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 Martin Jakobsen

Carol Baker

Founded in 2017, Cybanetix has quickly become one of the UK's fastest-growing Managed Detection and Response providers. Offering 24/7/365 managed cybersecurity services, Cybanetix leverages advanced security technology, expert analysts, and a Security Operations Centre (SOC) to protect businesses and networks. We speak with Martin Jakobsen, Managing Director, Cybanetix, about what is driving their rapid expansion and why 'good enough' security is no longer sufficient.

Martin Jakobsen
Managing Director
Cybanetix (https://www.cybanetix.com)

Martin Jakobsen is the Managing Director of Cybanetix and brings over 20 years of experience delivering NOC and SOC services to a wide range of customers. At Cybanetix, Martin has overseen the company's growth into a trusted MDR specialist supporting clients across multiple sectors, including large-scale enterprises and public sector organizations. Martin remains focused on expanding Cybanetix's capabilities and its use of advanced, AI-enabled security operations to deliver practical, intelligence-driven services.

Prior to Cybanetix, Martin served as Managing Director of Capita Cyber Security and holds board positions at KonsensIT A/S and CapMon A/S, contributing his expertise in governance and strategic growth.

He has played a central role in the design and build of some of the UK's largest government networks and has provided outsourced security operations to multinational enterprises. His combination of technical expertise and leadership has enabled organizations to strengthen their defences and run more resilient security operations.

Tell our readers a little about yourself.

I am a technologist at heart. I started programming at the age of six – learned binary numbers by the age of 9 and encryption maths at 16. I taught university encryption when I was 18, and at the same time started my first tech business. I am now on business number four. I have been part of a startup or have started it myself since then, and have undertaken numerous roles through everything from developer through network to security. Funnily enough, I like the complexity of trying to build a business. Tech isn't easy but add people and processes to the mix and it gets a lot more complex, which is the challenge you face as a CEO.

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**

Given your 20 years of experience providing NOC and SOC services, what are the most significant changes you have observed in cybersecurity threats, and how has Cybanetix adapted its strategy to address them?

Many think that cybersecurity wasn't a problem before the internet – but that's not entirely true. The first ransomware was delivered on floppy disk and sent to people via post. Since then, cyber security has evolved from deploying basic perimeter security using firewalls to defending against the really complicated attacks we see now involving everything from social engineering and service desks, through to phishing emails and credential hacks, and even bribing people to get access to organizations. Today, the complexity of cyber has evolved along with the monetization the malicious cyberattacks, resulting in what some statistics state is a $2 trillion dark cyber industry.

How does Cybanetix differentiate itself from traditional value-added resellers and larger systems integrators, and what market gap as the founder of Cybanetix did you originally identify that led to the company's creation?

When I sold my last business to a very big integrator, I ended up running their cybersecurity division. One of the things which became obvious very quickly was that the integrators were wholly inadequate when it came to dealing with the mid-size market. UK enterprises with 1,000 to 20,000 employers have very complicated cyber problems, but they don't have the scale to build out what say, the likes of Barclays Bank has, yet these enterprises have the same complexity of problems as say a Fortune 500 company.

Initially, I thought I could get the organization to develop new propositions relevant to the market, but it was just evident they weren't agile enough, so I created Cybanetix with a view to initially serving the mid-market. That's where the biggest problem was in terms of talent retention, building scale and everything else, whereby outsourcing makes more sense for those businesses.

Establishing a 24/7/365 operation in itself requires quite a big footprint of talented people, for instance, identifying them in the first place, training them, and then maintaining them is the next challenge.

But there's also a fundamental lack of knowledge at the vendor/reseller end which means that they struggle to do managed services well. Yes, they have some professional services arms and they might wrap them up and call them managed services, but cyber moves extremely fast. If you sell a three-year contract, and you are still delivering the same service in year three as you did in the first year of the contract, then I think you have failed.

For example, if I was a CISO in any big business, and three years later I had not evolved my cybersecurity posture, I would be fired because that would not be seen as unacceptable in the board's eyes. Therefore, Managed Security Service Providers (MSSP's) need to evolve themselves. But if you are a big integrator, you sell a service and you deliver that service – that's what they contract you to do. Any change from there will be chargeable. For instance, if there's an improvement of service, or that service is adapted and tailored to a customer-specific environment,

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**

it would be chargeable. Therefore, what we see is that some of the approaches adopted by the very big suppliers or very small suppliers is a very 'cookie-cutter' way of doing things, where 80% of what they do is good enough. But in cyber 80% is not good enough anymore. It needs to be 100%. The advancement of attacks with AI makes it easier for attackers. They just need to find one little hole and then they're through.

We recently had 16 CISOs in for a partner advisory board. As part of the conversation, one of the CISOs said that his coverage for Endpoint Detection and Response (EDR) was 98.8%. If someone had told me that five years ago, I would have said that was amazing in terms of the coverage they've got. Today, that is not the case – good enough, just doesn't cut it.

Last weekend, we had a customer who had 100 devices out of the 10,000 on the estate, so 1% not covered, and perpetrators got in through a device that had no security controls. Fortunately, we identified it and got it stopped. But, you know, it just took one device.

With AI-driven technologies rapidly changing the threat landscape, what is Cybanetix doing to leverage AI in its services, both to enhance its own offerings and to advise clients?

We divide our AI endeavours into three distinct streams in business.

First, our own internal use of AI, and the productivity gains and other things which we get from the technology. So that's everything from notetakers, auto-summarizing cases and writing notes. We deal with around 150,000 alerts every month and every alert needs a summary written when it's investigated. When 95% of all those comments are identical, because it's the same thing that's happening, writing two or three paragraphs on the alert takes a surprising amount of time. We now increasingly using AI to summarize that information.

We have always used machine learning (ML) and AI in detection capabilities, especially in the work we do with Exabeam. ML is natively built into lots of tooling which is used for security today.

In addition, next year we will be testing some of the new autonomous SOC analyst tools which are out there. The pace of AI is moving fast and while the AI SOC analysts are still fairly immature, we are expecting this strain of technology to evolve quite rapidly.

Secondly, is end user protection. For instance, if you put IP sensitive data into ChatGPT, does AI then divulge everything that goes to the internet relating to that data? It's important to make sure that end users in organizations are using AI in a safe way. There is a huge tendency for end users to blindly trust the technology. When it comes to end user AI engagement with ChatGPT, the majority of people start to personify it and this raises the question of how do we control and monitor AI for IP and data loss?

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**

Thirdly, is the use of AI in organizations. It doesn't matter whether you are a commodity trader, bank, manufacturer, or one of the biggest education facilities in the world, all businesses need to deploy AI and have AI programs. But herein lies the problem. Money gets funnelled into some IT teams and DevOps teams, and the first thing they do is a search on Google.

There are over 2.1 million open source AI models which can be downloaded and used, but what people don't know is how these AI models are trained, what data they are trained on, and who developed it. Add this to the tons of AI models which people then develop independently, and what we see are that security teams are not even being engaged because the business priority is to deploy AI first and think about the security later. People don't think about the ramifications.

With the velocity that AI is being adopted, it is important to have guardrails around knowing what you've got, understanding which models are there, what they do, and what they are connected to.

I was recently talking to a CTO who works in financial trading. She said, "What if we report the gold price wrongly for four hours? If gold prices were reported wrongly for four hours and trades were executed on it, depending on how long it was, there could be a financial collapse." So, the challenge is trying to underpin AI security technologies which are not quite there yet.

In a world where many companies rely on a hybrid work model, how is Cybanetix helping clients secure their distributed networks and protect against vulnerabilities that arise from remote work?

This comes back to my first point where everything sat behind a firewall. The adoption of cloud started to change that. Your data set was no longer sat behind your own walls, instead it sat somewhere on the internet or in the cloud. But the biggest disruption this caused was probably the change in the human mindset. When you used to go to work to a workplace location, you would be in a work mode. Likewise, when you used to go home, you were in home mode but the blurring of those boundaries eroded our sense of security.

A large proportion of attacks are identity based and phishing, smishing and Vishing often focuses on apps running on mobile devices. This makes it really hard for end-users, because if you have your work accounts and your private accounts on the same device, the human mind needs to do a mental switch to get into the right mode. For example, if you just switch from email to LinkedIn mentally you're still in work mode.

But people have a tendency to believe that they're safe in controlled environments. So, if someone suddenly gets a message saying "We're contacting you from IT" and the user has just been looking at corporate email on their phone, but suddenly they get that on LinkedIn, people are much more likely to respond, only to find it is a phishing message. It's more the mental state of users that's the problem than the technical problem itself, so what we are seeing is that people are more likely to do things that they shouldn't in certain situations.

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**

Cybanetix has been recognized with awards such as "Technical Star Partner of the year" from SentinelOne. What are the key factors that contribute to this technical prowess, and how do you foster a culture of expertise within your teams?

I think that there are a few things here. One, is that we have chosen to work with as few technologies as possible. Obviously, the number of technologies has been expanding over the years, but the problem is if you try to become – especially in cyber – master of all, you'll end up being a jack of all trades because there are simply too many solutions in the market.

The reality is we chose to work with as few as we could and then go very, very deep in with them, and on that basis, we ended up developing very, very extensive capabilities with a small number of cutting edge technology partners.

From a team perspective, Cybanetix is a very tech heavy organization with 80% of our workforce being techies and analysts. This stems a little bit from our culture, because obviously I'm a techie by heart, and that probably drives the culture down in the organization.

We want to take on the biggest and the best in the market and do it better, so we deliberately invest very heavily in both a very senior technical approach, but also training programs for our juniors to evolve and advance them.

Beyond building secure networks, Cybanetix also emphasizes transitioning clients "from legacy security setups to cutting-edge solutions". What are the biggest challenges companies face during this migration, and what is your philosophy for managing a seamless transition?

If potential clients talk to our clients, that's the best way of selling, because generally we have exceptionally happy clients. Our total retention of clients since the Cybanetix's inception is 98.7%.

This means we don't really lose clients. I believe this comes back to our partnership philosophy in working with them and achieving 'continuous improvement' for that client. Clients love us and they know if they sign up with us, they will see improvements during the contract period, and that sees them sign up again because they expect and get continuous improvement.

Perhaps the biggest indicator of that is what happened recently when I was at a conference. At an executive forum I attended recently, two of my clients happened to be there as well. Another executive at the table said they were looking for an MSSP, and what were people's thoughts? I stayed quiet but one of my two clients just said, "It's a very simple answer, he's sitting next to you."

After I left the room, once the session was done, my other client was just selling on my behalf. That level of recommendation only comes from trusting existing clients and working hard to ensure that they are happy – and that's having a little bit of a snowball effect for us.

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**

But coming back to the original question, for someone who has never had a managed service product, or SOC before, or never built one, they cannot articulate what we do, because they fundamentally don't get it. They ask what they think is a simple question, "Can you deliver us a 24/7/365 SOC or MDR service?" and we say, "Yes, we can do this."

But everybody says they're a 24/7/365, offer a SOC, and will respond. What it comes down to is the detail underneath – coming back to that 80% or 99%. It's the difference between a BMW and a Ferrari; they're both good cars, but you wouldn't take a BMW out on the track and race against a Ferrari, it's just pointless. For those people who are unfamiliar with the nuances, they just see four wheels and a motor, then an engine – and they don't understand the devil is in the details or in our case our capabilities, philosophy and customer track record.

In what ways does Cybanetix help organizations meet and simplify compliance with regulations like ISO 27001?

ISO has already driven a need for monitoring and security because there are particular controls in the standard that require you to have telemetry data, access data, and to keep it for a year. Even so, ISO control states that you should review a particular event, but that review is left open to interpretation. Some businesses will get all the events on a spreadsheet once a week and look through it, and then say they reviewed it, while others will do it in real-time and use a SOC provider, so it's how diligent the company is that is the determining factor in terms of how effective the framework is.

While ISO initially drove a lot of compliance, businesses now think of compliance as a guidance for security and for most people, compliance has become perhaps not a tick box exercise but certainly a minimum baseline. The danger is that a company that is ISO 27001 compliant believes it is secure which is not necessarily the case.

Beyond the UK market, which specific geographic regions or market segments does Cybanetix see as key expansion opportunities for its cybersecurity solutions?

We are expecting to see 50% growth year-on-year. We will be looking at the evolution of Managed Detection and Response (MDR) services, and how we tackle AI, and we will be launching some completely new services to address that new challenge next year. So it's more and more growth.

On top of that we be looking at expanding internationally. We've already got quite a few clients in the Middle East who came to us inbound, and we have been debating whether to build a presence there because we could easily expand on that and accelerate. The US is also a market that's always interesting just due to its sheer size and advancement in cyber. However, the dilemma is do you keep growing 50% organically in the UK market or risk the distraction by building out other markets? But it's a nice problem to have.

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**

Any closing thoughts?

I think it's important to realize that the world of 'Good Enough' is dying in cyber and people need to be ultra paranoid. We're seeing the tenacity of attacks, complexity of attacks, and sophistication, increasing daily. Not much needs to go wrong before it goes really, really wrong, and the ramifications are easily found in the newspaper stories we're now seeing on a daily basis. Best practice two years ago is no longer good practice. It would be seen as probably malpractice in my eyes! But then, I'm a little bit draconian!