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 Mickey Bresman

Carol Baker

As Semperis announces research findings into the Active Directory security posture of organizations, we catch up with Mickey Bresman, CEO and co-founder, Semperis, to explain more about just how powerful an attack targeting an organization's Active Directory can be.

Mickey Bresman is CEO and co-founder, Semperis (https://www.semperis.com), a leading provider of enterprise identity threat detection and response (ITDR) products and services headquartered in Hoboken, New Jersey. Among the top three fastest-growing cybersecurity companies in the US, according to Inc 5000, Semperis is widely recognized to offer the industry's most comprehensive hybrid Active Directory (AD) protection technology and services.

Beginning his technical career in the Navy, Mickey's comfort zone is on the front lines helping organizations thwart and respond to cyberattacks. The long-time cybersecurity expert and entrepreneur has an extensive track record of driving revenue growth and scaling organizations across the globe.

Prior to founding Semperis, Mickey held the position of CTO at YouCC Technologies, a Microsoft Gold Partner integration company. As a cybersecurity thought leader, Mickey has been quoted or featured in many major publications, including Forbes, CNBC, and others. He has a B.A. in Technical Management and a Minor in Electronic Engineering.

What is Active Directory, and how can Purple Knight help identify risk?

Active Directory is Microsoft's proprietary directory service running on Windows Servers that enables administrators to manage permissions and access to network resources such as computers, printers, scanners and other devices. It stores data as 'objects,' which could be a single element, such as a user, group, application, or a device, and handles the interaction of the user. With a single network logon, administrators can manage directory data, and authorized users can access resources anywhere on the network – making it a prime target for cybercriminals.

Created over 20 years ago, Active Directory has borne witness to various configuration changes and network upgrades over the years. While AD withstood the change of times, organizations are now finding that security configuration assumptions made 20 years ago are no longer relevant in today's cyber world.

Workforces are now more globally distributed. The pandemic has seen employees work remotely from home – in most cases – highly successfully, and whilst companies are keen to get staff back into offices, many are realizing that in a time of need technology stepped up to the mark and delivered.

In the last three years, we have seen a slew of attacks specifically looking for Active Directory vulnerabilities and abuses, and this has generated new types of indicators which security people need to look at from a configuration perspective. If you are not staying on top of things, those looking to penetrate your environment will find holes in your defense, and in your organization's configuration in general.

To assess how serious the risk is, a year ago we launched our free Purple Knight tool, and already over 5,000 organizations have used it to assess and gain visibility to their Active Directory risk. What it revealed was how shockingly vulnerable many organizations are to cyberattacks via Active Directory.

Are there any industry sectors who are most at risk?

Every industry is at risk of Active Directory attacks, and we are working with various companies to help them protect their most critical infrastructure. For instance, we focus on helping multiple healthcare providers which have been hit by ransomware attacks and we go into situations where organizations have lost control over the environment – in many cases their most critical piece is the identity management in Active Directory. We help those customers rebuild their infrastructure as fast as possible, gain back control by kicking out the adversary, and close the security gaps which the attacker had access to so that organizations can have trust in their environment again.

Another sector under attack is the insurance industry. A lot of attackers will go after insurance companies because they want to see the cyber insurance policies of the customers of those companies. They know that if they can access these policies, then they are likely to be paid the amount of the insurance policy when targeting their customers. It becomes a two-step approach: (1) gaining access to the insurance company's systems; (2) going after the policy holder for a guaranteed payout.

How has the way cybercriminals operate changed in the last few years?

As a society we now have a much higher dependency on technology, and what it has created is the ability for the cybercriminals to demand much more in return for everything that is out there. Ransomware attacks are prevalent right now – it's actually an industry all of its own. Cybercriminals are much better organized and we see different cybercrime organizations and groups coming together to commit attacks.

What is the difference between 'wiper' and 'ransomware' attacks?

In a 'ransomware' attack the cybercriminal will get into an organization's computer, encrypt it, demand money. The company pays the demand, then the cybercriminal potentially gives a key to the company to decrypt its environment.

Whereas a 'wiper' attack is basically a weapon that is used to wipe the computers and there is no ability to revert them back. It is a weapon intended simply to destroy, as we saw in the first few hours of Russia's attack on Ukraine, before the switch in focus to kinetic warfare.

Given that it's impossible to prevent every cyberattack, what are some factors that the Semperis team has seen in their incident response work that determine whether a business will successfully recover from an attack?

We see more of the hybrid multi-cloud approach. With a higher adoption of cloud applications, we are starting to see companies take more things to the cloud. Along with this, we have seen some major service providers being breached.

We are also seeing companies trying to adopt a best of breed usage approach – adopting the best tools for whatever need, as opposed to going out and buying everything from the same vendor. This will create a multi-cloud challenge, because to some degree, you want the benefit from everything which has the multi-cloud approach, but you must accept the challenges that come with it including the security, management, and financial challenges. As a result, we are seeing a lot of companies struggling to wrap their head around how much everything is going to cost them, why it's better to go for this service as opposed to that one, and so on.

Trends also show that as companies take everything to the cloud, cybercriminal activity is going up, so organizations will need to gain better control of their security environments, not necessarily by outsourcing it but by putting it inside - which is quite an interesting trend to watch.

How will this impact on the data centre?

When we think of the data centre, we traditionally think about the basement of an organization where they put their own racks, with their own servers, and so on. In the future, we can expect that to reduce significantly, if not even go away completely. To some degree, what will replace it will be cloud infrastructure.

Data centres are here to stay, but we will see a shift and lift approach where you basically take your servers and you move those to be virtual in somebody else's infrastructure, but you still own a lot of what's happening at the above layer. This means you can still create your own applications and you still create some of your control of the configuration of those servers, and so on.

What is a data loss or breach via cyberattack and what does a cyber resiliency plan look like?

In the last year and a half, we were brought in to help multiple businesses with their incident response situations and typically we are being brought into the worst kind of scenarios. The first question is always; how good is their disaster recovery plan? How often has the plan been tested? Can it be trusted? Because at the point that a disaster is happening, everything else in the entire company goes down.

Typically, everybody is running around with their hair on fire, you have multiple people shouting and they all want to know when systems will be up and running again. The business is also most likely bleeding millions on an hourly basis – if not on a minute basis – depending on the size of the organization. If you don't trust your disaster recovery plan because you haven't tried it often enough, you're going to have to pay because there is no way around it.

Much more mature organizations have done their business continuity planning: they have adopted policies in terms of what happens when they are being hit by ransomware; how they recover the environment; what their offline offsite backup policy is, because we’re going to assume that those systems are encrypted. I have had calls coming in with a company saying that its backup and recovery server has been encrypted, and asking what do they do now? Unfortunately, it's probably a bit too late to think about that. But there are multiple things that businesses can do today to prevent being hit by a ransomware attack – and it starts with closing the gaps. While prevention is definitely high out there, we must also assume that an attack is likely to succeed at some point – and when it happens, we’ll go down. Now let’s make sure we know how to come back up.

What does identity-driven cyber resilience mean and why is Active Directory security driving more headlines in recent years?

The world has changed significantly, and the pace of technology is only going up. Up until a few years ago, we were all sitting in our offices behind closed doors to some degree and all the company assets were inside the same building behind the firewall. That meant that there was only one type of approach to protection. Gradually, we started to go out and use mobile devices from any location. This has been accelerated by the pandemic. For many of us, we no longer need to sit in our standard offices – we can work from anywhere. To do this, we have had to adopt the cloud which meant that we no longer had the option to put firewalls around our assets. This means identity has become the new de facto perimeter, because to some degree, the only thing that stands between somebody getting access to an organization’s resources is the identity and access level that can be defined on that resource. And that’s basically the whole concept behind identity-driven cyber resiliency. If you come to the conclusion that cyber resiliency is going to be dependent on the connection between identity resource and access, then protecting the identity store becomes super critical.

Semperis has a strong ethos on how to be a force for good, what does this mean?

For everyone at Semperis it means help first, ask questions later. What I mean by that is when we are being approached by companies that have been hit with the worst type of day, we first ask how we can help – and it's not about how do we make profit or anything like that. This is purely about how we can help them. What do they need? Let’s get started and help you sort this out. But it is not just that; at Semperis we have seen that by adopting a force for good for helping people in need as our general culture, it has a far more reaching effect and we have seen our employees adopt this ethos in their own lives. Suddenly, we see a force for good between people. It goes far beyond being kinder and nicer to each other, its helping people to see the force for good in themselves – and that’s truly inspiring.