

# Inside Active Directory Security Australia, 2023

*Understanding the  
new drive to protect the  
bedrock of identity and  
access management*

# Contents

*Click below to navigate*

---

**1** *Executive Summary*

---

**2** *Understanding Active Directory Risk Today*

---

**3** *Gauging Maturity and Awareness*

---

**4** *Resilience Strategies and Challenges*

---

**5** *Conclusion*

---

# Executive Summary

Active Directory architecture is critical to every Microsoft-based organisation or entity that operates a network of connected infrastructure with multiple staff and segmented or configured levels of access.

As the central set of services to manage authentication and authorisation of all users and computers on a Windows network, Active Directory represents the keys to the kingdom for cybercriminals. Infiltrating a domain controller server can allow an attacker to propagate their compromise much further across a network with relative ease if they are not detected.

The very purpose of Active Directory has been to give access to people, albeit with permissions governing this. However, decades of Active Directory use without proper security governance has led to sprawl in these user account libraries, creating opportunities for attackers to abuse and give themselves certain privileges.

Active Directory may not itself be a security control, however, it is an IT control with security implications. It is a target for cybercriminals, but it is not always a focus area for tailor-made defensive policies, strategies or technologies.

Continued breaches and usurpation of identities to gain access to sensitive systems demand more resilience for account management infrastructure. According to the Australian Signals Directorate, Active Directory is almost always targeted by cybercriminals looking to move laterally across a network following an initial breach.

In this report we will explore the topic of Active Directory security with cybersecurity leaders from Australian organisations over three chapters.

The purpose of the report will be to build understanding of and bring attention to the state of Active Directory security and its relevance in modern organisational risk and defence, as well as offer some resilience considerations to other CISOs on the topic. ■

## Contributors



**Jamie Norton**  
Partner  
McGrathNicol



**Stephanie Crowe**  
First Assistant Director General,  
Cyber Security Resilience  
Australian Cyber Security Centre,  
Australian Signals Directorate



**Rob Wiggan**  
Cybersecurity Advisory  
WTW



**TM Ching**  
Security Chief Technology  
Officer, Asia Pacific  
DXC Technology



**George Abraham**  
Chief Information Security  
Officer  
Novatti Group



**Sean Deuby**  
North American Principal  
Technologist  
Semperis

# Understanding Active Directory Risk Today

*The importance, ubiquity and age of Active Directory installs combine to create a considerable access risk*

Active Directory is a centralised repository that stores information about users, computers and other resources in a network.

The service provides authentication, authorisation, user and group management, policy enforcement and a hierarchical structure for organising information. As such, it is an essential component in large organisations for managing networks, users and systems.

Long having been the central database for users, computers and resources in the networks of most large businesses, Active Directory also represents an attractive target for cybercriminals, with estimates suggesting it is [exploited in 90% of cyberattacks](#).

The Australian Signal's Directorate's First Assistant Director General for Cyber Security Resilience at the Australian Cyber Security Centre, Stephanie Crowe, says from its release with Windows 2000 and continued integration into Microsoft products ever since, Active Directory has become a near ubiquitous system in Windows Networks.

"Successful compromise of Active Directory will typically give an adversary the keys to the kingdom, providing access to nearly all systems, applications, and resources," she says.

"Effective Active Directory management is vital to protect credentials, applications, and sensitive data from unauthorised access. Taking action early limits the impact of a breach, and can prevent the adversary in further compromise of the network."

Jamie Norton, who is a partner with specialist advisory firm McGrathNicol and a former CISO for the Australian Taxation Office, similarly observes the ubiquity of Active Directory in organisations today, saying there would be very few large organisations that wouldn't use Active Directory, unless they had made a very specific choice from their beginnings to use alternative technologies.



Norton adds that it is important not to forget this underlying architecture when talking about identity and access management.

"Often there will be multiple Active Directories within the environments of large organisations," he says. "The IAM (identity and access management) space typically provisions into Active Directory. Assuming that you are using Active Directory for authentication and authorisation, how things get into Active Directory, how things are removed from it and all of the hygiene around that is critical to IAM.

"For example, you need a process and framework to integrate your users with your payroll system as people get onboarded. Which roles get provisioned into Active Directory, what permissions they get and what authorisations they have are key considerations.

"That doesn't have to be done within Active Directory itself, Active Directory can just be the transactional piece where you then have other systems that manage the identity. And some organisations do use Active Directory almost like an identity store, rather than as a technical building block.

"However, it remains the underlying directory that will provide opportunities for bad actors if not well maintained."

## Risks with Active Directory

The risks inherent in credentials and user account management is well known in the modern business world, and organisations today think a lot about identity and access management.

One major risk when it comes to Active Directory and its associated infrastructure relates to legacy IT, particularly how these databases and domain controllers have been established and then maintained in big, decades-old organisations.

Rob Wiggan, Cybersecurity Advisor with global risk management consultancy firm WTW, who has also held security leadership roles in higher education and the banking sector, says that in many cases it is infrastructure teams who build and maintain domain controllers and user directories, often without the security team's direct involvement.

"In a number of the organisations I've observed, the Active Directory might be 15 years old from when it was first developed," he says. "When people first started working with Active Directory, they didn't really understand the power that it would have in 10 or 15 years' time.

"The CISO role and security team's role was not to determine the construct of the directory, but more often thinking more about what controls to have in place, similar to how many other applications in an environment are approached from a security perspective, with certain permissions and authentication for use.

"So, there are many Active Directories that have no real structure to them, they've got users in them that have been there for a long time. They may be disabled or they may not be. There may also be user objects within that Active Directory that are critical to the running of certain applications in the organisation, particularly organisations with a lot of legacy."

Decades of organic growth for certain Active Directory forests runs at odds with the approach organisations are leaning

into today with application development, configuration and design done with security in mind from the ground up.

Jamie Norton says over time, without modern risk oversight and Active Directory governance, these services can become disorganised.

"I don't think it will be too revealing to say that most large organisations are going to have a degree of untidiness in their Active Directory," he says.

"Typically, there will be multiple forests and multiple instances of directories that have different Active Directory data in them and that may be based on different environments, like development environments or production environments. It could even just be a bit all over the place depending on how it has transformed and morphed over time.

"Unless you are very diligent from the start and you've got a process that's very robust, you will end up with an Active Directory that's got different artefacts that shouldn't be there, and things that have been left to rot over time. You end up with an Active Directory where no one really knows everything that's in there. There will be scepticism over whether there are

*"I don't think it will be too revealing to say that most large organisations are going to have a degree of untidiness in their Active Directory."*

**Jamie Norton**  
Partner  
McGrathNicol

people still in it that shouldn't be, or objects still in it that shouldn't be, and you lose overall confidence that your Active Directory is up to scratch.

"Then, as a big organisation, you have to look at how you start again and rebuild, which is like trying to fly the plane and build it at the same time. You have production environments that can't stop while you're trying to redefine your whole directory structure.

"This also impacts the applications that interact with it, and whether the artefacts inside are there from a bygone era or there because they need to be there. Rectifying that is a huge challenge."



## A Vulnerable Target

The ubiquity of Active Directory as the underlying software and infrastructure for authentication and authorisation, coupled with years of potential sprawl and patchy governance, makes these services a target for attackers.

Australian Cyber Security Centre's Stephanie Crowe says Active Directory is commonly exploited by adversaries after obtaining an initial foothold in a network.

"Attacks will often focus on gaining an understanding of the network and subsequently moving laterally through the network to sensitive systems and accounts, and elevating access by compromising privileged accounts," she says.

"There are many publicly available tools that make targeting Active Directory achievable with relative ease, and if the attacker is successful, they are easily able to hide their tracks, which can make it difficult for organisations to detect."

McGrathNicol's Jamie Norton agrees, noting that gaining access to Active Directory and domain controllers enables attackers to create their own credentials that pass as being totally legitimate.

"Particularly if Active Directory is in a bit of an untidy state, it's less likely to be monitored well, and it may be misunderstood," he says.

"That means there is less chance that any alerts will be raised if an attacker does happen to escalate privilege to, say, a domain admin account.

"This then feeds directly into the ability for threat actors to create their own illegitimate credentials that are genuine as far as the system is concerned.

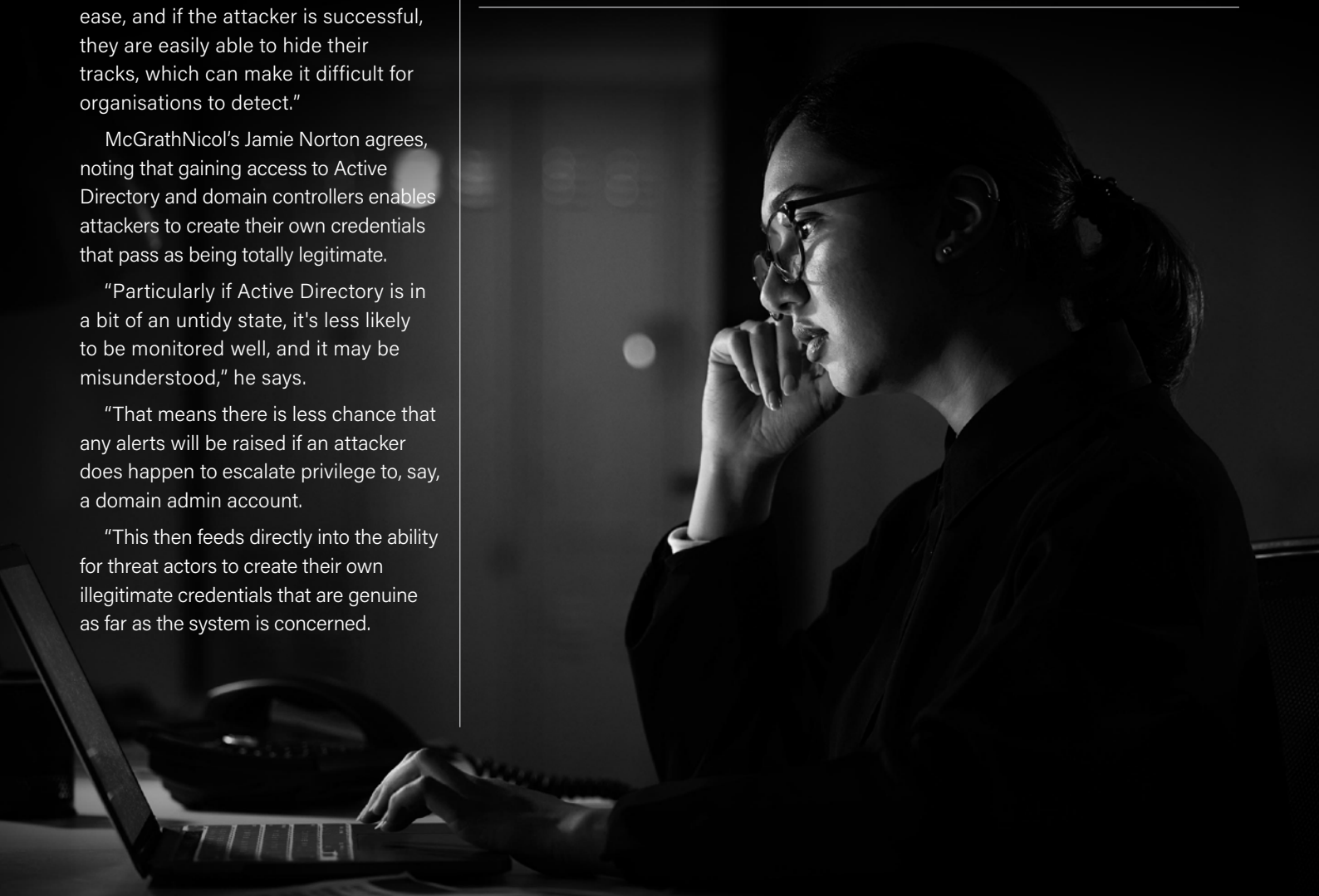
"Once that's done and the trail is removed, a hacker has persistent access into the system. The chances of those on the operational side of security discovering the adversary in the network is then very challenging. It is much harder to track at that point.

"There's probably a lot more of this happening than we think because it's a risk factor that you just can't spot easily unless you have really good governance over your Active Directory."

Based on its engagement across the Australian economy, the Australian Signals Directorate understands the most common Active Directory attacks and vulnerabilities exploited by bad actors to include:

- Plaintext passwords in user-accessible locations
- Kerberoasting and authentication service response message (AS-REP) roasting
- Weak passwords and password configurations
- Overly privileged accounts
- Insecure domain controllers

The risks areas around legacy or ungoverned Active Directory installs are exacerbated by the changing wider cybersecurity landscape, which we will touch on in the next chapter while examining the drive to increase maturity around Active Directory security. ■



# Gauging Maturity and Awareness

## *A changing security landscape calls for attention toward Active Directory security maturity*

As the number of online interactions and transactions has increased over the years, not to mention the remote work shift, the risk of identity theft, data breaches and ransomware has also increased. Hackers have also become more sophisticated in their methods.

This is driving a renewed need to examine Active Directory governance and to scrutinise the maturity of the cybersecurity industry in Australia when it comes to dealing with this risk.

Payments company Novatti Group's Chief Information Security Officer George Abraham says that identity has become a huge focus given its position in the attack kill chain.

"For a significant cybersecurity breach to play out, you need two things. You need access to the system, which in our world is mainly presented as a TCP/IP connection or a network connection, and the other thing you need is a set of credentials to get onto the system," he says.

"Ten to fifteen years ago, most systems were internal to the network on local data centres behind enterprise firewalls.

The kill chain was broken that way. But now, many organisations are on the cloud and accessible via the internet.

"The security industry has moved to create very robust authentication technologies because the kill chain is halved and network access is easily available, so the next opportunity for a lot of security teams and CISOs to prevent a breach is to secure the credentials."


Given the role identity and credential security now plays, poorly configured or ungoverned Active Directory services and domain controllers will only present more of a risk to organisations the longer they are not dealt with.

In its Annual Cyber Threat Report for 2021-22 the Australian Signals Directorate reported observing a shift in cybercriminals' behaviour, with an increased focus on privilege escalation and lateral movement within victim networks.

"As organisations have become better at dealing with ransomware incidents, through more effective regular backups and an increased ability to deal with commodity malware, adversaries have been forced to adapt in order to stay profitable," says ACSC's Stephanie Crowe.

"Escalating privileges and moving laterally through a network allows cybercriminals to increase their chances of success by destroying secured backups, disabling network and endpoint protections, and disrupting IT systems to hinder defenders.

"Based on ASD's experience, Active Directory is almost always targeted in order to achieve these goals."



*"The security industry has moved to create very robust authentication technologies because the kill chain is halved and network access is easily available, so the next opportunity for a lot of security teams and CISOs to prevent a breach is to secure the credentials."*

**George Abraham**

Chief Information Security Officer  
Novatti Group

## Maturity

As the focus on identity security has increased in recent years, have knowledge and maturity around Active Directory's role kept up?

Australian Cyber Security Centre's Stephanie Crowe says in Australia, there is room for improvement in this area.

"In ASD's experience, organisations are failing to adequately secure Active Directory for a number of reasons, including: a lack of visibility of insecure configurations; complex environments; a lack of in-house expertise; and legacy systems requiring insecure configurations, or not supporting secure features," she says.

"Active Directory is often not listed as a priority for security uplift, even in organisations with significant security flaws, implying these issues are not well known or understood."

DXC Technology's Asia Pacific Security Chief Technology Officer, TM Ching, says the maturity of Active Directory security can be broadly evaluated through the lens of small, medium and large organisation sizes in the Australian market.

Starting with the small organisations, with 50 seats and below, Ching says there is typically no knowledge of Active Directory security.

"For small organisations, the Active Directory is mainly a mechanism to set up things like people logging into the corporate network to use printers, to access email etc. Beyond that, if something goes down, the security strategy will be to review processes after the fact," he says.

"Mid-size companies with 2000-4000 employees may have already been affected by a breach in their Active Directory environment and understand the importance of Active Directory security. The problem is, they may not have the resources to

supervise and protect the environment in real time.

"A lot of mid-sized organisations treat Active Directory just like another IT asset and secure it through a generic means such as a firewall, restricting who can access the Active Directory firewall and installing endpoint agents. Those operate at the operating system level, not really at the application level relative to what Active Directory does."

At this level, Ching says a more suitable protection might include intelligent monitoring that would raise an alarm if there was abnormal user behaviour from an Active Directory. Often this is not what mid-sized organisations are equipped with.

Ching says the organisations at the top of the maturity curve are large organisations, like banks. These companies have the skills to deal with Active Directory security and know the importance of it. Of course, there is a reason that large organisations are in this position.

"Very few organisations are like this, because you need to have the skill, you need to have the size, you need to have the team and the resources in order to manage it," he says.

"Unfortunately we see mid-sized and small organisations struggle with this."

*"Unfortunately we see mid-sized and small organisations struggle with this"*

**TM Ching**

Security Chief Technology Officer,  
Asia Pacific

DXC Technology







## Visibility and Awareness

While groups like the Australian Computer Society's Technical Security Committee have produced presentations and information to grow awareness on improving Active Directory security locally, McGrathNicol's Jamie Norton says there hasn't quite been enough cut-through at an executive level for many organisations.

"It's one of those technologies that I think we [in the industry] have been slow to catch up with the fact that the governance around Active Directory needs to be really strong," he says.

"It's a bit of a double-edged sword. You need really strong security governance around it but at the same time, it sits at the core of the operational part of an organisation, which is often managed by the infrastructure team, and things need to go in and out without someone constantly watching over it.

"It's not like change control where you can vet every change. I think what

is needed are strict mechanisms by which things go in and out, but not necessarily humans looking at that all the time.

"I think there needs to be more focus on control and auditability when adding or removing objects from Active Directory. It's the classic case of the infrastructure team not necessarily appreciating the security implications of what happens if objects are lacking in hygiene and actions are just performed as and when the business calls for it."

Sean Deuby, North American Principal Technologist for Active Directory security solution provider Semperis, similarly commented that awareness was a key piece of the maturity curve, noting that he had observed this awareness starting to grow in the Australia and New Zealand region.

"The pattern of thought tends to be that Active Directory is, 'just looked

after by an infrastructure guy in the corner' and the rest of the business thinks, 'it just works, it's never been a problem, why care?'," he says.

"I saw this in ANZ. People don't think they'll be affected. But it doesn't matter if you're in the US or Australia, the only difference is latency. If you're online, you're exposed.

"What I've seen in the US, then Europe, is this pattern of companies saying that their Active Directory just works, they're not worried about it, they're backing it up, it's OK. But when company leaders learn how they are at risk and the size of that risk, they do have kind of an, 'Oh no!' moment.

"The knowledge is growing. Where I see ANZ right now is more in the growing awareness stage of the curve." ■

# Resilience Strategies and Challenges

## *Recognition of risk, assessing threats and targeted investment will support good basic hygiene*

Active Directory is clearly an important component of an organisation's security architecture given the increasing security challenges of the modern, digital world. However, the organisations that are best equipped to have this security are often the largest.

Given that Active Directory is almost always targeted by cybercriminals looking to escalate privileges and move laterally through a network, as per the Australian Cyber Security Centre's advice, organisations of all sizes should be cognisant of this risk and take steps to protect themselves.

In the first chapter, the ACSC's Stephanie Crowe outlined some of the most common vulnerabilities related to Active Directory. In this chapter, we will cover building some of the ACSC's advice for resilience against these attacks. Further, we will examine other defensive considerations before lastly exploring some common challenges.

### Plaintext Passwords

When it comes to plaintext passwords, the ACSC's Stephanie Crowe says developers and administrators should not store passwords within scripts and scheduled tasks, which may be discovered and used to take over accounts of interest.

"Passwords should not be stored in user-readable fields within Active Directory, such as description and userPassword," Crowe says.

"Defenders should ensure proper processes and technologies, such as Privileged Access Management (PAM) solutions or enterprise-grade password managers, are in place to prevent passwords being stored in user-accessible locations. It is recommended that the network is regularly searched for credentials, and if any incorrectly stored passwords are discovered, the reasons why should be explored."

### Kerberoasting

"In Kerberoasting attacks, password hashes are obtained and taken off the network by an adversary, then cracked to reveal the plaintext passwords," Crowe says.

ACSC experts advise that to mitigate this attack, only service and computer accounts should be configured with

SPNs and Kerberos pre-authentication should be enabled for all accounts where possible. Any account with a SPN, or without Kerberos pre-authentication, needs to have a long (30+ characters), complex, and unique passphrase.

### Weak Passwords and Password Configurations

For increased password resilience, ACSC experts say highly privileged accounts, such as the Kerberos Ticket Granting Ticket (KRBTGT) account, administrative accounts, and machine local administrator accounts, should have increased security controls and monitoring in place.

"In particular, the KRBTGT account password should be changed twice every 12 months, using a long, complex, and unique passphrase. Local administrator accounts can be managed within the domain using Microsoft's Local Administrator Password Solution (LAPS)," ACSC experts advise.

"To mitigate these attacks, organisations should enforce strong password policies within the domain, and rotate the KRBTGT account password every 12 months, in line with Microsoft's KRBTGT guidance. PasswordNeverExpires and PasswordNotRequired should not be set on accounts."

### Overly Privileged Accounts

Hackers will prioritise attacks on accounts or users that have high-level privileges, so the ACSC also advises that accounts should not be provisioned with any further privileges than absolutely required. Restricting unnecessary access to the internet will reduce the opportunity for adversaries to compromise these accounts.

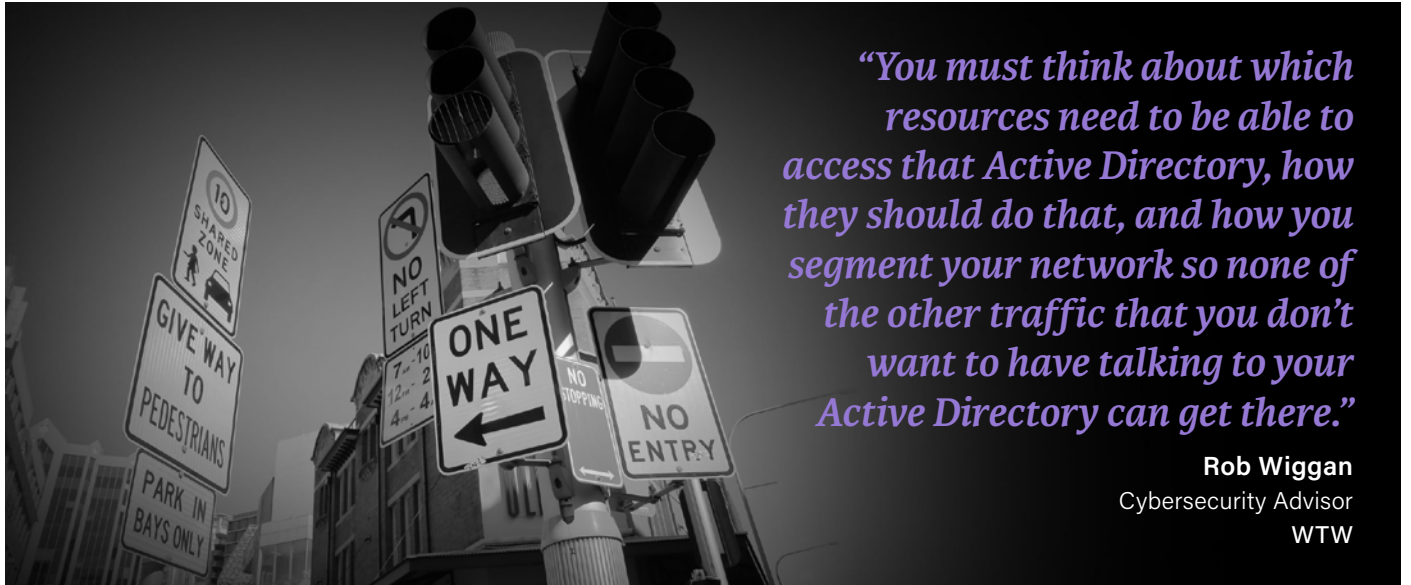
"Domain Administrator accounts should not be used in place of accounts with more restricted permissions," Crowe adds.

### Insecure Domain Controllers

Domain controllers, the computers that run Active Directory and provide its primary service to member servers on the network, should be tightly locked down.

"Defenders should restrict access to these systems to a small set of dedicated accounts that are not used for other purposes," Crowe says.

"Taking steps to harden domain controllers, such as limiting the software installed, and applying security patches within a short timeframe, will further reduce the risk of an adversary compromising and gaining complete control over all systems and computers in a network."



*“You must think about which resources need to be able to access that Active Directory, how they should do that, and how you segment your network so none of the other traffic that you don’t want to have talking to your Active Directory can get there.”*

**Rob Wiggan**

Cybersecurity Advisor

WTW

## Segmentation and Ownership

Beyond good hygiene practices, our contributing security leaders also shared further insights and key considerations based on their experiences protecting Active Directory services.

WTW’s Rob Wiggan emphasises that security leaders need to think about how Active Directory interfaces with the rest of the environment, with considerations both for on-premises IT and cloud.

“If you’re on-prem, you have to think very carefully about where Active Directory is in your network and how it can be accessed. You must think about which resources need to be able to access that Active Directory, how they should do that, and how you segment your network so none of the other traffic that you don’t want to have talking to your Active Directory can get there,” he says.

“If you’re using Active Directory in the cloud, you don’t have the complication of the physical hardware that you have to secure, but you still need to manage your users. In both cases, cloud and on-prem, you really must have a good handle on your domain administrator accounts.

“You shouldn’t have very many of those at all. When a user requires it, it

should be allocated to them to do the task they need to do, and then be revoked.

“One of the positives about cloud is that there are some very good security baselines that are being applied in cloud services. People who are configuring those services are doing so with security in mind, which doesn’t always happen to the same rigor on-premises.”

Meanwhile, McGrathNicol’s Jamie Norton says organisations should consider rethinking the traditional approach of the infrastructure team owning Active Directory.

“I like the model where security is the system owner, possibly even the business owner depending on the nature of the organisation,” he says.

“Having security own Active Directory as an outcome is worth considering. Infrastructure can obviously manage Active Directory on a day-to-day basis, but security should actually own it, given how critical it is to the overall security of the organisation.

“Within that, you need to start with a known good. Taking an existing, years-old Active Directory and trying to go through each artefact and fix it is almost impossible to do in a large organisation. You just can’t get the

scale you need. You basically need to start again to ensure that you have a known good, and that you are not copying potentially malicious credentials back across into the new version.”

Norton says that once security teams can establish that Active Directory has this known-good baseline, another strong security control is to configure it so that no one in the organisation can access it to add or remove objects.

“You don’t want anyone putting anything into Active Directory manually,” he says. “It should only be specific workflows. In the case of someone being onboarded, there’ll be a payroll or HR system that would be the trigger to provision data into Active Directory via an identity and access management solution interface. There would also be a corresponding action if someone was to leave the organisation.”

Norton adds that when credential entry is done this way, it enables the security team, using security monitoring tools, to instantly raise an alert if anyone attempts to access Active Directory, given that the need for manual, human management has been engineered out of the process.

## Testing, Tooling and Investment

An important aspect of any security strategy is that processes are documented and recovery plans are practiced in the event of an outage or breach.

When it comes to Active Directory recovery, Semperis' Sean Deuby says extra attention is required given the service's complexity.

"Active Directory is not your average application to recover in a disaster recovery situation, it is fiendishly difficult," he says.

"The process is called forest recovery, and if you talk to any Active Directory professional that has ever been through a forest recovery process, they never want to do it again.

"It is 28 manual steps that you must do perfectly across multiple domains and across multiple individual servers in multiple data centres. And if you get it wrong, you may have to start over. It takes a long time to do it."

Deuby adds that in the event of a security crisis in the middle of the night, CISOs are doomed without a prepared and practiced plan.

"It's not something you can sit down and figure out in the moment, that's a recipe for disaster," he says.

"The CEO is calling you asking how things are going, you can't use Zoom, you can't use Teams because the infrastructure has been attacked. Your crisis bridge that you've invited people to may have threat actors listening in to hear what steps you plan to take. It's mayhem.

"At the very least you have to practice like crazy, but sadly I know a lot of people don't do this enough."

For DXC's TM Ching, protecting Active Directory revolves around three main factors: recognition, assessment and investment.

"First and foremost is the general acknowledgement that within a security investment, Active Directory is a critical

control. A lot of organisations don't identify Active Directory as a critical control and that's a big mistake," he says.

"Most mid-sized organisations do not build Active Directory to be resilient, and when its importance is not wholly understood, things start to go wrong. This might occur when there is no backup of the Active Directory forest and there is a need to restore it after a security incident.

"The amount of information that's stored in an Active Directory needs to be understood. Organisations need to know what a password can be used to do in the event it is stolen. In the first instance, it's important to ensure cognisance of the Active Directory.


"The next element is to perform a technical assessment. You can do this yourself or engage a third party. This will form a threat assessment of your attack vectors, which you need to test on your environment to know

how susceptible you are to a potential breach.

"This will also help you find out if it's the controls that you need to build around protecting Active Directory or if it's a bigger, more systemic problem related to the process of how you manage your entire environment.

"Once you acknowledge Active Directory as a control and you have done an assessment, the third step is to determine what exactly you can put in or do to mitigate the relevant attacks. Is it through a technical control? Is it through a process? Is it through education? Or is it through investment of resources?"

Importantly, Ching says, the investment an organisation makes in protecting Active Directory needs to be balanced with the risk of that asset being breached. It's critical to know the most cost-effective way to get the best result based on the threat assessment.



*"If you talk to any Active Directory professional that has ever been through a forest recovery process, they never want to do it again."*

**Sean Deuby**

North American Principal Technologist  
Semperis

## Challenges

In the pursuit of any security outcome, there will always be challenges that arise along the journey.

Having heard from security professionals on strategies and considerations for protecting Active Directory, we asked them which challenges might arise for other CISOs looking to harden this area of their security environments.

While we have discussed how to prioritise investment areas for security control, choosing the technologies to invest in can still pose a challenge, according to Novatti's George Abraham, given the number of available technologies in the market.

"I think the question a lot of CISOs are trying to solve is where do we invest more? Do we want to invest in preventive capabilities or do we want to invest in responsive capabilities?" he says.

"I don't think from a technology sense we are ahead or behind. I think it's more around how companies invest to get the extra protections in authentication and identity and access management."

The Australian Cyber Security Centre's Stephanie Crowe lists several significant challenges to securing Active Directory.

"These include staff skillset shortages; the complexity of the corporate environment, particularly in hybrid deployments as organisations move into the cloud, and where multiple domains have been combined; limited and complex tooling to understand and remediate issues; and cultural issues, where staff are not encouraged to hunt for or report on security problems," she says.

WTW's Rob Wiggan says some challenges are tied to the basics of identity and access management. Seemingly straightforward processes such as revoking access and removing accounts when someone leaves an organisation can sometimes be more complicated depending on the kind of environment you work in.

"Removing dormant user accounts can be done 80% of the time but there are some situations where a user may own an object within an application and must stay in the system until the app is reconfigured, which in reality, often doesn't happen because it isn't 'broken' per se," he says.

"There are lots of those sorts of considerations. If you've got basic hygiene factors in place, you will do pretty well. When I worked in banking there was a lot of rigor around the termination of users, for instance.

"However, in the education space, for example, there can be a lot of special user requirements, particularly in the research world. That means some accounts need to be maintained and not necessarily deleted as soon as the relationship ends. Things like that are sometimes beyond the CISO's control." ■



# Conclusion

In a highly connected world with ransomware on the rise, identity has become a leading threat vector and vulnerability for organisations globally.

With privileged access being a highly sought after asset for cyber criminals, the risks inherent in unprotected Active Directory installs and infrastructure should not be ignored.

Active Directory is targeted by almost all cybercriminals looking to gain greater control over a network after usurping a single set of credentials.

With a long legacy in business systems, Active Directory has in some cases become subject to sprawl and artefacts created due to years of infrastructure growth and change, with less-than-ideal security oversight.

In reviewing Active Directory security, one of the first things security leaders need to ask themselves is how well they understand the state of their organisation's Active Directory when it comes to hygiene, scope and risk.

Following that, creating a more resilient user directory environment and configuration should be complemented with testing, governance and the other considerations mentioned by the security leaders contributing to this report.

As often is the case, gaining investment and executive buy-in can put up challenges. However, knowing the risks and growing awareness of these and others issues in the identity security space should help security leaders chart a course forward. ■

## About Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%.

Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organisations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies.

For more information, visit [www.semperis.com](http://www.semperis.com)



## About the Editor

Michael Jenkin is an editor and journalist with more than a decade of experience producing content across broadcast, print and digital media. He specialises in business technology reporting and analysis.

At Corinium, Michael develops content to inform and support data and analytics and information security executives.

To share your information security story or enquire about appearing in a Corinium report, blog post or digital event, contact Michael directly at [michael.jenkin@coriniumgroup.com](mailto:michael.jenkin@coriniumgroup.com)



## Discover More Essential Information Security Insights

As anyone who has attended our global conferences or events will know, our 300,000-strong network of information security leaders boasts many of the most forward-thinking minds in the industry.

Our new content hub, **Business of InfoSec**, brings those same essential insights direct to you and is packed with exclusive research, video podcasts, in-depth articles, interviews, and reports. Discover how other information security leaders are tackling the challenges they face today while maintaining the confidentiality, integrity, and availability of their organization's data.

For a limited time, subscribing to the **Business of InfoSec** is free. So, make sure to subscribe today for complimentary access to exclusive insights you just can't find anywhere else.

**SUBSCRIBE NOW**



# Corinium

## Partner with Business of InfoSec by Corinium

We'll develop industry benchmarking research, special reports, editorial content, online events and virtual summits to establish your brand as an industry thought leader.

**FIND OUT MORE HERE**











## Discover Corinium Intelligence

Corinium is the world's largest business community of more than 700,000 data, analytics, customer experience and digital transformation leaders.

We're excited by the incredible pace of innovation and disruption in today's digital landscape. That's why we produce quality content, webinars and events to connect our audience with what's next and help them lead their organisations into this new paradigm.

Find out more: [www.coriniumintelligence.com](http://www.coriniumintelligence.com)

## Connect with Corinium

-  Join us at our **events**
-  Visit our **blog**
-  Read our **reports**
-  Follow us on **LinkedIn**
-  Like us on **Facebook**
-  Find us on **Spotify**
-  Find us on **YouTube**
-  Find us on **iTunes**