trowers & hamlins

thinking Business

ISSUE ONE

Contents

Welcome to our first edition of Thinking Business - where we aim to share our expertise and ideas with you to support growth and sustainability for your business.

Change is normal for any business. But the pace of change in today's world means businesses must be more adaptable and innovative than ever, and having the support in place to access specialist advice can often make all the difference.

One of the topics on everyone's lips in the business community, of course, is Brexit, and perhaps the real challenge will be how we respond to it: how we adapt to the inevitable changes, and where we look for new opportunities. If you'd like more on Brexit, we have a separate publication, so please visit www.trowers.com/Brexit or drop us a line, and we'd be delighted to give you our thoughts.

For this first edition of Thinking Business, though, we've decided to focus on some of the more day-to-day issues we come across when talking to clients:

- Family businesses – family businesses account for the vast majority of UK small and medium enterprises, but face a range of issues, from succession to tax treatment to intellectual property. We look at each topic from the perspective of both owner-managers and investors.
- Cyber-security – cyber-hacking is just 3% of the problem, IT risks are much wider – how well-informed are you?
- Private capital in health and care – proper care provision will depend on getting private capital more heavily-involved. We discuss some of the opportunities and pitfalls.

We hope you'll enjoy reading this – we've tried to write it in the way we like to talk to our clients – unstuffy, pragmatic and real conversation. So, please get in touch with any of us directly at thinkingbusiness@trowers.com with any questions or comments, and follow us on twitter @Trowers.

SEPTEMBER 2016

PRIVATE CAPITAL IN HEALTH AND CARE CAN BE AN ALL-ROUND WINNER

The UK is entering a period of unprecedented political uncertainty, and there is nothing of greater concern to investors than uncertainty.

And yet capital needs to make a return, so reliable investments in growth sectors will be at a premium in the next few years. Health and social care are two of the safest bets around, according to the corporate team at Trowers & Hamlins, which has a longstanding reputation advising investors and operators in these complex, interlinked and heavily-regulated sectors.

Private equity is already quite active in the Care sector, where long-term residential care beds are expected to rise from today's 450,000 to 780,000 by 2040, taking sector revenue from £13bn to £44bn, but a few investors have had their fingers burned.

"The key thing for investors in the Care sector to be thinking about is reputational risk," explains Tim Nye, corporate partner in the firm's London office. "Now, you might think you know what that means, but in Care, risks can be magnified out of all proportion, because vulnerable people are involved. As an investor, you back a management team to do their jobs, but Care is heavily-regulated and can get a lot of press attention, so you need to keep a very close eye on what is going on in the homes you're operating."

Fellow corporate partner Alison Chivers agrees. "It's very important to have good regional management," she says. "Referrals into a care home will be from the locality, and while a big scandal might hit the national press and affect your reputation that way, other incidents might not make the nationals but might be big news locally, so it's important the investor is on top of things wherever they have assets."

> **"Reputational risk needs to be managed proactively," says Nye. "Spending money on setting up a separate quality assurance board with independent assessors – not just your CEO or operations director – makes good commercial sense. You shouldn't just see it as an additional cost item."**

The Care Quality Commission has the responsibility of regulating the Care sector but as Nye explains, if a CQC visit results in an inadequate (or worse) rating, "local authorities have a duty of care, and may well embargo referrals to care homes they or the regulator judge inadequate. That will affect your ongoing income stream, and have an effect on your exit too, it can become a vicious circle and so it's best to avoid that happening."

"The CQC has a very broad remit," Chivers explains, "and they're stretched in terms of time and resources, so relying on their – infrequent – inspections to alert you to problems is going to be far too late. The prudent investor is going to make sure that doesn't happen in the first place."

Another of Chivers and Nye's recommendations is to set up a whistleblowing hotline for staff. "Whistleblowing is one of those things some employers run scared of," says Nye, ", but you need to think about it as a vital early warning system, an insurance policy for your investment."

Long-term residential care is the sharp end of the Care sector, but with the UK's ageing population, housing with a care element can be a much more cost-effective, and less dramatic option. Nye and Chivers see considerable potential for retirement communities, a very popular option in the US but thus far an idea which has seen relatively modest activity in the UK.

"Retirement communities can free up housing stock, take care back into the community and put much less pressure on the NHS," says Nye.

"They're great," agrees Chivers, "when they're done right, but developers and operators need to think about creating true living experiences with amenities that are appropriate to the specific locality and

demographic being targeted. It cannot be a one-size-fits-all model - not everyone in retirement wants their day to be filled with endless group activities. Research has shown that most people don't want to move more than three or four miles from where they've been living, so there's a need for these communities everywhere in the UK."

While Care has for some time been a focus for private equity interest, partnering with the NHS has been slower to crystallise other than in some discrete areas, primarily due to political factors, but the team see change on the horizon in the Health sector too.

"The outlook for private investment in the Health sector is very positive," says Chivers. "The NHS is facing a very difficult financial climate, and everyone knows that something has to give. Hospital beds remain one of the most expensive items, but we all hear the stories in the press of bed-blocking, with beds being occupied by people who don't really need to be there, for instance those waiting for an operation the next day or those who are convalescing after a procedure and require monitoring rather than clinical input."

"In Scandinavia, the concept of patient hotels is well known and popular," she explains.

A patient hotel creates additional bedspace, not just for patients but also for their relatives, with the creation of purpose-built accommodation on hospital grounds, using private capital for the build, and creating an income-stream for developers.

"There's capacity for a massive cost-saving," says Nye, "because you need very few nurses in a patient hotel. Admission is according to medical assessment, and anyone needing to be in hospital still goes into hospital, but in the patient hotel, there will be other, regular hotel staff and care assistants. It's much better for patients, they get their own room – which is not always possible in hospital – often room service, all the creature comforts such as a TV, and there is none of the anxiety of being in hospital."

So far there are just a handful in the UK, something Chivers and Nye see changing, but there are obstacles.

"One of the major sticking points is that NHS Trusts don't want to pay for voids – unused rooms – whereas if you're an investor expecting a particular income stream, you need a degree of reliability," says Nye. "So there are discussions to be had there, and it may involve some degree of central government underpinning."

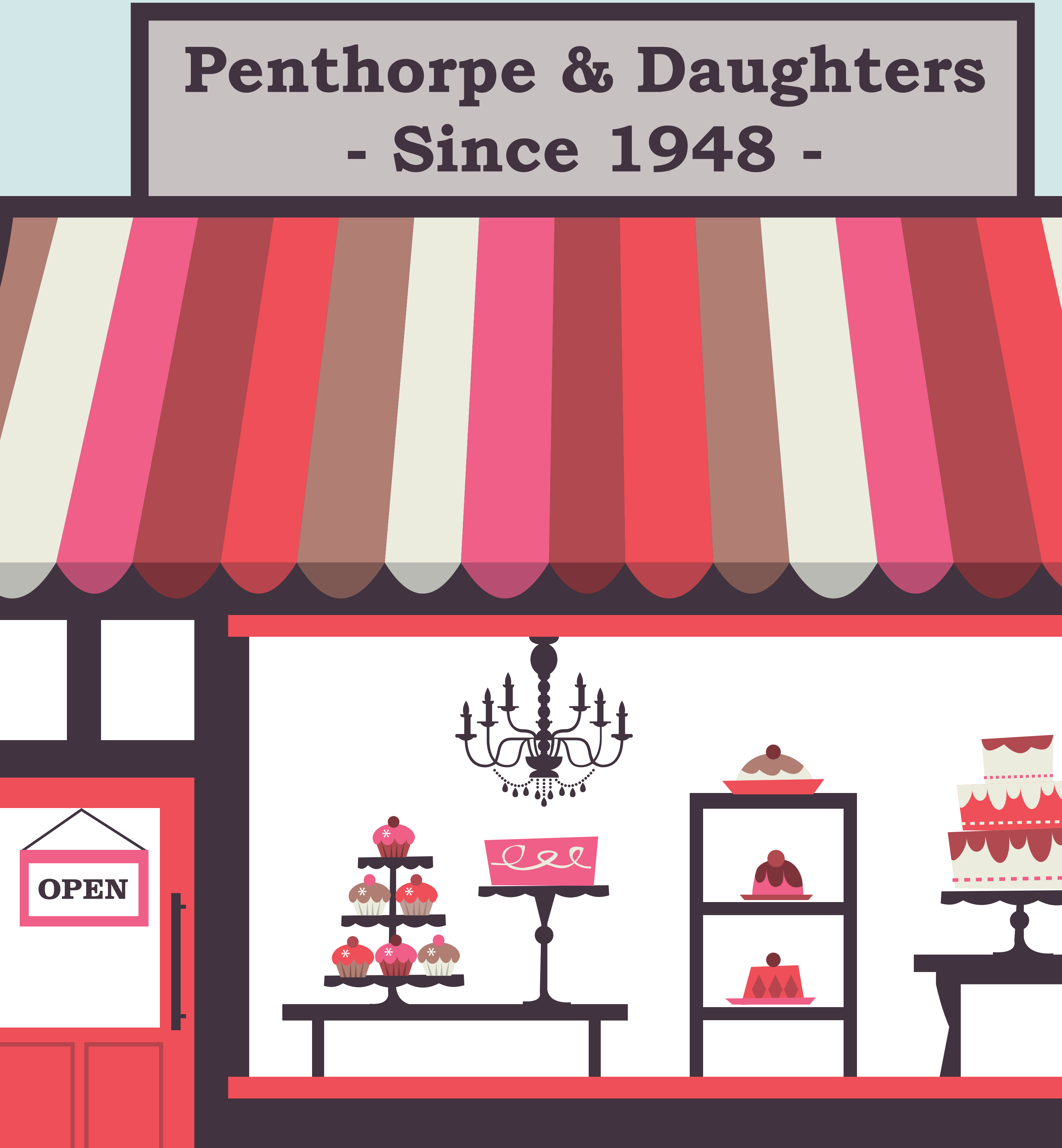
"Another problem is that you're not just dealing with one bloc that is 'the NHS'," says Chivers. "You're needing to deal with individual trusts, and they're all under financial pressure and nobody wants to be one of the first to move on this, relatively untested idea, until some others do it. But it will happen, it just makes so much sense for everyone involved."

As positive the climate, and reliable the rewards may seem to be, investing in health and social care is not for everyone.

Nye recalls one instance in the health sector, where a client bought a mental health services hospital in a 'fire-sale' from a company in distress. "Because the price was so low, they wouldn't give any warranties," says Nye. "We had to reverse-engineer the transaction to protect the buyer, put down a deposit so we could get in to the hospital to see what was happening on the ground and verify the limited information we had been given. To ring-fence risk we then created a separate structure into which we could decant the assets and manage the liabilities. We had to close down the old, distressed company and create a new one. All the while there were patients to think about, so we had to arrange transfers to the buyers other facilities and there were redundancies while our client built a new mental health unit on the site with staff either applying for transfers to other hospitals of the buyer or re-applying for what were effectively their old jobs in the new company once the facility was re-opened. There are a lot of angles in that kind of deal."

Chivers points to clients also needing to take care in Care, as it were.

"We had one client, already active in the Care sector, who had found what looked to be a great, cheap asset, a care home owned by four members of the same family, and they wanted to do the deal quickly," she recalls. "Six months later, we were still doing the deal. Every corner we turned, we found something else to worry us: financial information that wasn't supported; non-existent corporate records; looking at the Company's assets only to find out that those assets were legally owned either by another company which the family owned or by the members of the family personally; vehicle leasings done through the company that the Sellers wanted to keep because they couldn't get personal credit for a car, stuff like that. We got it done, nothing was insurmountable, but it was a bit of a nightmare. The lesson is that if something looks too good to be true, it just might be!"


Penthorpe & Daughters
- Since 1948 -
OPEN

The Descendants

When we usually think of ‘business’, we naturally think of big business, household-name brands or headline-grabbing FTSE100 companies.

And yet the backbone of British business is not the major multinational, but the family-owned business. Family-owned businesses comprise two-thirds of the total of UK SMEs, according to research by the Institute for Family Business, generating 35% of private sector revenue, or £1.1trn.

There are family-owned businesses in practically every sector, but certain patterns and challenges are common throughout, and a key one is the issue of succession.

“There’s that old saying about ‘clogs to clogs in three generations’,” says Caroline Hayward, intellectual property (IP) partner at Trowers & Hamlins, adding that IP is one of the issues most-overlooked and which can cause most problems down the track for family businesses.”

“Some bright chap with nothing – the first set of clogs – sets up the company initially, becomes incredibly successful, passes it onto his kids who respect what he’s done and do a great job growing the company, but then their kids have only ever known wealth and don’t understand the work ethic which made the company, which then declines and then the third generation end up back to clogs!” she says.

Corporate partner and Islamic finance specialist Tony Poole also sees successful succession as one of the major challenges for family businesses. “People often leave it too late to think properly about it, or make assumptions that one child or other is going to take it over, and they may not be that interested or may not be the best person for the job,” he says.

“The figures are quite stark,” he adds, echoing Hayward’s point. “A survey by PWC found that 48% of family firms in the UK currently have yet to identify a successor, and estimated that 172,000 family businesses a year leave family control entirely because they fail to resolve the succession issue.”

“Problems are also created if the founder wants to step back from the day-to-day management of the business, maybe to give the kids a chance to take on management responsibility, but then wants stay on in some capacity” adds Poole. “That can cause all sorts of tensions. I would advise not sharing out the equity too quickly and certainly not losing control of the company until you’re ready to hand over entirely.”

"Beyond that, where there are a number of shareholders, all the children, for instance, you want to make sure there are appropriate measures in place such as powers of attorney, to ensure someone can take over if something bad happens to one of the shareholders, or 'drag-rights', so that a minority shareholder can't just dig their heels in and prevent a deal that all the other shareholders might want," he says.

Creating a sustainable and successful business is problematic whatever the structure, but Adrian Jones, corporate partner in the firm's London office, adds that the nature of growth in family businesses can also present major challenges.

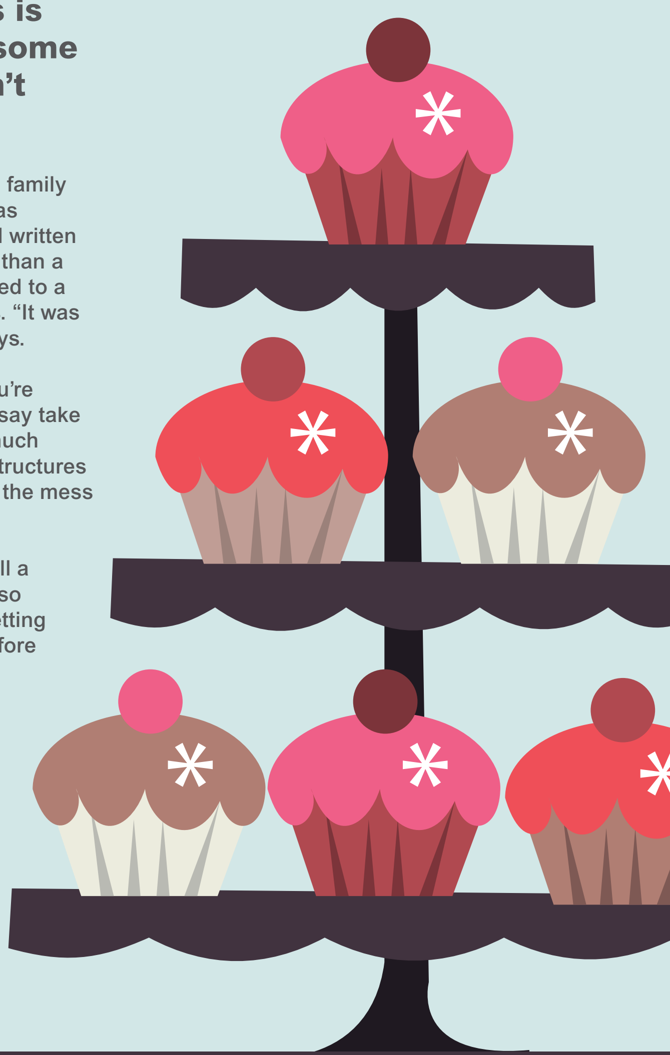
"Very often you'll get a situation where the business has started quite informally," he says. "It is started and runs successfully for a number of years on that basis, and it's only when it comes to an inflexion point – say where the business is looking for external investors, or perhaps a sale to a larger business or outside investor – that you discover that everything is all over the place. There are no written contracts, IP rights aren't registered or are registered to a founder, multiple premises and other assets have different ownership."

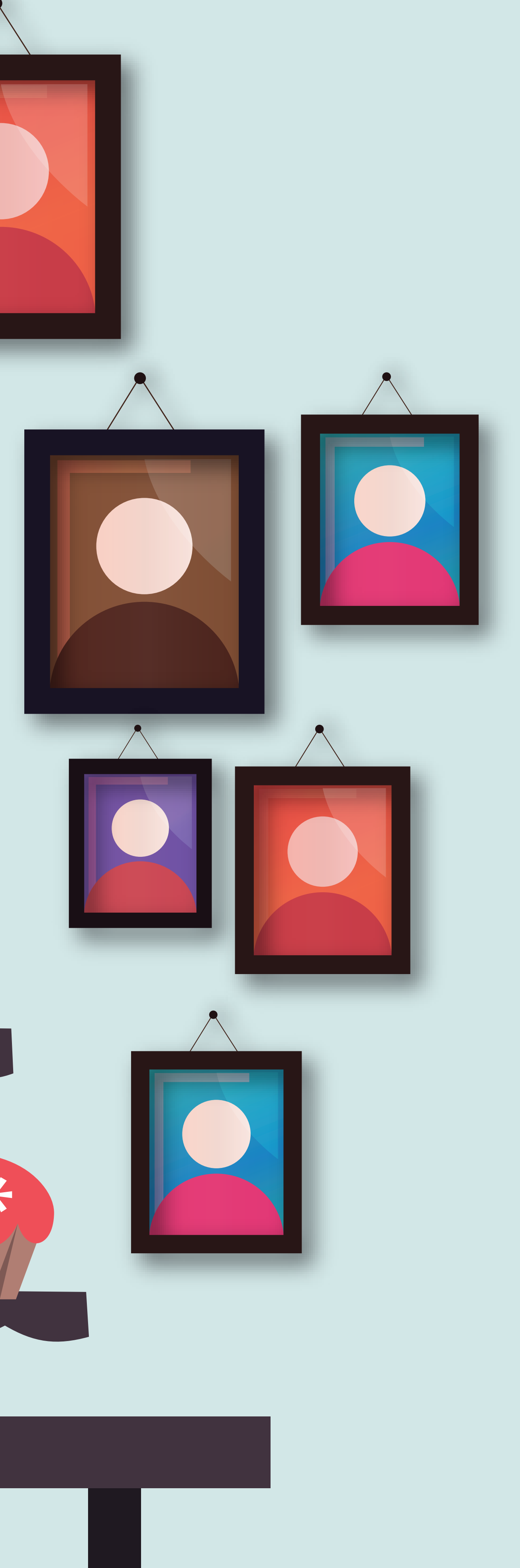
> **"Some people think 'oh, we're family, we work on trust and don't need contracts," agrees Caroline Hayward. "But you need contracts in place, and which are the same as the contract you would have, as if, this is not your brother but some external guy you didn't really know."**

She relates the tale of a family and family friends company "which in 1993 was organised on the basis of trust and written agreements which were little more than a handshake", an informality which led to a dispute which went on for 12 years. "It was like a grumbling appendix," she says.

"I'm sure people would say 'oh, you're lawyers, of course you're going to say take advice early'," she adds, "but it's much easier and cheaper to put proper structures in place at the outset than sort out the mess down the track."

"It's going to be very difficult to sell a business in the midst of litigation, so you need to start thinking about getting everything in order a good year before you're going to sell."





WHO OWNS YOUR IP?

Intellectual property can be a tricky area for the family business. For a start, who owns the name?

“If your business is John Jones Ltd, set up by your grandfather John Jones way back when,” says Caroline Hayward, “and then the grandson – also John Jones – wants to break off and set up his own business as John Jones Ltd, you probably have a problem. That’s why, and it’s sad to say this, trust is never enough when it comes to family. You just can’t rely on situations like this not cropping up sometime in the future.”

“IP ownership in itself can also be an issue,” says Adrian Jones. “If you’re a software company in particular, it’s wise to check whether some of your programs were written by people who were contractors when they worked for you. If that was the case, then you might not own the IP. Copyright originates and remains with the author, unless it is assigned.”

“IP is often the last thing a family business might think about,” adds Hayward. “They’ve got enough to be getting on with, keeping the business running. But it’s vital to get everything registered that you need registered, and make sure you’re clear on ownership. You don’t want to have to be sorting that out in the midst of succession or sale.”

Caveat emptor

Given that the majority of SMEs are family businesses, navigating a few quirks is par for the course for any purchaser.

However, the lack of formal contracts, poor administration and unconventional wage-arrangements occasionally arising when business has grown from the kitchen table can be offputting, says Adrian Jones.

“We had a situation a few years back where we were acting for a multinational looking to buy a UK business which had been a sub-contractor of the acquirer for years,” he says.

“But the target company was in a complete mess. There were irregularities in the accounts, people were paid in cash, company cars were registered to individuals, purchase receipts were just stuffed in carrier bags in the office. The buyer pulled out, not surprisingly you might think, but it also left them questioning the underlying commercial relationship – were they confident having these guys working for them as a sub-contractor?”

But it’s not just poor administration that puts a purchaser off. Sometimes there might be a ‘poison pill’ for a potential acquirer, as Jones explains. “There might be a change of control clause in a major supply contract, for instance, so it’s important sellers consider such issues before engaging in a sale process.”

One other instance Jones recalls involved the purchase of a company which relied on a number of substantial fixed term contracts.

“The business was sold at a time when a number its key fixed term contracts were coming up for renewal. The director sellers were on a six-month earn-out which expired before contracts were renewed. Of course, they all left after six months, and all the contracts expired and were not renewed.”

“Quite often it’s the assets of the business themselves which cause problems,” adds Tony Poole. “We’ve seen situations where a family business has managed to acquire all kinds of things down the track, yachts, a ski-chalet, and then when they came to sell, it turned out assets were owned or part-owned by individual shareholders. Sorting all that out can be a real mess, and can hold up or even end a deal entirely.”

BUYOUT OR SELL-OUT

Entrepreneurs' choice?

Continuation of a family business through succession may not be possible, or even desirable, and many owner-managers set up not to create some kind of family dynasty, but with the express purpose of selling it, either to retire or to go off and do something else.

SMEs are of growing interest to the private equity industry, according to a recent survey by Cass Business School and Lyceum Capital, which found that deals below £50m – the largest proportion of SMEs – accounted for 80% of all private equity buyout activity in the UK in 2015.

Nick Harrisingh, corporate partner in Trowers' London office, finds himself acting for a lot of what one might term 'classic' entrepreneurs contemplating selling up.

"They've started the business right out of university, grown it, and now want to sell and go off and do something else," he says, "and very often they sell out to a bigger rival or a private equity house, and there will be an earn-out. That change in role can be quite challenging. They have been used to being the dominant, driving force in their company, and now the company might be taken in a different direction. That can be challenging for both sides."

Fellow corporate partner Ian Dobinson agrees. "There can be a conflict between meeting the financial targets of the earn-out and the wishes of the new owner, which may be more long-term."

Dobinson often finds himself looking at things from the vantage point of the acquirer, frequently a private equity provider.

"So much of the successful acquisition depends on the financial arrangements," Dobinson notes. "Quite often the founder will have given shares to the people around him, or made promises behind the scenes to 'see you right' when the deal is done, and so you suddenly have all these people working for the business who come into a chunk of money. Now, if you're the investor buying that business, how do you ensure that people remain motivated when they've just received a large amount of money?"

Money, of course, remains at the root of any entrepreneur's decision to sell, and in particular tax. Few people are happy giving the government a significant proportion of the profits of a sale where they feel they have put their blood, sweat and tears in over the years.

Hence Dobinson and Harrisingh recommend that entrepreneurs keep a keen eye on the availability of Entrepreneurs Relief – tax relief on Capital Gains Tax when selling your business, which can mean you pay as little as 10% on the money you make when you sell.

"Last year there was a feeling that the Chancellor had made this a bit too generous," says Dobinson, "and that was creating the wrong kind of incentive."

"We did think he was going to row back a bit," says Harrisingh, "but Brexit may have changed that. I suspect the new Chancellor is going to want to give the impression that Britain remains open for business."

NOT JUST HACKERS IN HOODIES

When it comes to areas of business risk, those associated with IT are front of mind, at least where big business is concerned.

Technology risk topped the poll in leading insurer ACE's Emerging Risks Barometer 2015, a survey of 500 executives in large and mid-sized companies in 25 countries. Among the risks, hacking or technological attacks which cause service disruption were of greatest concern (33%), with data theft by staff (23%) and theft of intellectual property (18%) some way down the list.

It is an issue," says Riccardo Abbate, corporate partner in Trowers & Hamlins' London office, and specialist in technology, "that when people hear the words 'cyber-security' or 'cyber-risk' they typically think of 'hackers in hoodies'."

"In fact, hacking, in the sense that it's so often featured in movies and TV series, that of deliberate intrusion by a determined individual or group into a computer system for 'sport' or the demonstration of intellectual prowess, is a tiny part of the picture – just 3% of the total," he notes. "The truth is much more mundane and/or organised for criminal financial gain, and therefore much more dangerous to businesses in the real economy."

And while big business may have the big systems and therefore may be expected to suffer the greatest risks, the ubiquity of technology means risk can happen anywhere.

"We are all dependent on our IT, these days," Abbate adds. "And if you're running any kind of business, your attention to technology is vital."

"SMEs are particularly vulnerable," according to fellow corporate partner Adrian Jones. "They don't have the resources of larger companies either to have IT specialists in-house or the time or cash to spend trying different solutions. And there are criminals who specifically target SMEs because they're easier."

While a cyber-attack or hack can be devastating, technology risks comes in a number of different flavours.

"As well as intrusion into systems, either to steal data, or simply to use network resources, which will commonly may be the unauthorised action by a employees or former (disgruntled) employees," says Abbate, "there is also the simple failure of systems – hardware or software – and potential corruption or total loss of data. 'Cyber', to me, is therefore about resilience in the first place, and recovery in the second. Whether you're using IT primarily for computational, informational or archive reasons, are your systems resilient enough, and if they fail can you continue in business and do you risk any permanent losses?" Unexpected IT system outages are more common than systems hacks, after all.

The true cyber-risk, then, is more a function of lack of thought and preparedness than direct action by the kind of social misfit/ computer genius recently seen in Amazon's hit series 'Mr Robot'.

"A lot of companies will have policies on social media, what their employees can post on Facebook and Twitter," says Adrian Jones, "and people are increasingly wise to clicking on a link in an unknown email. But how well do you control access to your system? It could be a consultant working for you on a temporary basis who downloads or accidentally transfers something via memory stick, or it could be much worse."

"We had one client, some years ago, who were visited by a Chinese company they thought they could do business with" he recalls.

"One of the visiting delegation asked if he could access the internet, so of course they allowed him to use a terminal. It was subsequently discovered that he had uploaded a 'sniffer' (a type of spyware which targets specific data) which gave the Chinese company access to all their designs, pricing details and customers."

"Of course, it's very important to have good policies and procedures in place," says Abbate, "but there will always be human error. You can't guard against everything, but you should at least try to guard against everything you can, because your entire business could be at stake. So, ensuring that you have appropriate procedures that are supported meaningfully by the requisite resource is key to managing an organisation's cyber-risk."

"And just because you think you have something in place, it might not be what you think it is or what is appropriate given the operational circumstances of your business," cautions Jones.

"For instance, you may have offsite data recovery, but it's important to ask questions there," he says. "The company may be based in Dagenham, but its own disaster-recovery might be in Singapore or the US, and that has implications for data protection. Life is never as simple as thinking 'I'll just do what the IT suppliers say and everything will be fine'."

Getting insurance is a natural consideration to add to the cyber-risk management 'tool box', but that may not be the comprehensive solution that it might appear to be. "The issue there is that the policy might be inadequate or useless if its scope and terms have not been procured properly to reflect the circumstances relevant to your organisation", according to Abbate. "The risk is that you get an insurance policy which you think covers you and you think 'ah well, that box is ticked' and move onto something else, and find out later when the cyber event occurs that you do not have the cover you thought you did" he says. "It is always useful to liaise with your insurance brokers and your legal advisors in such regard. But insurance (even if properly selected and procured) is only ever part of the solution: if disaster strikes and you've permanently lost sales records or customer data it might be impossible to continue in business. Financial compensation is no substitute for having robust systems and proper backups."

TEN TOP TIPS ON CYBER-RISK

1. Make sure all your staff understand policies on social media, use of data and email.
2. Insurance, yes, but check what it covers and make sure you declare everything you need to, or the insurer can void your policy.
3. Insurance can't restore lost data – make sure you have backups and good disaster recovery processes in place.
4. Make sure you control access to your system – including contractors and visiting 'clients'. Nobody should be putting memory sticks into your network! 'Bring your own device' facilities need attention to ensure that confidential information does not leak outside of your organisations control.
5. If you use Software as a Service (SaaS) products, make sure you make get periodic data downloads which reflect your needs – week-old data may be no good at all.
6. Offsite disaster recovery, fine, but check where their offsite is. If outside the European Union you may – as things stand – be at risk of infringing data protection rules.
7. Hacking is 'glamorous' and high-profile, but is actually rare. Organised and well-resourced criminals are making it their business to extract data for sale to competitors and/or to hijack systems for ransom. Make sure you understand the real risks to your business, on data, software and hardware.
8. Check what data you are processing and who is processing it – you might be sharing data without knowing about it. There may be service or contract terms which allow use of your data by a third party.
9. Change passwords regularly and ensure that staff are required to use strong passwords.
10. Do not use passwords for work that you use for personal accounts.

trowers & hamlins

trowers.com

London —— Birmingham —— Exeter —— Manchester —— Abu-Dhabi —— Bahrain —— Dubai —— Malaysia —— Oman