IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Ian Brown

Carol Baker

As Integrity360 announces a major strategic investment from leading private equity firm August Equity, we talk to Ian Brown, Executive Chairman on his new role at one of the UK and Ireland's fastest growing cybersecurity specialists, and how he plans to expand Integrity360 ready for the future.

***Ian Brown** is the Executive Chairman of Integrity360 (https://www.integrity360.com), one of the fastest growing cybersecurity service providers in Europe. Ian is also Chairman of Tailor Made Technologies and Air IT, both IT services providers. Both Air IT and Integrity360 are backed by August Equity.*

Previously Ian was Executive Chairman of SecureData, a private equity backed cybersecurity services and solutions provider where he led the turnaround, growth and highly successful sale of the business to Orange, returning circa 7.5 x money.

Ian has operated as a CEO for over 20 years, working in partnership with private equity institutions. Until 2014 he was CEO of Axell Wireless, a company he created in 2007 through the acquisition and merger of AFL from the UK, Avitec AB of Sweden and Dekolink of Israel. Ian developed Axell into one of the world's leading manufacturers of wireless coverage and management solutions, exporting products to over 150 countries and operating from a network of 16 worldwide offices. In 2013 Axell was acquired by Cobham plc for £85 million.

Prior to Axell Ian was CEO of Redstone plc, a circa £100 million LSE quoted telecoms services provider, where he led the rescue and transformation of the group. Previously in 1995 Ian created Fastnet Group, which grew to become one of the UK's leading independent network and communications services companies. Fastnet was sold in 2000 returning private equity investors 10 x money. Ian has also served as the Chairman of GCI, a UK managed IT/cloud services provider which was backed by the Business Growth Fund.

Ian is highly experienced in handling both growth and turnaround situations, all aspects of M&A, strategy, general management, mentoring and leadership.

Background on Integrity360 and Ian's role

Integrity360 is a well-established cybersecurity practice, especially in Ireland, where it is the overall market leader, and has a growing presence in the UK. It is also what I would call an end-to-end cyber services business.

You will find some cyber businesses just do security assessments, or just supply the infrastructure, or just do a bit of managed services. One of the benefits of Integrity360 for our customers is that we are a 'one stop shop' for all of that. Increasingly, we find that this message is appealing to customers, because they don't want different suppliers who provide different aspects of cybersecurity and prefer a more joined up approach.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Integrity360 is a dedicated cyber services company. If you did a map of the European cyber services landscape, you would not find many companies that have that broad end-to-end capability. This makes Integrity360 something of a rarity, and this capability is one of our biggest strengths.

Through the investment with August Equity we intend to accelerate the company's already pretty impressive growth and expand rapidly around the European market and also further in the UK. Target markets include the Nordics, Central Europe, and Southern Europe.

Our aspiration is to take the company from where it is today at circa €45 million in revenue, up to around €200 million in revenue, as fast as we can. We are planning to do that by becoming a European market leader.

At the moment, we are already a market leader in Ireland and an established player in the UK, but we're not operating in other countries around Europe. To turn our plan into reality, we will be focusing on even more aggressive organic growth coupled with some further acquisitions.

Why did you select August Equity as your equity partner of choice?

August Equity is a very well-respected equity house and one of the leading mid-market private equity firms in London. It invests in a wide range of different companies including technology, healthcare, education, and business services. August Equity has a specialty – adopting a 'buy and build' approach. That involves taking a company that has a quality proposition, and helping that company grow into an overall leadership position, through making further acquisitions and integrating them.

Also, I have worked with them personally for five years, so we know each other very well. I've been working with private equity firms for the best part of 30 years now. When I first started there were maybe only 25 private equity firms in London; now there's over 350.

August Equity was previously the major shareholder in a cybersecurity business called SecureData, which grew to become the UK's leading independent cyber services practice. I ran that business as the executive chairman before the company was sold to the Orange Telecommunications Group in early 2019. It's now part of the €40 billion Orange empire.

So, August Equity not only has expertise in buy and build methodology, but also has expertise in the cybersecurity space. SecureData was a very highly successful investment for August Equity.

What sort of acquisitions are in your sights?

In terms of acquisitions, we're looking at players in other key European markets such as the Nordics, Italy, or Central Europe for example. For us, it doesn't particularly matter if those companies do not have the breadth and depth of skills of


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Integrity360. They may only have part of the service portfolio we have, but we can take them on a journey to expand their services, as they become part of our group. For example, we might buy a business in Scandinavia that has great professional services expertise, but they haven't really developed their managed services cybersecurity proposition. As we have already done so we are well placed to help them set that up and roll out that service to those local customers.

Integrity360 has a big reputation for supplying high quality, highly skilled services. We are not at the bottom end of the market When acquiring companies, we look for those who have a similar quality and attention to detail outlook as ourselves with respect to cybersecurity services.

Can you tell us about Integrity360's role with Managed Services?

Integrity360 focuses on both mid-market and enterprise customers – which include several of Ireland's leading banking organizations. Mid-market companies include regional airlines, airport authorities and local authorities, through to medium sized law firms, and pharmaceutical companies.

Our specialty is really providing quality sophisticated services for organizations that need to take cybersecurity seriously – because of regulation or compliance, or just by virtue of the kind of data they are holding, for instance highly confidential data that they need to protect.

Very often, when a new customer comes knocking on the door, one of the first services we might offer is a security assessment, where we do some consulting work which enables us to say to them, "here's where we think you are in your cybersecurity journey". Quite often for many companies, this can be very revealing and can also in some cases be quite horrifying because they realize that they've got quite a lot of holes in their IT estates, and they're not as secure as perhaps they thought they were.

In some cases, during the cybersecurity assessment work we will simulate doing an attack. What we call a red team assessment. This is where we basically act as a bunch of bad guys and try and hack into the company's infrastructure and see how far we get. One of the things I can tell you is that in 99% of cases, we breach the company's infrastructure.

Then we analyze the results. How did we get in? What was the vulnerability? What was the issue, where is the gap? That quite often then leads to remedial work. Then, sometime later, we may do another assessment. This is because for many businesses their IT estates are not fixed – they evolve over time. They grow and expand as the customer acquires other companies and opens offices, and in so doing, creates other potential vulnerabilities. This means security assessments and red team assessments are services that need to be done on a continuous basis.

Likewise, we can set up a secure infrastructure around corporate networks, deploying firewalls, email and web monitoring, to make sure emails are not going to peculiar places and employees aren't accessing websites that are known to contain viruses or malware.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

On a managed service level we might just be looking after the maintenance and support of the infrastructure, for instance, the firewalls, through to "threat hunting" where on a 24/7 basis we work to spot vulnerabilities and investigate potential security issues. If you look at one piece of data by itself, you might not think anything is going on, so you need to have the ability to join up the dots. So you spot something going on in one part of the corporate network, and you spot something going on in another part of the corporate network, and in isolation they don't amount to much but if you put them together, you can see an attack is underway, so we provide the remediation on those issues as well.

In a sense, our customers are almost giving us the keys to their security infrastructure and asking us to handle it for them – and companies don't do that lightly. Obviously, trust is a very big thing.

Do you see an end to the skill shortage currently affecting the IT industry?

There is currently a colossal skill shortage. Many end user companies are finding it very difficult to hire people, experts, consultants, engineers, who do this work for them – and if they do hire them, how do they keep them?

We are constantly hiring people and developing our staff. IT engineers generally like to work for people in the trade because the work is more varied than if you work in an end user environment. For an end user customer, it can be quite challenging to hang on to people. So, a lot of companies are turning to Managed Service Providers (MSPs) such as Integrity360 who are also able to provide cybersecurity managed services. This is a big growth opportunity, because the issue is not going away any time soon.

Are organizations taking cybersecurity seriously?

I remember when GDPR came into force a few years ago, I was certainly having conversations with directors in companies and saying to them, "if you got hacked, or you had a security incident this afternoon, or one of your IT people said, we think some of our data may have been stolen, what would you do?" And, you know, 90% of them at that time didn't have a clue. Today, 50% of businesses still don't have a clue. They are not talking about cybersecurity in the boardroom.

Now under GDPR if you get hacked and personal data is stolen, you must report it to the relevant regulator within 72 hours. One of the first things the regulator will ask is, "well, what was your plan?" If you haven't got a plan, you are going to have a problem. It's a good idea to have a plan, and it is something that we're constantly educating customers on. Not necessarily the larger customers, such as banks for example, but quite a lot of mid-market companies who may not think that they are going to be attacked. Some businesses are unprepared. All organizations should take cybersecurity seriously.

What impact has working from home had on cybersecurity?

During the pandemic, cybersecurity attacks increased. This was because people are used to accessing company resources while being on the company corporate

network in the office. When everyone started working from home, suddenly they were accessing corporate resources from their bedroom, their kitchen table, the dining room, and in some cases accessing those resources using their own devices, as opposed to company devices.

The thing about cyber is that it is not something that you can just do once, and it is done. It is something that constantly evolves. Every week operating systems are in development, new code is being written, upgrades made, new software launched, and to a degree everything has a vulnerability in it – a backdoor that someone hasn't plugged properly. Or, if it was plugged, it had to be implemented in a certain way, and it hasn't been done appropriately.

Therefore you have to constantly invest in cyber. Your IT estate is constantly evolving. Organizations are constantly adding new systems, such as an HR system, or a new ePOS system, for example. With companies now accelerating their digitalization, the downside of relying on digital tech is cybersecurity. So, you need to make sure you handle it, and handle it well. It needs to be a topic of conversation on a regular basis for the senior leadership of the business.

As companies start moving staff back into the office, what advice would you give to those now needing to deal with the hybrid workforce?

During the last 18 months or so, people went from everyone being in the office and accessing corporate resources in the office, to accessing corporate resources at home through unsecure Wi Fi networks using their own devices. It's not surprising that there were breaches.

Under the new hybrid model, the challenge for the IT team is larger because you have got to design systems and cybersecurity policies capable of operating in both environments. There is a balance between having everything so locked-down that it basically forces a data protection policy that says, for example, any email that goes outside the business is checked by someone else. It simply isn't practical. So, there are always some trade-offs.

The benefit in organizations working with cybersecurity partners like ourselves is that we get to see this, across multiple estates, across many different types of customers. We get a very good view on what works, and what doesn't work. What works in practice versus the theory, and what is appropriate for certain types of businesses. What is manageable, and what is enough to make sure that they tick the boxes for the regulator, but doesn't impede them from growing their business.

What is a closing thought you would like to get over to our readers?

Don't be complacent over cybersecurity. It's not just the inconvenience of personal data being stolen, or the hurdle of dealing with the regulator, but imagine what that does for your business's PR. It takes a long time to repair reputational damage. Once your customers have got a certain impression of you, they lose confidence in you. It takes a long time to get that back. So that's why I say: "Just take it seriously."