



# Security as a business enabler

PROJECT PARTNER

Secureworks® |  Taegis™





# Security as a business enab

WRITTEN BY JONATHAN DYBLE  
PRODUCED BY CRAIG DANIELS





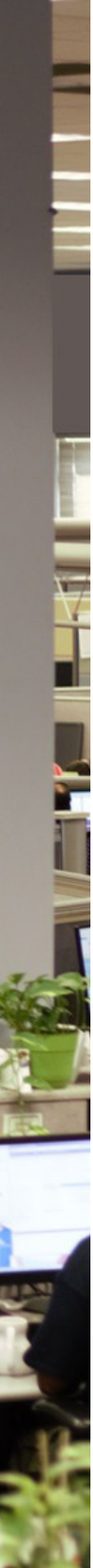
A portrait of Brent Deterding, a man with a goatee, wearing a blue checkered shirt and a dark blue blazer. The background is a blurred green landscape. A large white diagonal shape is in the top right corner.

ler

Afni and its CISO Brent Deterding are breaking down the traditional and perceived barriers between security and the boardroom, transparently positioning cyber effectiveness as a critical enabler of improved business outcomes







cybersecurity has never been more important than it is today.

Where the COVID-19 pandemic prompted national lockdowns and stay at home orders, many companies adapted their IT infrastructure to prioritise business continuity amidst extreme uncertainty.

Since then, firms have found the benefits in flexible, cloud-based operating models. From improved productivity to enhanced employee satisfaction, they have proven their worth; and so many companies are naturally continuing to consolidate their digital toolsets in order to maximise the opportunities available to them.

**FROM A SECURITY PERSPECTIVE, HOWEVER, THIS TRANSITION HAS PRESENTED SEVERAL CHALLENGES.**

Those firms continuing to integrate more technologies and solutions are in turn expanding their overall attack surfaces, creating new vulnerabilities and opening

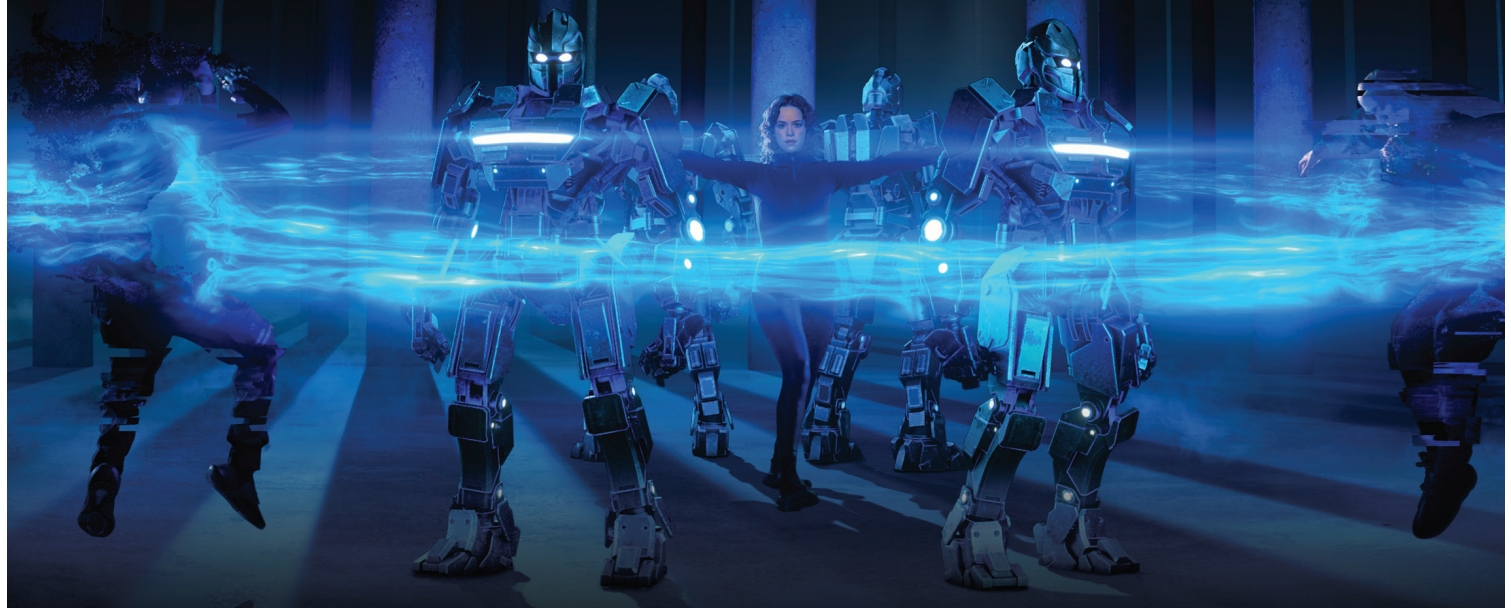


**OUR MISSION**  
Our mission is to enable better outcomes through  
**positive and worthwhile engagement**  
with employees, clients, partners,  
and customers of the world's best brands.



Secureworks® |  Taegis™



**ARE YOU READY FOR THE INEVITABLE CYBERTHREAT?**

Detect Ever-Changing Threats and Defend Against Them.





potential entryways for attackers to exploit.

Unsurprisingly, nefarious actors are ramping up their efforts in response. According to Accenture, the average number of cyberattacks per company increased 31% in 2021. Meanwhile, the International Data Corporation reports that 37% of organisations globally were the victim of a ransomware attack in 2021.

“The simple fact of the matter is that, for most organisations globally, the threat posed by cyberattacks is among the top business risks in financial terms,” explains Brent Deterding, Chief Information

Security Officer (CISO) at contact centre solutions specialist Afni.

“To put it another way, the most likely extinction level threat for many firms comes from cyberattacks.”

### **EFFECTIVE COLLABORATION IS CRITICAL**

Deterding brings unique expertise to the role of CISO. For almost 20 years, he acted as a security practitioner working with a leading security vendor specialising in threat detection, incident response, and security strategy. Deterding spent





15 of those years in various operations roles, while the latter five were spent in sales positions. With experience in both backgrounds, he brings plenty of cross-business knowhow to his new role.

However, it is not just this career history that puts Deterding in a distinct position. Equally, the newly appointed CISO brings fresh perspectives and ambitions, voicing his enthusiasm in relation to breaking down traditional barriers and ensuring security functions as a business enabler.

“Frequently, CISOs and CIOs have strained relationships. Often, CISOs are seen as a hindrance to ‘getting things done’, but our CIO Mike and I have a fantastic relationship because we’re both

focused on enabling the business.”

“Frankly, the level of risk posed by cyber threats dictates that companies simply need to move past that and develop functional, working relationships that operate in the best interests of the wider business.”

### **BIG PICTURE PHILOSOPHY**

It is this big picture philosophy that drew Deterding to working at Afni specifically. Having spent over a year scoping out various companies for the right cultural fit and found it at Afni; an environment in which he could succeed.

“I needed to go somewhere that truly cared about security and was open to a



vision of a business enabled by security,” he explains. “Afni expressed that they would trust me, by giving me the authority and autonomy needed.”

In the eyes of Deterding, this culture is a critical part of the puzzle in ensuring CISOs can be effective. However, fundamentally, this is a two-way street. For the relationship between board members and security teams to be functional and effective, all parties must ultimately be aligned and headed in the same direction.

“CISOs can be prone to blaming their organisations,” Deterding states. “They can be prone to claiming that senior leadership doesn’t care about security, explaining that they’re underfunded or overstretched, or a scapegoat for challenges.”

In Deterding’s view, that’s a ‘learned helplessness’... “Yes, the organisation has to play its part in enabling CISOs. If the CISO is buried under the CIO, for example, then they might never get a voice at the boardroom level. And that



## Brent Deterding

Chief Information Security Officer  
Afni

Deterding is a veteran of the information security industry with over 20 years of professional experience. For the past 19 years, he’s worked for Secureworks, a leading global cybersecurity firm, where he has served as their Global Solution Lead since 2019.

As CISO for Afni, Deterding ensures security risks are identified, assessed, and mitigated; leading efforts to prevent and respond to security threats; implement threat modeling; and oversee areas including disaster recovery, business resilience, governance, and more.

Risk management and information security are more critical than ever, and it’s Deterding’s mission to optimise and elevate Afni’s strategies and practices.

Deterding is a Certified CISO who earned a bachelor’s degree in computer science from the University of Missouri. He lives in northern Illinois with his wife and three sons. He and his family are involved in their church and have a passion for adoption, foster care and leading youth.

**“For most organisations globally, the threat posed by cyberattacks is among the top business risks in financial terms”**

- BRENT DETERDING, CHIEF INFORMATION SECURITY OFFICER, AFNI



would be frustrating. However, when CISOs do get that opportunity to be heard, they need to use it effectively. CISOs must earn their seat at the table. That is done by bringing value to the organisation; by effectively looking beyond security at the big picture and speaking in a language that other board members will not only understand but listen to.”

### **UNLOCKING SECURITY AS A SALES ENABLER**

This idea that the CISO should enable the business manifests itself in several key objectives for Deterding – ambitions that he actively pursues in his current role at Afni.

The first of these is compliance, ensuring the business is adhering to regulation and legislation to prevent violations and protect the organisation from potential fines and lawsuits.

Second is avoiding other potential costs that might be incurred through security failures, achievable by reducing the organisation’s attack surface and catching potential threats as early as possible.

“Third is increasing efficiency – helping internal colleagues to not only operate more securely but equally effectively,” Deterding adds. “This might entail moving towards a password-less architecture, for example. If employees don’t have to type in a password, their lives become easier and the whole company works









more efficiently. But guess what? We've also increased security."

Additionally, in the view of the CISO, there is a relatively new fourth role – sales enablement.

Operating as a contact centre solutions specialist, Afni faces stiff competition in a market of many players. Within this context, differentiators can be critical – something that security is increasingly able to offer.

"If security can participate in the sales process, then the advantages are clear," Deterding affirms. "Clients aren't convinced by a company's security effectiveness simply by being presented with a report of certification. They require trust and confidence, but trust and confidence are ultimately emotive, and this needs to be appreciated. This is a skill. CISOs need to speak directly to the client. They need to be able to articulate what's important, to empathise with any relevant requirements or concerns, ask and answer questions, and help to create a partnership.

"That includes being transparent about any potential gaps, anticipated risks, areas for improvement, and areas of accepted risk. That level of honesty will feed into trust, and trust will enhance relations and create confidence."

Indeed, demand for insight into the security practices of service providers is rapidly rising up the priority list of customers across almost every industry.

## **"If security can participate in the sales process, then the advantages are clear"**

- BRENT DETERDING, CHIEF  
INFORMATION SECURITY  
OFFICER, AFNI

Supply chain attacks, also known as value-chain or third-party attacks, are becoming increasingly common, with attackers infiltrating systems via outside partners or service providers. Furthermore, those companies falling prey to breaches have been shown to suffer monumental financial and reputational damages that can leave a hugely negative lasting impact.

Those CISOs that can address these concerns effectively can dramatically improve the sales prospects of the entire organisation, unlocking security as a competitive differentiator.

This begins with communication – a soft skill that will assist at all levels. That doesn't just mean conveying an understanding of business needs and gaining buy-in from internal board members or unlocking a competitive advantage in the sales process. Equally, it ensures CISOs can work closely with



their colleagues to remain at the cutting-edge of security developments.

“We’re in the business process outsourcing (BPO) space, so I regularly talk to other CISOs from other BPO specialists,” Deterding outlines. “We might be competitors, but we’re not competing in security. It is not a trade secret – the better we all are, the better it is for everyone.”

### **MAKING SIMPLICITY AND TRANSPARENCY PRIORITIES**

Having been in his new role at Afni for only a matter of months, Deterding’s patience in taking the time to find the right cultural

fit and belief that the CISO should bring value to entire organisation is starting to pay dividends.

And now he has achieved his two key priorities of ensuring 100% of Afni’s users are using multi-factor authentication and that every single one of the firm’s external systems are patched within 72 hours, his attentions are turning to a series of broader objectives.

“One thing that really excites me that I did not necessarily expect is how broad a scope my company wants me to have,” the CISO explains.

“It has allowed me to begin driving towards establishing a formalised











enterprise risk management programme, as well as increasing the maturity level of our internal audit programme.

“My ability to focus on these initiatives is testament to our team and vendors. Our staff are outstanding, and I know the value of true partnerships which we have here at Afni.”

In every one of his endeavours, Deterding is focused on maximising simplicity and transparency, again to extend the value that security is able to bring to the wider organisation in a clear and obvious manner.

Looking ahead, this CISO expresses optimism that the often-fractious relationships between a CISO and their fellow executives will soften in the future as the spotlight continues to be shone on the paramount importance of security.

“Part of the change that is needed is likely to come from regulation,” he affirms. “In the US, for example, the Securities and Exchange Commission is discussing the implementation of rules that would require cybersecurity expertise at the Board of Directors level for publicly traded companies. And as we require cybersecurity at the board level, the role of the CISO will naturally mature to be more business focused.

“In that eventuality, the problem of cybercrime should become diminished, as boardrooms will more actively buy into processes that will help to reduce risks dramatically. I am confident that we will get there as a sector together, but it will be a process.” ■



