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 Mark Kedgley

Carol Baker

Now part of Netwrix, NNT help organizations monitor and control changes and configurations, which are foundational to protecting against data security threats. As one of the co-founders we talk to NNT's Chief Technology Officer, Mark Kedgley about what and who has inspired him throughout his career.

Mark Kedgley has been the Chief Technology Officer (CTO) at NNT, now part of Netwrix (https://netwrix.com), since January 2009 and has approaching 30 years' experience in the IT industry covering support, solution sales, and business development. Prior to his tenure at NNT, Mark studied Physics at the University of Birmingham then held leadership positions at Cable & Wireless and ASG.

As CTO at NNT, Mark is responsible for driving ongoing product development of Netwrix Change Tracker.

The objective is to protect sensitive data against security threats in the most efficient and cost-effective manner, while maintaining market-leading ease of use.

How did your career in IT start?

After a stint packing 35-millimetre film boxes during the Easter holidays while I was studying, I decided working on a production line wasn't for me. So, when it came to finding a summer job during my first year at university, I joined a company and began running the help desk for an X25 network which I probably wasn't experienced enough at the time. Fortunately for me, the man who interviewed me really didn't know much about computers and, luckily, I knew just enough to get by – and the rest is history, as I have remained working in IT ever since.

One of my earliest customers was Essex County Fire and Rescue, and we were involved with connecting offices and providing connectivity between those offices. There was no internet service or high-speed broadband to speak of, and it really was a case of just buying telephone lines from BT and putting equipment on the end of it for voice and data. Back then, security was not the complex issue that it is now. However, over the last 20 years, security threats have been such a growing problem and technology has had to transform in order to address these issues, which has been really interesting to observe.

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 2009, I became one of the co-founders and CTO for NNT, which was later acquired by Netwrix in 2021. Over the years, I had always been involved in sales, technical support, and designing solutions – and have seen much develop right from before there was an internet. Through the dawn of the internet age to the present day, as technology continues to evolve, there are of course a plethora of security issues which are continually being introduced.

Who has been inspirational to you in your career in IT?

There are many who have influenced my career over the years, but the one who stands out to me the most is Bill Gates. I know it is probably the unfashionable thing to say, and it's probably a generational thing, but Bill Gates has been inspirational to me mainly because he can do it all: he can develop a product better than any software engineer, but he is also a brilliant businessman. Especially when it came to licensing Microsoft technology and taking it all over the world; he has also remained front and centre – which is quite unusual.

I have met many people who are natural salespeople, or who are good at designing clever solutions, or great support people – most people in life are good at something. But to identify someone as a genuine all-rounder is more unusual.

Another person who comes close to that was the late Martin Hewitt, who was the MD of a company I had worked for when I was working with Essex Fire and Rescue. He was a really clever man and if a customer had a problem, he would be the first to take off his jacket and get stuck in to get things up and running. Martin was also great in building the business, spotting new products to sell, and identifying the newest trends in the market.

When it comes to data security, are there any key events which have changed how we now look at security?

There are two big events which will have a lasting impact. One event is the Colonial Pipeline ransomware attack – which had greatly impacted computerized equipment managing the pipeline. This was visually very tangible with people queuing for fuel in the US and had led to the company shutting down for the best part of a week. It was very unusual in that, quite often, we see that there has been a computer outage or computer problem. However, with the Colonial Pipeline ransomware attack it was laid bare and made headline news for days.

The second event would be the 2020 SolarWinds cybersecurity attack which saw hackers secretly break into the Texas-based SolarWind's systems and add malicious code into the company's development systems. As SolarWinds sent out software updates to its customers it had unwittingly sent the hacked code which then created a backdoor to their customers' own IT systems, installing even more malware to expose sensitive data. This caused the US government to issue an instruction for more to be done to protect organizations and their data. In turn, businesses were also encouraged to invest more into their security to keep their clients and themselves safe from cyberattacks.


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**

These two incidents have been a wake-up call for the IT security industry, government organizations, and every business regardless of their size or industry sector. The financial implications of an attack can be severe as we have seen with the WannaCry ransomware of 2017, which cost the NHS £92 million through services lost during the attack and IT costs in the aftermath.

Unless industries wake up to the evolving cyber threat landscape and embrace security best practices, we most likely will see more attacks of this nature in the future.

Which industries do you feel are more likely to be targeted?

The financial services industry is always a prime target, and we have already seen hackers infiltrate banks around the world, for instance, by reprogramming ATMs so that they pay out $100 notes instead of $10 and so forth.

When it comes to ransomware specifically, businesses are advised not to pay demands, but many will do so simply because the impact on their businesses can be so great. IoT devices are often a weak point and can be used to co-ordinate a DDoS attack and as one is shot down, another attack on an IoT soon emerges. It can be a constant battle.

In financial services, there have already been several scams around crypto-currencies, and attacks on crypto are likely to be the next big thing. With cryptocurrencies beginning to become normalized, it poses yet another way for a hacker to monetize a cyber-attack.

At Netwrix, we aim to bridge the gaps between various security silos, such as data, identity, and infrastructure, so that you can protect not only 'the first among equals', your data, but also the vehicles used to get to it, in order to make your organization more secure tomorrow that it is today.

Cloud is a big weak spot because it is still relatively new and very, very complex. If done incorrectly, particularly for public clouds, businesses are prone to opportunistic or outright malicious attackers. At Netwrix, we have built a solution that will look at any of these public cloud infrastructures and identify the weak spots so that security can be improved. After that process, we provide continuous surveillance so that we can spot if any configuration drift occurs. The technological challenge is to distinguish between a planned software update and an unwanted breach or infiltration on any assets. The goal is to make sure a breach is addressed immediately – not months and months later.

What mindset do businesses need to adopt to address cyberattack issues?

Breaches will continue to occur, and only when businesses learn to develop an ingrained understanding of security will they be able to deal with the issues effectively before damage is done. Security spending is on the rise, but it is important to more closely integrate operations and security. It is vital to know whether a change is good or bad or whether it was planned by the operations team

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**

or not. If the change is suspicious, it could be anything from ransomware attack or a zero-day threat coming in from outside the organization through to an insider threat such as someone hijacking or misusing legitimate credentials. If businesses can tackle the issue at the source and can identify the difference between planned and unplanned changes, then they have a fighting chance of protecting the business against cyberattacks. It is a world where developments in cybersecurity hold the key.