obtain stakeholders support, be clear on what support you require from them, when you will require action from them, why you need their support, and how it will benefit them.

Build it in the business

The place to start is leadership, and leadership of the data governance program sits best in the business. This is not a technology role, although it will be required to liaise extensively with the information technology team. However, it is imperative that data governance sits somewhere in the organisation that is senior and has access to the C-suite. This is because data governance is really facilitating a dialogue between the business, risk management, privacy and cyber security.

To setup a data governance office you will need a leader who can work at all levels in the organisation, brief executive stakeholders, navigate politics, facilitate meetings, and ensure that work commitments are kept. This person does not need to be an expert at writing SQL

queries, but they do need to be able to converse with all stakeholders, and to understand data, risk, privacy, and cyber security.

Data governance is a team sport. It requires collaboration and coordination between data governance, risk management, privacy, and cyber security. Data governance is a critical foundation for a successful cyber security program. Start by asking the following questions about your data, adapted from **Mike Burgess**:

- Do you know the value of your data?
- Do you know who has access to your data?
- Do you know where your data is located?
- Do you know who is protecting your data?
- Do you know how well your data is protected?

These are great practical questions that will enable people to focus on meaningful contributions to the data governance program, instead of being confused by what data governance really means.

As you start to delve into these questions the interplay between data governance, risk and cyber security will become obvious.

Some of the other concerns of data governance include data quality, reference data management, data life-cycle management, cyber security, privacy, and metadata management. It is about controlling and protecting data, ensuring its adherence to standards and increasing its availability and usability for the organisation.

Developing an operating model

The best place to start is in developing a data governance operating model that includes:

- Data governance policy framework — to provide a mandate for the program, and to ensure that it aligns with corporate strategy. This is critical because it provides the authority for the data governance program.
- Data governance structure, including roles and responsibilities, and the data governance council or steering committee, as well as an agreed organisational decision-making process. The decision-making process is also critical, and it works in conjunction with the policy framework, because without it there will be disputes.
- Data governance work flow and work practices, which outline which activities will be undertaken, and how they will be undertaken.

- Definitions and asset types, including everything that is an organisational data asset, such as reports, systems, policies, databases, and database columns.

This is a good and practical starting point for a data governance program, and it will make sense to both business and technology folks. Business glossaries are also a useful component to start with, because they provide a focus that is relatively low tech, and they provide useful outputs quickly. They also provide a mechanism for implementing the data governance roles and responsibilities fairly quickly.

Metrics

The metrics that you decide upon will depend upon your organisational context, but it is important to decide upon them and track them so as to substantiate the data governance program. Here are examples of some metrics that could be tracked:

Metadata – Technical Metrics

- Data flow metrics – number documented, monitored
- Data dictionary – number of terms, number of search term lookups
- Orphaned data assets – number of unused reports

Metadata – Business Metrics

- Response time in determining whether a question can be answered
- The percentage of data elements where the lineage of a data item can be tracked
- Number of data elements with an agreed upon business definition

Things to avoid

Some of the ways that data governance programs can fail to thrive include:

- **Analysis paralysis.** Failure to just get started and to keep analysing and planning is a common issue. Just get going.
- **Believing that technology will solve everything.** The idea that if you can simply find the best technology, then data governance nirvana will be yours, is simply not true.
- **No change management.** Data governance is at its heart a change management problem, and this needs due cognisance.

- **Failure to focus on delivery of business value.** If the data governance program does not have delivery of business value at its heart then it is guaranteed to fail.

Some final thoughts

There is no set place to start on your data governance journey, and there is certainly no rule book. It is important to ensure that the data governance program is a good fit for your particular organisational environment and culture. But the most important thing is to just get started.

References

- Getting Started with Data Governance Using COBIT 5, <https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Getting-Started-with-Data-Governance-Using-COBIT-5.aspx> retrieved at 30/11/2017
- ISO/IEC 38505-1:2017 Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data, <https://www.iso.org/obp/ui/#iso:std:iso-iec:38505:-1:ed-1:v1:en>
- Telstra's 'five knows of cyber security', CIO, Byron Connolly, 31 August, 2015, <https://www.cio.com.au/article/583438/telstra-five-knows-cyber-security/>



002.002

How the robots wrecked advertising

*What will automation, AI, and robotics mean to businesses, and society more broadly? It depends who you ask. Predictions range from a golden era of greater wealth through to a dystopia of mass unemployment and rogue machines. **Paul Wallbank** takes a look through the prism of advertising.*



One industry has given us a glimpse of our machine-dominated future, and it's not going well. The advertising industry isn't seeing 1980s Sci-Fi movie Terminators just yet, but new technology is **causing a crisis of confidence**. Their story offers lessons for directors and executives in other industries.

The problems stem from the rise of “programmatic advertenting” — digital advertising bought and sold electronically rather than in the traditional method of being booked and placed manually.

Programmatic advertising promised to eliminate the long standing uncertainty about what actually works, something best articulated by 19th century US retail store magnate **John Wanamaker's statement**:

“Half my advertising is wasted, I just don't know which half.”

The stakes are certainly high, what with advertising being a \$500 billion a year industry. Last year, programmatic was estimated to be worth \$30 billion and growing at 20 percent per year, **according to industry magazine AdWeek**.

Beyond the web to streaming video

Programmatic advertising has largely been focused on websites. Both Google and Facebook grew wealthy from an early version of it. But the technology is now being applied to print and television. Broadcasters are seeing “addressable TV”, which targets consumers through streaming services and smart devices, as the answer to the industry's at best static revenues.

Unfortunately the promises of programmatic advertising haven't been delivered. Facebook and Google's domination of the online ad spend has left the traditional ad agencies and adtech startups to fight over the remaining 20 percent of the market.

A key problem with programmatic advertising is the plethora of middlemen. In one study the peak industry body, the Interactive Advertising Bureau, identified **ten different value layers in the ecosystem**. This complexity creates a range of opportunities for various industry players to engage in dubious and often illegal behaviour, and that has put the industry offside with its own customers.

The IAB study claimed that programmatic middlemen took 55 percent of advertisers' dollars. **Other surveys have put that figure closer to 80 percent**, which means that four out of every five dollars spent on online advertising are wasted.

And in come the lawyers...

Ridesharing service Uber, itself no stranger to allegations of misbehaviour, **sued programmatic platform Fetch**, owned by Japanese advertising giant Dentsu. Uber alleges fraud and negligence, with "tens of millions" of dollars paid for non-viewable advertisements, and for space bought on fictitious websites.

Publishers too are turning to the lawyers. In the UK, the **Guardian is suing the Rubicon Project**, one of the leading ad trading platforms, alleging the service siphoned undisclosed fees from programmatic advertising buys across its site.

The Guardian claims Rubicon obtained "secret commissions" from advertisers without the paper's knowledge, and the publisher was kept in the dark with "misleading and inaccurate" monthly reports of buyer activity.

The traditional ad agencies themselves were also quick to set up their own programmatic divisions which many clients are now finding are no less trustworthy.

On a panel at the Advertising Week conference in New York earlier this year, Dentsu Aegis Network owned Carat agency suggested all the big agencies had been **engaging in arbitrage behind their clients' backs** and they still had a long way to go to "clean up" their acts.

Outright fraud

A large part of the industry is engaging in outright fraud by coupling excessive commissions with agency arbitrage. Ad exchanges, supposedly matching advertisers and publishers, are selling ads running on faked domains. The platforms pocket the cash, and the advertiser's message doesn't get shown on the sites promised.

Ad fraud has affected all the major publishers. A **Financial Times investigation** into its own advertising inventory earlier this year uncovered 15 different ad exchanges offering video ads on FT.com, despite the publication not having that type of the inventory available.

During its investigations the FT found there were actually more fake ads being offered by scammers than the publication actually had available.

In mid November this year, Danish research company Adform **discovered the Hyphbot network**, which was placing up to \$1.2 million a day in fake ads in a swindle that was affecting almost all the major global publishers, including The Economist, the BBC and, in Australia, both Fairfax and News Corporation.

None of this had gone un-noticed by the major advertisers. The industry received a loud wake-up call at the beginning of the year when Procter & Gamble's chief marketing officer Marc Pritchard demanded "a transparent, clean and productive media supply chain". He gave agencies a 12-month deadline to deliver it. P&G is the world's biggest advertiser with an annual ad spend of over \$7 billion.

At the industry's DMEXCO Conference in September, **Pritchard expressed his company's disappointment** with the advertising industry, despite saying his agencies were 60 percent of the way to meeting his demands.

"Despite spending an astounding \$600 billion a year in marketing, our collective industries still aren't growing enough, holding stubbornly onto low, same-digit growth. You might say never has so many done so much for so little," Pritchard said.

"The reality is in 2017 the bloom came off the rose for digital media. The reason is, is the substantial waste in what has become in a murky, non-transparent and even fraudulent media supply chain. Only 25 percent of our spend was making it to the consumer. It was time for digital media to grow up."

Procter & Gamble itself was one of the more prominent advertisers to try and build its own programmatic service, threatening to bypass traditional media holding companies. That's proved difficult, however, even for the largest players. P&G has now moved back to trusting agencies.

It's never a good idea to irritate the customers

Widespread user irritation has added to the digital advertising industry's woes. One problem is inappropriate ads for things like weight loss programs. Another is irrelevant and intrusive promotions based on last week's web searches.

The advertising being delivered by many of the poorly designed or managed adtech platforms was only encouraging consumers to block ads, making it still harder for both publishers and brands.

For business in general, the issues facing the advertising industry are part of a greater problem. As automation becomes further embedded in industry, more functions are being driven by computer and managed by middlemen vendors. More core business functions risk becoming subject to fraud, hidden commissions and overspending on suppliers.

The Internet of Things is literally embedding literally into the logistics industry. Supply chains are becoming more automated, so the opportunities are ripe for a programmatic advertising debacle across many sectors. And as computers make purchasing and delivery decisions, the possibilities for mischief and profiteering increase.

So while we worry about Terminators and Chinese cyberhackers, the sad truth is we're looking at something more mundane. As long as there's greed and perverse incentives, industries are going to see perverse results.

Advertising's lessons for us all

Like many things in technology, programmatic advertising isn't as simple as it first appeared. There's some lessons for company directors and managers in other industries.

- Don't trust "black box" service providers. A vendor who says "trust me" probably can't be trusted.
- Keep things simple. The more straightforward and transparent vendor relationships are, the easier it is to manage them.
- Cut the number of middle men. More tickets being clipped means more value lost.
- Understand the technology. Relying on agencies and vendors to do the right thing doesn't always work out.
- Keep a close eye on the data and business results. If something seems amiss, it probably is.
- Make sure technology is living up to its promises and delivering results for the business.

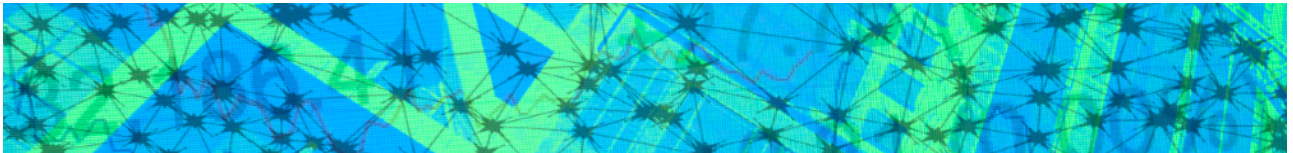
Despite the challenges, automation will increase. It's essential that managers and company directors make sure the algorithms and robots are working for them, not against them.



002.003

Strategic implications of automation

*We're drowning in a deluge of PR telling us that everything will soon be automated and run by AI. But as **Justin Warren** explains, automation isn't always the right answer.*



It is immensely gratifying to this author that the IT industry has discovered the **Toyota Production System**, and that automation is a good thing. Humans are being freed from the drudgery of soul-destroying menial tasks.

But if everything is automated, humans won't have jobs any more. That's either excellent or terrifying, depending on which start-up you're talking to.

Should we automate everything? Just some things? Which ones, and how? Answering these questions for the firm has substantial strategic implications, and that means boards need to have a view on how automation will be used.

When Everyone Is Special, No One Is

Automation works best on repetitive tasks, where each task is essentially identical to the previous one. We therefore need to identify tasks that occur repeatedly, and which create enough value in aggregate to make the cost of the automation process worthwhile, whether that be buying a robot, or writing some software.

And here we come to a conundrum of automation. If we're buying a robot from a third party, then the market for these robots must be big enough for the external firm to sell them. If we've established that the robot can automate a standard process, and if the vendor is selling these robots to other customers, then all these customers must have the same set of tasks to automate. The same applies to automation software.

If multiple competitors are all automating the same set of tasks, then these tasks are not a source of competitive advantage. Any firm can perform them if they buy the same robot we did. Similarly, any firm could perform the same automation tasks if they buy the same software as us, or outsource to the same firm.

The key in using the automation technologies, therefore, is to support the way in which your organisation creates its unique value for customers, rather than slavishly copying everyone else.

Automation Provides Leverage

Automation magnifies the effects — both good and bad — of the tasks being automated. Like financial leverage, it magnifies the good and lucky choices, but also the bad and unlucky ones.

Knowing when and where to deploy automation is therefore a strategic management decision, and should be treated as such.

What To Automate?

The best candidates for automation fall broadly into two categories:

Firstly, tasks that do not add substantial value to the customer experience, but do add cost. What is the competitive advantage of having email? Of outsourcing email services to Microsoft's Office365 service? These functions are hygiene factors, because not having essentially the same system as everyone else places a firm at a competitive disadvantage.

A note of caution, however. Over the past decade or so, many firms outsourced major sections of their IT functions to third-parties to focus on their so-called core business. These firms now find themselves in a world where IT provides enormous value to customers, but they no longer have any in-house capability. Will you be giving up future competitive advantage to save a few dollars today?

Secondly, tasks that add value to the customer and that are not reliant on humans to generate that value are good candidates for automation. Replacing the human waiters in a high-end restaurant with robots would fundamentally change the experience, possibly destroying it altogether. However, mass-produced frozen pizza doesn't need humans to be laying the same amount of cheese on each base by hand. Automation will work well here.

The challenge is accurately determining in advance what customers actually value, compared to what you imagine they value. Would customers value "artisanal hand-crafted frozen pizza" enough to pay for the cost of the extra human labour? This is the core of what running a business is about, so hopefully you have at least some ideas here, but it pays to check your intuition with research and data before you destroy what your customers love about your products with ill-conceived automation.

What Not To Automate

Areas that should not be automated tend to fall into the following categories.

Firstly, tasks that should not be performed at all. A common mistake is to apply technology to reduce the cost of business processes that should not exist. Before spending a lot of time and effort automating a process, first ensure that it is necessary to perform it in the first place.

Secondly, if the setup cost is greater than the long-run aggregate value of the tasks being automated, then it is a poor candidate. This sounds obvious, but determining the value created by a given task is often challenging, and the time horizon for “long-run” is arbitrary. In the long-run, we are all dead. Similarly, the cost of a project is often underestimated, particularly for technology related projects, so what looks economical in the initial business case may not pan out if the project overruns its budget as most typical technology projects do. Are you confident you’re better than average at these projects?

Thirdly, automation is a poor choice if the cost of changing the automation system is too high. The ability to change and adapt to future circumstances becomes more important the closer the automation system comes to the customer. Imagine a fashion house spending millions of dollars on a machine to build last year’s pants that cannot be changed to make this year’s pants without spending more than the entire season’s profits.

Finally, any processes that are important parts of the value your organisation provides to its customers, but you’re not sure what effect automating the process will have. Automating here risks damaging the customer experience while failing to derive any of the benefits of automation.

Choose Wisely

In most organisations, plenty of business activities are obvious candidates for automation. The more arguable cases can be safely left until later. Spending limited management and board oversight time on marginal prospects is a poor use of resources when plenty of juicier fruit hang much lower on the tree.

Have the discipline to identify the lowest risk and highest payoff candidates, and address them first, before moving on to more challenging, marginal cases.

It is important to clearly articulate why the chosen cases are the most attractive. Staff who are keen to automate are extremely valuable champions. If they become discouraged because they feel their advice on what to automate is falling on deaf ears, they are likely to decamp for greener pastures, placing your chosen automation projects at risk.

Organisational change is difficult enough without alienating your biggest internal supporters.

It's also important to understand the reasoning, because business conditions may change. Actions by competitors might mean that excellent choices from six or twelve months ago may no longer be. Or innovation by vendors might make a once unattractive option very attractive indeed.

It is perfectly acceptable to change your decisions based on new information when the reasoning is clear.

Next Steps

- Perform an audit of the use of automation in your organisation. Where is it being used, and where is it absent?
- Look at the overall business strategy and identify which tasks add value or competitive advantage, and why. Are some tasks hygiene factors that should be automated or outsourced? Are you sure they will stay that way?
- For tasks that add competitive advantage, are they sufficiently static and numerous to be worth automating? What is the cost of changing your automation system if the underlying tasks need to change, such as to respond to changing customer desires or actions by competitors? Will automating these tasks constrain your organisation unduly?
- Are there redundant processes you can simply eliminate instead of automating?

Further Reading

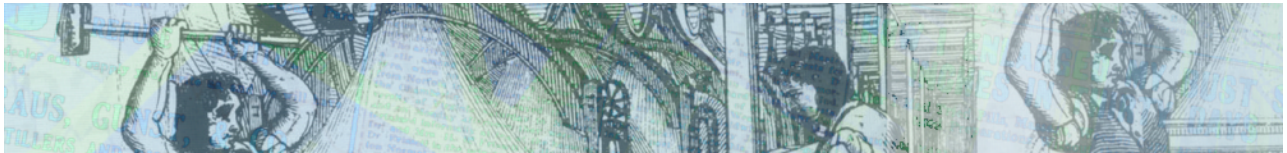
- On the concept of **financial leverage**.
- **Hertzberg 2-Factor Theory**, which is where hygiene factor comes from. That's from the book:
- Herzberg, Frederick, Bernard Mausner, and Barbara B. Snyderman. *The Motivation to Work*. 2. ed. New York: Wiley, 1959.
- The concept of "Core Business" stems from people misunderstanding this HBR article: Prahalad, C. K., and Gary Hamel. '**The Core Competence of the Corporation**'. *Harvard Business Review* 68, no. 3 (May 1990): 79–91.



002.004

The ethics of automation

*As the latest wave of artificial intelligence hype washes over us, we must be mindful of the ethical considerations of how we deploy technology. The is that we'll go too far down a dark path without realising what we've done. **Justin Warren** explains.*



There's a lot to like about automation. Indeed, the history of humankind is a history marked by the regular invention of technologies that improve our lot in life. While this progress is far from evenly distributed, we humans have managed to improve our circumstances rather a lot since we first discovered that fire was useful.

But just like fire, technology can be used for both good and evil. This isn't exactly news, but as Aldous Huxley is purported to have said:

"That men do not learn very much from the lessons of history is the most important of all the lessons that history has to teach."

Right now we're attempting to stuff as much autonomous computing power as we can into every passing watch, car, sex-toy, refrigerator, or light-bulb with nary a thought for what will happen when they're let loose upon the world. We're also discovering what happens when these tools go awry.

Strategic Incompetence?

Automation leverages the bad as well as the good. Computers can make mistakes at a scale and speed that dwarfs we mere humans.

The Commonwealth Bank (CBA) added fancy new automation technology to its (already) Automated Teller Machines, but there was a flaw. CBA says that single flaw was responsible for the bank's alleged failed to notify AUSTRAC of 53,506 transactions that were over the statutory reporting threshold.

One flaw, but a huge number of errors.

Similarly, misconfigured software lead to the **flash crash** of 6 May 2010 that wiped billions off the US stock market in seconds.

In 1995 **Barings Bank collapsed** because, in large part, it lacked internal controls to manage risk, an unacceptable excuse. It's hard to see shareholders accepting a similar excuse when automation magnifies a small operational loss into a billion dollar failure.

Boards need to consider the risk automation poses to the underlying business before it's deployed. After all, the board is expected to ensure is adequately managed.

Responsibility Failure

Poor risk management is often excused because "software systems are extremely complex". But many other extremely complex systems are expected to operate safely, especially when there's a risk to human life.

Airplanes rarely fall out of the sky of their own accord. Pre-packaged food tends not to kill us immediately.

Software will probably follow in the path of other human products and services: regulation of the risks will only happen after clear and obvious harm befalls a politically charged number of humans. In short, many people will need to die before society cries "Enough!"

Organisations that manage these risks poorly may not technically be breaking the law — yet — but that's a fairly low bar to clear. Besides, there are other advantages if you get it right.

Customers tend to prefer products that don't maim or kill them. If your organisation's use of automation has fewer negative side-effects, that's a big competitive advantage — particularly if you draw attention to your superior ethical position.

Addressing these issues now will also give you a head start on those who wait until they're forced to be more ethical.

Getting complex automated systems to adhere to new legal frameworks will make compliance with Sarbanes-Oxley or GDPR look like filling in quarterly BAS. The sooner your organisation gets on top of having its systems behave within well defined parameters, the better off it will be.

Is Not Automating Unethical?

There are situations where a failure to automate may also be seen as unethical. The key is to understand who the automation serves.

Joseph Bironas, a site reliability engineer at Google, **argued**:

“If we are engineering processes and solutions that are not automatable, we continue having to staff humans to maintain the system. If we have to staff humans to do the work, we are feeding the machines with the blood, sweat, and tears of human beings. Think The Matrix with less special effects and more pissed off System Administrators.”

Reducing the amount of tedious, meaningless labour humans are forced to endure would seem to be an unalloyed good thing. Refusing to automate these kinds of tasks could be seen as unethical, because it forces humans to serve machines created by others. That means they’re serving those human masters in a kind of machine-driven slavery.

Automation can even lead to an efficiency dead-end. Toyota has placed humans back into automated factories so they properly understand what the machines are trying to achieve, and can find new and better ways of achieving the desired outcome.

“We cannot simply depend on the machines that only repeat the same task over and over again,” project lead Mitsuru Kawai told Bloomberg. “To be the master of the machine, you have to have the knowledge and the skills to teach the machine.”

Providing meaningful work for humans has long challenged organisations, but until recently that concern has mostly been confined to blue-collar jobs. Now the professions and middle-classes are finding that their knowledge work is also being automated. They’re left to wonder “What will I do now?”

Happy employees are important if for no other reason than companies need paying customers. Replacing the entire workforce with robots is of no use if robots don’t buy what you sell.

Next Steps

- Make sure that governance of the use of automation in decision making is on the board’s agenda. Boards should ensure they’ve defined clear parameters of the level of understanding required before decision-making is even partially automated, lest the board’s authority be undermined by poorly understood automated systems.
- The board should ensure that all automated systems have a custodian who is responsible, and accountable, for overseeing their operation. The person should be able to clearly and readily answer questions about the decision parameters used by the automated systems.

- The board should also ensure that automated systems have clearly defined scope. If they begin to make decisions outside their remit, they can add unforeseen risk. This would be like a staff member overstepping their purchase authority. The board should ensure the organisations has appropriate controls in place to detect and correct such behaviour, just as they do to guard against internal fraud.



002.005

The workplace law of social media

*As the boundaries between corporate life and private life blur, comments employees make on social media can get them sacked, and the law seem to back up the employers. **Nigel Phair** highlights some recent cases before the Fair Work Commission and the courts.*



Australians love social media. As of August 2017, some **17 million of us use Facebook at least monthly**, with 12 million logging in every day. Instagram had 5 million monthly active users, LinkedIn had 4.2 million, and Twitter had 3 million.

Many of us also post details about our employment. That's obviously the case with LinkedIn, less so with the other channels. But as these four cases illustrate, the personal nature of social media hasn't been a barrier to employment termination.

So what are employees' obligations?

Employees have a number of duties to their workplace, many of which are implied at law, such as the duty to obey lawful and reasonable directions. At face value this makes sense, but what does "reasonable" mean? And what about an employee's implied right to freedom of expression, particularly via social media?

The Fair Work Commission, as Australia's national workplace relations tribunal, has been adjudicating on several of these matters.

Can insults on social media be workplace bullying?

The Commission's anti-bullying jurisdiction, which commenced on 1 January 2014, allows an individual who believes that they have been bullied at work to apply for an order to stop the bullying.

In **Sharon Bowker; Annette Coombe; Stephen Zwarts v DP World Melbourne Limited T/A DP World; Maritime Union of Australia, The Victorian Branch and Others [2014] FWCFB 9227**, three employees of DP World Melbourne Limited (DP World) had made an application to the Fair Work Commission for an order to stop alleged bullying by some of their colleagues.

Central to the case were various Facebook posts made by employees of DP World who were members of the MUA, and by MUA officials, making various “unreasonable and insulting allegations” and comparisons of two of the applicants.

DP World and the MUA sought to have those posts struck out from the application, claiming that posting on social media didn’t happen “at work” in terms of the phrase “bullied at work” defined in s.789FD of the **Fair Work Act 2009 (Cth)**.

The matter was referred to the Full Bench of the Fair Work Commission for a ruling.

The use of social media to engage in bullying behaviour created particular challenges for the Commission. They found conceptually there is little doubt that using social media to repeatedly behave unreasonably towards a worker constitutes bullying behaviour. But how does the definition of “bullied at work” apply to such behaviour?

Where the bullying behaviour consists of a series of Facebook posts, there is no requirement for the person who made the posts (the alleged bully) to be “at work” at the time the posts were made, but what about the worker to whom they are directed?

The Full Bench declined to strike out those claims. “The application of the meaning of ‘at work’ in a particular case will depend on all the circumstances and it is appropriate that the jurisprudence develop on a case by case basis,” they ruled.

Whether social media posts can count as workplace bullying is therefore still an open question.

Threats are threats, even when they’re on Facebook

In **O’Keefe v The Good Guys [2011] FWA 5311**, The Applicant, Damian O’Keefe, was dismissed from his employment with the The Good Guys for serious misconduct after four years of service.

In mid 2010, O’Keefe noticed that outstanding payments due to him remained unpaid. He then wrote, while absent from work, on his Facebook page:

“f...ing work still haven’t managed to f...ing pay me correctly. C...s are going down tomorrow.”

O’Keefe told the Commission his Facebook page was set to the maximum privacy setting, and only his select group of friends (70 people) could see what he had written. He said that nowhere on his webpage is The Good Guys mentioned.

However, under cross-examination, he stated that there were probably 11 co-workers in his select group of friends who, arguably, would have seen the entry.

The following day The Good Guys claimed that they thought O’Keefe had written was his “letter of resignation”, and some days later they’d followed up with a letter of termination, paying him three weeks notice plus annual leave payments.

O’Keefe made a complaint to the Fair Work Ombudsman. As a result, the Fair Work Inspector noted that O’Keefe hadn’t contravened any Commonwealth workplace laws or the relevant industrial instrument.

However they found, *prima facie*, that threatening another work employee is a serious issue, and one which would not be tolerated in any workplace. The manner in which the threat was made and the words used provided sufficient reason for the O’Keefe to be sacked for serious misconduct.

Twitter pseudonyms won’t protect public servants who vent

In **Banerji v Bowles [2013] FCCA 1052**, the Federal Circuit Court refused to make orders to prevent the dismissal of a public servant who had anonymously made a number of critical comments on Twitter about the Department of Immigration and Citizenship (DIAC), and, more broadly, the government and its policies.

The Applicant, Michaela Banerji, was a “public affairs officer” in the Department of Immigration and Citizenship (DIAC) when a complaint was made about her inappropriate use of social media, as well as her being employed in outside employment without permission.

A departmental investigation found that she had breached the department’s *Guidelines on Use of Social Media by DIAC Employees* and the APS Code of Conduct. A recommendation was made to terminate Banerji’s employment, and she was invited to comment on that recommendation, associated declaratory orders, and an interlocutory injunction.

Banerji argued that the department had planned on terminating her employment because of an investigation that was triggered by earlier bullying complaints that she made about her manager. She also submitted that any disciplinary action imposed for these tweets would be “unconscionable” and amount to a breach of the “constitutionally guaranteed freedom of expression”.

In rejecting Ms Banerji’s claim, the Court found there is no unfettered right (or freedom) of political expression/communication. This ruling highlights there is no unfettered freedom of political expression for public sector workers across Australia and that anonymous venting on social media about the Government’s policies is a breach of the APS Code of Conduct and departmental policies on social media use.

Employees' opinions can damage their employer's reputation

In **Little v Credit Corp [2013] FWC 9642**, the Fair Work Commission held that an employee's opinions can become a disciplinary matter if they can damage the employer's reputation or viability, or destroy the employer's confidence in them.

The applicant, Cameron Little, had posted disparaging comments on the Facebook page of a stakeholder organisation which had commercial dealings with the Credit Corp. This was not the first time Little's online activities had been noticed at work. He had been warned previously for making comments during work time on another website, in breach of the company's policies.

Little did not deny the allegations, or that the conduct breached his employer's code of conduct. His position was, in essence, that it was his time, his thoughts, and he hadn't identified himself on his profile as an employee of Credit Corp, so it really wasn't any of his employer's business.

The Commission ruled, however, that there was a valid reason for sacking Little. Deputy President Sams pointed out:

"The applicant is perfectly entitled to have his personal opinions, but he is not entitled to disclose them to the 'world at large' where to do so would reflect poorly on the Company and/or damage its reputation and viability... The fact the applicant made both Facebook comments in his own time is of no consequence. It was not when the comments were made which is important, but the effect and impact of those comments on the respondent, its other employees and on the new employee."

Lessons for Employers

Having a clear and easily accessible social media policy which reflects the expectations of the organisation is essential. The purpose of this policy is to protect the brand and reputation of the business.

The policy needs to get the balance right of what is "at work", and set out any likely disciplinary action, including termination.

Employers also need to consider who should be subject to this policy, and consider including contractors or volunteers.

Employees should receive social media training upon induction and at regular intervals, and include such issues as different kinds of social media platforms, public v private comments, and privacy settings.

When undertaking an investigation into an alleged breach of a social media policy, an employer should ensure procedural fairness. Consider the reach of the comments, whether individuals or the organisation are identifiable, and what damage may have occurred.



002.006

How do you put a price on cyber risk?

*Australia's new Notifiable Data Breaches laws will change the risk equation should an organisation suffer a cyber attack. Could cyber insurance help manage that risk? **Nigel Phair** looks at the state of the industry.*



Soon, very soon, many Australian organisations will need to reconsider the potential cost of a data breach. The **Privacy Amendment (Notifiable Data Breaches) Act 2017** comes into force on 22 February 2018. From then on, organisations covered by the **Privacy Act** will have to notify people when they're likely to be at risk of serious harm following a breach.

Many existing risk models won't work once data breaches have greater notoriety. They focus on security controls, rather than holistic risk management. Decisions are often based on an incomplete understanding of the cost of the vulnerabilities an organisation faces, and often fail to take into account all of the possible consequences

Focusing on revenue losses alone is imperfect. The challenge is to build a smart, well-designed cyber risk model that can analyse potential losses of direct revenue, liability to stakeholders, and loss of reputation.

How much does a data breach cost?

Mature organisations are realising that a cyber breach can be expensive, but quantifying their cyber risk exposure really is difficult. That in turn makes it difficult to budget for the resources needed to mitigate the risk. In every sector, every organisation will have a different risk profile, and probably a different risk appetite.

The Ponemon Institute estimated that in 2017 that the average cost of a data breach to an Australian company was \$2.51 million, with the cost per stolen or lost record being \$139. Their sample size was only 25 companies, though, so make of that what you will.

Could cyber insurance be the answer?

Cyber insurance is already the fastest-growing sector of the insurance market, according to Nick Abrahams, a partner with law firm Norton Rose Fulbright.

“The US has a massive amount of class actions in relation to privacy breaches, and the reason those class actions occur is because people know that there is insurance there to back it up,” Abrahams told the InnovationAus.com conference *Cyber Security – the Leadership Imperative 2017* in Sydney in May. As ZDNet reported, **he expects a “steep rise” in litigation.**

Back in 2013, the Centre for Internet Safety’s first **Cyber Insurance Research Paper** (PDF) found that cyber insurance would need to be a tailor-made offering. It would have to provide comprehensive cover for liability and expenses a business may incur arising out of unauthorised use of, or unauthorised access to, physical and electronic data or software within an organisation’s computer network or business. Cyber insurance policies can also provide coverage for liability, costs and expenses arising from network outages, the spreading of a virus or malicious code, computer theft or extortion.

That’s what we need. But even though cyber insurance products are in demand, the market still can’t accurately calculate the risk, according to Pip Wyrdeeman, Senior Adviser Cyber Policy for the Office of the Cyber Security Special Adviser at the Department of the Prime Minister and Cabinet (PM&C).

“The cyber insurance market in Australia is still quite immature, and there is a fundamental lack of data that enables insurers to determine what a more effective way to underwrite cyber-related matters needs to be,” ZDNet reported Wyrdeeman as saying.

“There are many impacts from a cyber incident; some can be insured against and some can’t.”

Can we trust an immature cyber insurance industry?

When it comes to buying cyber insurance for risk transfer, trust is still lacking, according to Meena Wahi, a Cyber, Data, and IP insurance specialist.

“Questions linger. Would claim payouts meet executive expectations? Are policy wordings adequate? Does the broker understand the risk? Do insurers have very high expectation for security management?” Wahi told DirectorTech.

“Insurance companies have moved up the learning curve in managing their own exposures. Lloyds of London, for instance, now insures cyber risk for one-third of all US businesses. Specialist brokers can help in building the trust between the Insurers and executives who demonstrate cyber risk management.”

What we need is data, lots of data

Fixing the cyber insurance market will require a lot of data. It will require modelling on many different loss scenarios

What does it mean to lose a percentage of customers? Or a percentage of the share price? Will margins on the sale of goods and services change? What is the cyber security posture of third-party vendors and suppliers? And what training do we give our staff?

It might seem easy to implement big, crunchy controls such as encrypting data, but how will this affect daily business operations, and what is the cost? Besides, having data encryption is useless if an employee accidentally or maliciously releases this data to third parties in clear text format.

As the modelling improves, so will the margin of error.

The responsibility lies with the risk and audit committee to spend the time analysing the various data inputs, working with internal staff and leveraging external experts. Only then will cyber insurance premiums be suitably tailored for an individual organisations risk tolerance and rating.



002.A1

About the Contributors

Meet this issue's writers.



Justin Warren @jpwarren

Justin is a 20-year veteran of the IT industry with a background in infrastructure and software development. He's a consultant and analyst to companies large and small, as the owner of Melbourne-based PivotNine Pty Ltd. He also writes about the business of IT, with particular interests in infrastructure, security, open source software, and marketing.

www.eigenmagic.com



Kate Carruthers @kcarruthers

Kate is Chief Data Officer for UNSW Sydney, and an Adjunct Senior Lecturer in the School of Computer Science & Engineering at UNSW Sydney. She is a member of the Telstra Industry Advisory Board and the NSW Government's Data Analytics Centre Advisory Board. She has extensive experience in senior executive roles for diverse organisations including Citibank, General Electric, AMP, Westfield (now Scentre Group), and NSW Treasury. katecarruthers.com



Paul Wallbank @paulwallbank

Paul Wallbank is a speaker, writer and broadcaster who has been helping businesses and communities deal with technology and change for over twenty years through his presentations and consulting services. paulwallbank.com



Stilgherrian @stilgherrian

Stilgherrian is a freelance journalist, commentator and broadcaster who covers the politics of the internet, cybersecurity, cybercrime, and privacy. He studied computing science and linguistics before a wide range of media and technology work. He currently files for *ZDNet*, *Crikey* and others, is a frequent guest on radio and TV, and was technology consultant for the recent ABC TV drama *The Code*. stilgherrian.com

002.A2

About DirectorTech

Who we are, and how to find us.

DirectorTech is a regular advisory aimed at company directors of government entities, listed companies, private organisations and not-for-profits. The content for each advisory is researched, analysed and written by a diverse range of international contributors, each expert in their field. Advisories include written content specifically tailored for company directors and individual interactive webinars which focus on identified organisational issues.



Nigel Phair, Managing Editor and Publisher @nphair

Nigel is an Adjunct Professor at the Centre for Internet Safety at the University of Canberra, and is an influential analyst on the intersection of technology, crime and society. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.



DirectorTech is an initiative of the **Centre for Internet Safety** at the University of Canberra.

Web: directortech.com.au

Email: admin@directortech.com.au

Phone: +61 408 437 056

Twitter: [@director_tech](https://twitter.com/director_tech)

Centre for Internet Safety
University of Canberra ACT 2617
Australia

ABN 28 150 165 343

DirectorTech is ©2017 Centre for Internet Safety. All rights reserved. Copyright in individual contributions is retained by the authors. Cover and internal digital illustrations ©2017 Stilgherrian.