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 with Dermot Williams

Carol Baker

Cybersecurity specialist, Threatscape (https://www.threatscape.com) has just won Microsoft's Security and Compliance Partner of the Year award. The company was honoured among a global field of top Microsoft partners for demonstrating excellence in innovation and implementation of customer solutions based on Microsoft technology. We ask Dermot Williams, Managing Director at Threatscape what he believes has contributed to the company's success.

Dermot Williams is the Managing Director of Threatscape (https://www.threatsacpe.com).

Prior to establishing Threatscape, Dermot founded and led Systemhouse Technology, a pioneer in understanding the emerging threat of computer viruses.

Over two decades Systemhouse grew to become one of Ireland's most successful providers of IT security solutions. In 2004 Dermot sold Systemhouse, but reacquired it in 2010 when Threatscape bought its assets.

Dermot is a frequent speaker on technology topics on TV, radio and at conferences, particularly those related to information security and digital privacy.

Congratulations on winning the coveted Microsoft Global Security and Compliance Partner of the Year award. How many companies were you up against to get top place?

As a pure play cybersecurity company, the only category that Threatscape was entered for was this award – and we won! We were up against 3,300 partners in over 100 countries around the world, so I am amazingly proud of the team and all that we have achieved.

Of course, in normal times the winners would have been in Las Vegas in August, up on stage in front of tens of thousands of people at the global Microsoft conference being presented with the award, before attending an executive dinner with Satya Nadella, CEO of Microsoft – all set against the backdrop of the entertainment and lavish meals that Vegas can provide. Instead, we had a virtual video award ceremony– although we have received some scarves via Fedex – but it doesn't quite have the same impact!

But regardless, it is a tremendous achievement for the team – and I am so proud of each and every one of them.

Around the world, we have had people reaching out to congratulate us. Even our competitors have sent messages, which I think is a classy touch.

Who are your main competitors?

I hate answering questions about our competitors because it is so difficult to give a single answer.

For example, we have one customer who has about 2,000 retail stores in the UK and we do very specific work for them to secure their in-store system. They see Threatscape as being their in-store retail systems security experts – because that's what we do for them.

Whereas we have another client where we went in and did a major project to secure their cloud infrastructure – and they think of us as their cloud security guys.

The funny thing is we have these silos of expertise, and in the case of this award we have a specialist team which we refer to as our Microsoft Security Practice – all they do is Microsoft security work. The lead consultant came from Microsoft to join us because he wanted to focus on security, and in that space we have a different and fairly small set of competitors who do large-scale Microsoft security work; there aren't many though with the depth of experience we have which is why that part of our business is growing quickly including an increasing number of projects overseas.

One of the challenges that Microsoft had was that over the last three or four years they have considerably increased their investment in cybersecurity which has given them an impressive product portfolio – but traditional Microsoft partners who could talk to you about Azure, or talk to you about Windows, weren't as focused on or skilled in security.

As a result, Microsoft reached out to people like us and said we want some hardcore pure-play security partners. In many cases, when we go into work with people, they already have other companies which they work with for their general Microsoft requirements. We are cool with that – we don't deploy Office, and we don't train people on how to use Teams. But when it comes to securing those platforms, that's what Threatscape does all day long. So, when it comes to competitors, it would be fair to say that we work alongside our competitors and actually complement them – we all work together as a team.

Since winning the award we have had a few Microsoft partners, with which we had not previously engaged, around the world reach out to us, and say "Hey, haven't heard of you before. Been on your website because of the win. Seen the specialist services you provide and managed services you offer, can we talk?" We are delighted to get this response as a result of the win.

Can you tell our readers more about the background of Threatscape, how you started, your ethos, and what's your personal drive for the company?

My wife says 'I'm a geek in a suit' because I was originally a 'techie'. I studied computer science at college, and my own personal background is in the computer security business that goes all the way back to the 1980s. At that time, the computer virus problem was just starting to emerge. It was the days of the 'floppy disk', and some of my clients were asking "What is this virus problem? How do we deal with it?"

I looked for a solution. At that time, my business was very small, and I found a guy in America who had just created a solution for the virus problem. He had a small business as well with 11 people working for him – but he had the solution. He had a product that would find the virus, and I signed up to work with him as an agent. His business took off big time. His name was John McAfee. I was one of the very first people anywhere in the world to sell McAfee anti-virus software!

Very early on my general PC consulting business became a pure play computer security operation. I did that for 20 years, then I sold the business some years ago – and typically for any techie – I got bored, so, I set up Threatscape. Whilst we are a ten year old business, we have actually got a 30 plus year heritage – and yes, we do have clients who have been dealing with some of our key people for a very, very long time.

One of the reasons for such long lasting client relationships, and what hasn't changed through the years is our ethos – we want to make a difference to our clients, by delivering real value – and to be seen not merely as a supplier but as a trusted partner. We only recommend and deliver solutions and services we believe in, and which we are confident are a good fit for the client and will provide enduring benefit when it comes to securing their critical business IT assets. When it comes to protecting that position as a trusted partner – the only protection is performance. We can't ever let a client down or deliver anything less than the best in technology or service. We drill this into our people.

I personally dealt with John McAfee many years ago. In fact, I got a share allocation in their IPO because we had been one of their trusted partners around the world and we saw the amazing journey they went on. This was all back in the dot-com boom. I remember realizing one day that in my mobile phone I had three billionaires' phone numbers – and I kept thinking what was I doing wrong!

We had a great track record at picking companies to work with. We did look back some time later and say; "you know, rather than partnering with these guys, we should have just bought shares and gone to the beach – we would have made far more money."

But would you have had so much fun just buying the shares and going to the beach?

Its true we have had fun. One of the things I genuinely enjoyed most about my job is that in cybersecurity it is (a) very technical and I am a geek at heart, and (b) it really does bring benefits to organizations and their employees, everybody needs it so our customer base is very diverse.

Working in cybersecurity means I get to visit people in totally different industries. For example, I have been in the control room where they run traffic light systems for major cities. I have been out to the Isle of Wight where one of our clients is an aerospace manufacturer and seen how they build the winglets that go on to jets. We have clients in military and law enforcement who have very particular security needs. We work with UK major retailers who transact billions of dollars a year via their online platforms, which we help secure. We have clients in the City of London transacting and settling trillions of dollars of financial transactions per day across the globe. It is just mind-boggling stuff that these people are doing. For a techie – this is all pretty cool. We get to see how the real world operates and how what we do supports it.

A lot of people confuse security and privacy, so from your point of view how do you make that clear distinction?

It is an interesting question. One of the simple ways I explain the difference to people is to say is … “my ‘security concern’ is whether someone is going to hack into Facebook and steal my data. My ‘privacy concern’ is whether Facebook are going to sell my data.

This is because you could have all the security in the world – and I know Facebook spends millions of dollars, and hopefully will continue to do so – but it means nothing if their own corporate policy is to abuse, sell and republish your data.

What is your view on phishing emails and the CEO transfer of funds scam?

When people ask us about phishing emails the first thing we say is that it is not a technical failure. It is a process failure. A systems failure.

The classic example of this is the cartoon that says “you’re got your million dollar firewall, but I have your CEO’s PA’s post-it note with her password on it which cost 5 cents”. For a fraudster, that is all they need because if the people don’t follow things properly, they can fool people into doing something dangerous.

There was an infamous photograph in the national press some time ago when Prince William was still flying the coastguard missions out of the base up at Anglesey. The media were invited in just to see in action the ‘day in the life of a working royal’ it was all very fluffy and positive. However the photograph that was then taken and published in the UK press the next day, showed that over Prince William’s shoulder on the notice board could be seen a post-it note which said “This Month’s password login details are …’ It is this sort of thing that defeats the security!

When it comes to the CEO email type of attack. Yes, from a cybersecurity perspective you put in controls which is what we do for clients, we can reduce the likelihood that certain types of attacks will come in. There are some classic tell tale patterns of course. For example, if an email comes in to Threatscape that claims to be from Threatscape – naturally that’s a red flag, because it can’t come from outside claiming to be from inside.

One of the messages we have been giving to our clients over the last three or four months is that in many organizations where a finance team would be sat around the same office in earshot of each other, they might have, without even realizing it, developed an informal verification process where Bob would shout over to Mary to confirm something because they are in the same office.

Now that people are working remotely, the informal verification process has gone – and therefore staff are more susceptible to this type of attack. Therefore, people should make sure that they think about their independent means of verification, and it should not be purely electronic, because if you are relying on an email message to verify something, and the email gets compromised, then you have no verification. So, you need an independent channel of verification.

We have all heard horror stories. The classic case is about is an American network vendor who had the misfortune to disclose, as some companies are required to do because they are public, details of their finances, and details of significant corporate developments. In its quarterly filing two points caught the eye of an attacker.

Point 'A' was the fact that they were sitting on a bunch of cash in their Asian subsidiary, and for US tax reasons they just said, "we have x hundred millions sitting in Asia, and we are keeping it there for corporate purposes otherwise if we brought it back to America we would have to pay tax on it". Big companies do this all the time.

But then 'point B' was they said, "our chief financial officer resigned from his position and the company is currently in the process of searching for a replacement."

An attacker put two and two together and said perfect. There is a load of money sitting in Asia and the guy who normally calls the shots has just left. The attacker then figured out who was the temporary replacement was, crafted a fake email pretending to be from him and sent it to the financial controller of the Hong Kong office.

What happens with these well-crafted emails is that they prey on peoples' vulnerabilities. First of all it said, "this is super confidential and I am trusting it to you, you cannot discuss it with colleagues" – so that reduces the chance of people finding out that it is fake.

Then it said "As you know we have x million sitting on deposit" – so obviously this guy knows what he is talking about – "and we are going to use it through a transaction to acquire another company. Because this is mergers and acquisitions, its super secret. You can't tell anyone what we are doing."

So, the poor guy in Hong Kong now falls for it and is asked to transfer a couple of hundred thousand dollars to the fake bank account of a fake law firm. He is told that the law firm is doing the due diligence for the acquisition and makes the transfer. At this moment, the hackers are high fiving in whatever part of the world they are operating in.

A few days later they say, let's go for the big one. They send another email to the financial controller, saying "Great news, the lawyers have finished the due diligence ahead of schedule. Everything looks good, the deal is going ahead, we need you to transfer $81 million to the lawyers escrow account" – and incredibly, without any further verification … the money gets sent.

The attackers gained tens of millions of dollars just by sending two well crafted, cunning, targeted emails. Now a lot of the money was recovered, but not all of it. No system was breached, no hacking was done, it was just humans who were hacked.

Years ago, the bank robber, Willie Sutton was asked by journalists "why do you rob banks?" His answer was simple, "Because that's where the money is!"

In the modern day if you ask a hacker, "why do you attack people?", the answer is simple, "that's where the greatest vulnerability is. If a hacker is given ten companies to target, they are more likely to find individuals, rather than technology that they can break.

Bruce Schneier, a well-known cybersecurity commentator and expert, testified before Congress. His maxim, which I absolutely believe in, is that "amateurs hack [computer] systems, professionals hack people'' – because you are more likely to get what you want if you subvert people.

At the core, that is how the CEO email fraud works. The fact is that somebody in your company must be in a position to transfer money. So why try to break into the computer to transfer money, when you can just do it through that person?

Generally, a hacker will deceive, coerce, bribe, and even try and convince them that they are ideologically aligned, in order to induce an individual who has the privilege user access to assist them – then they can achieve their ends.

This is a very hot sub-set of the cybersecurity industry right now – the whole area of PAM – Privilege Access Management.

If you look at the totality of your risk within your IT system, the actions that are available to your privilege users tend to be those of utmost concern – that tends to be where you really need to put your focus.

If you spot an erroneous series of activities of the privilege user you need to start seeing red flags. For instance, let's say Carol logs in at 3am, and you know that Carol never logs in at 3am – that might be a red flag – or a 'signal' in cyber parlance.

Or Carol just did five bank transfers in the space of 12 seconds – you know what, Carol's fast, but nobody is that fast!

These are the sort of things that a well designed security system will look for in terms of privilege access management – because you know that compromising the credentials or the individual who has privilege access can be the keys to the kingdom in the digital world.

What do you think some of the security issues will be as we start going back to the office?

Everyone has had to adapt to the whole area of remote working in a hurry. It was all a bit of rush for organizations to make sure that all their systems were effective. Now as people have had a chance to catch their breath, there is a lot of back filling going on in terms of monitoring tools and security.

Where you have had staff taking company devices outside the corporate desk work, and working on them at home, you now have the same staff bringing them in through the front door to connect to the corporate networks – and some may not have been fully connected to the networks before. The easiest way to get malware and malicious code into an organization is when somebody walks it in via the front door and load it on to a laptop or some other mobile device.

Many organizations will be very conscious to undergo fever scanning and covid monitoring of staff when they come back into the premises, but they should also be putting the same level of scrutiny on digital devices that are coming back in from the cold.

What are some of the next growth areas for Threatscape?

We see our revenue streams and the sphere that we operate in as endpoint, network and cloud. In terms of what we do for people in those spheres, we provide solutions (which means technology), we work with vendors (who provide the actual products), we provide professional services (our expertise to advise people, architect solutions, deploy the solutions, train them, support them), and we provide managed service where we provide ongoing monitoring of enterprise-wide digital security.

We are seeing growth in all these areas. Possibly the largest growth recently has been in the managed service space, because there is simply not enough expertise out there and organizations struggle to get access to the experts they need. Outsourcing to somebody like Threatscape, who has the economy of scale to do it, and to do it 24/7 has become very attractive.

What would be a closing statement to get across to our readers?

The thing about Threatscape is that we tend to build long-term relationships with our clients. We find that once people bring us in to work on a project, we very quickly become a trusted adviser – and that is something of which we are very proud.

We measure our success – not just in pounds and pennies – but by the fact that at the end of every year we can look back and see that our list of clients who trust us has grown. That shows us that we are doing something right.

I think the greatest accolade for us – much as it is great to win an award from somebody like Microsoft, because that is an enormous proof of capabilities of our team – what really brightens my day is when a customer introduces and recommends us to somebody else.

That shows me that the customer is not just satisfied – they are super satisfied, and we love getting that sort of endorsement. That for us, is proof of a job well done, and we get that regularly. That is when we have our virtual high fives on our team calls.