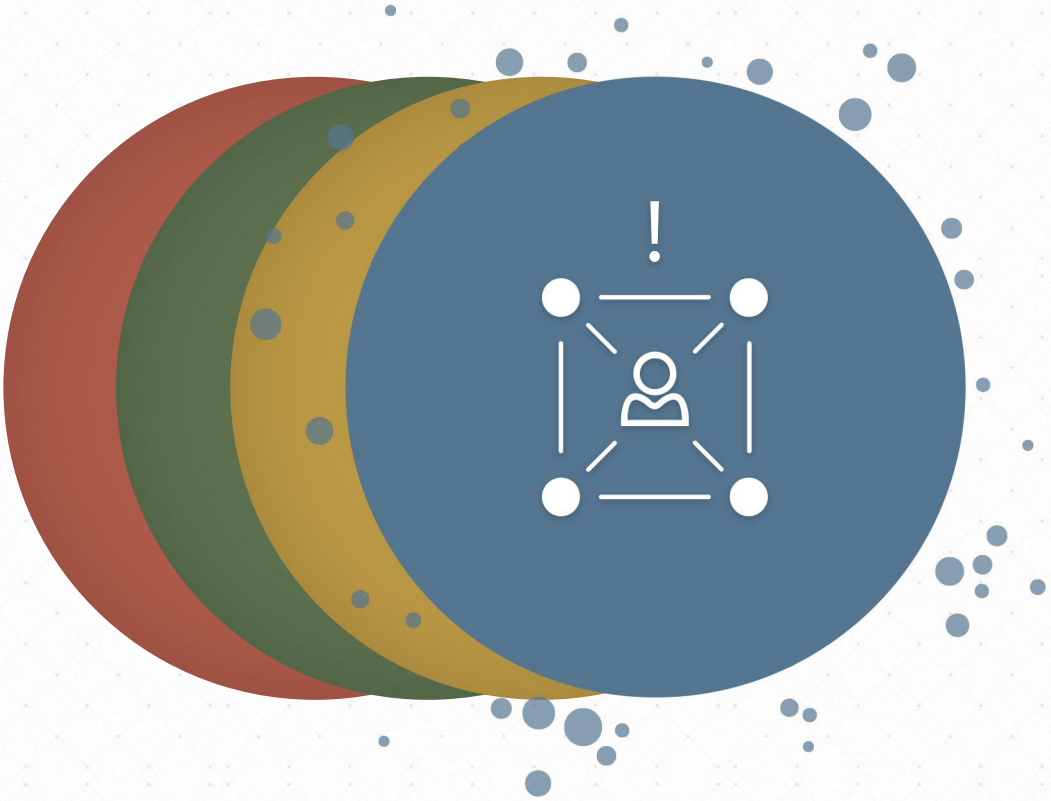
REPORT | 2017

State of Group *Insecurity.*

The 2017 State of Group Insecurity Report.



imanami

Imanami, a Microsoft Gold Certified Partner, is the leader in Group Management Solutions.

It has been an age-old management problem – no one really wants to manage groups. Modifying group memberships is the most mundane of tasks, and there are plenty of seemingly more important projects IT needs to attend to. In the last few years, there has been a rejuvenated focus on security, thanks to the rising amount of cyber-criminal activity; malware, ransomware, data breaches, and espionage – all having a material impact on the business.

In 2016, the average data breach caused a little over 8 hours of downtime, and impacted operations (**36%** of the time), finance (**30%**), brand reputation (**26%**), customer retention (**26%**) and involved intellectual property (**24%**) .[1]

In most cyber-attacks, credentials with elevated privileges are a primary focus by attackers. Using tools designed to seek out and extract credentials, attackers look for any account that gives them greater and greater access. The basis for this desired elevated access is all based on group membership in Active Directory. Groups provide access to systems, applications, and data – both on-premises and in the cloud, as well as are utilized by countless security platforms and solutions to organize the application of security policy and capabilities.

Because of this alone, the proper management of groups shifts from mundane IT task to critical part of the security strategy.

However, even with the increase in security concerns, are groups being properly managed?

To find out, Imanami asked members of IT organizations about who is managing Active Directory groups, what security is reliant upon groups, how IT works to keep groups secure, and whether the measures they are taking to maintain security through proper group management is effective or not.

Let's begin the report by looking at a bit about the directory environments and how it's being managed.

Active Directory: 2017

When it was first released, every AD environment was relatively the same – on-premises only, managed completely by IT. But with the advent of the cloud, Shadow IT, and a multitude of security solutions to create a layered defense for organizations, today's IT no longer can be categorized with such a simplistic single statement.

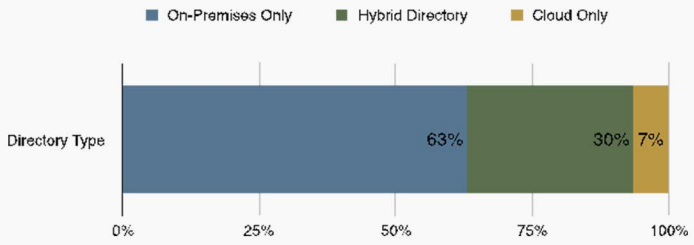
So, what does the directory look like, who's managing it, and how?

---

[1] Cisco, Annual Cybersecurity Report (2017)

Where's the Directory?

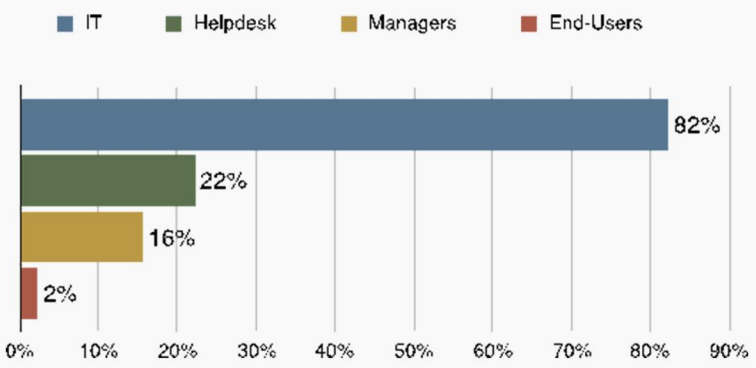
With the introduction of cloud-based directory services that synchronize with Active Directory (Azure AD, for example), as well as the cloud-based services that rely on those cloud-based directories (Office 365 being the obvious example here), the assumption that an organization's directory is solely on-premises (or even on-premises at all) is no longer a viable one. When asked how to best characterize their directory environment, the mix of answers came as no surprise. As shown below, the majority of organizations are still on-premises only, with slightly less than a third synchronizing with some cloud-based directory service.



While a small number, the percentage of organizations utilizing a purely cloud-based directory is still surprising. And it's the medium-sized enterprises (those in the **1000-7500** employee range) that are either adopting a hybrid-cloud directory or embracing a cloud-only directory.

Who's Managing Groups?

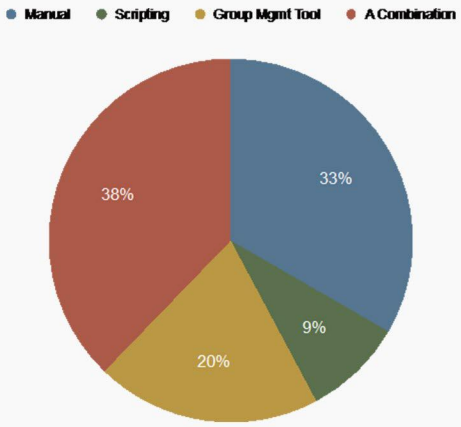
While this may be a question where you assume the answer is IT, there is a growing trend of organizations utilizing department heads, line of business owners, application owners, and even end-users to self-manage group management (usually via a third-party solution that establishes limits and policy of what changes are allowed). When asked, we did see the unsurprising abundance of organizations (**82%**) leaving the work to IT (shown below), with a respectable number of organizations allowing managers and end-users (nearly **18%** in total) to manage their group memberships.



With IT being the primary work force, it clearly indicates that they are a likely bottleneck in change management. They are also distanced from those LOB application that typically leverage groups, making IT the least likely to be informed on membership accuracy.

What Tools Are Used to Manage Groups?

The effectiveness of your group management – and the security it provides – depends heavily upon the tools being used. If group management is a cumbersome task (in addition to it already being tedious) because of the methods used, it becomes one of those tasks that falls to the bottom of the priority list. When asked about the tools used to manage groups, we found that nearly **40%** used a combination of tools, with a third using the built-in AD management tools.

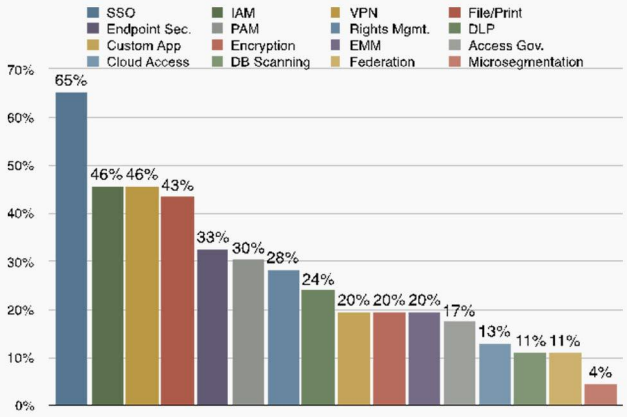


What Critical Security Relies on Active Directory Groups?

Nearly every solution addressing security utilizes groups in AD as the basis for establishing in-solution policy and privileges. So, it makes sense to better understand exactly how much influence AD groups have an organization's security.

We provided a laundry list of initiatives implemented today to improve an organization's security stance (shown below) to our survey respondents, inquiring whether AD groups are the basis for each of those initiatives.

Only **20%** of organizations are currently using a tool dedicated to managing groups and, despite the extensive capabilities available, only around **9%** of organizations use Scripting, such as PowerShell. This use of in-house tools and scripts to address mission critical changes leaves much to potential error.



While Single Sign-On, IAM, and VPNs were the top three security initiatives, what is important here is the overall use of groups as the basis for many, many different types of initiatives that secure the organization from different attack vectors.

Because groups are the backbone of your security, it's critically important that they be managed properly and consistently. That's why we sought to determine exactly how organizations today manage the one part of IT that has greater security implications than any other - Groups.

Group Management: 2017

> *Looking beyond the daily changes needed, we sought to understand whether groups were being ap proached as a part of the IT infrastructure that is continually managed – the difference being that daily management simply focuses on the requested tasks put in front of IT, while true group management focuses on establishing designated ownership of each group, along with the periodic review of the current state of each group.*

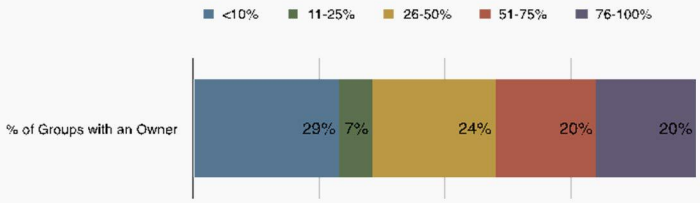
In the most mature of IT organizations, a group is managed from cradle to grave, putting each change made under scrutiny. An owner is assigned to each group who is then responsible for membership changes, permissions assigned, and whether the group needs to continue to exist. In larger organizations, this may evolve into a number of owners, each responsible for one part of the group. IT extends management functions and ownership out to those department heads, line of business owners, and even end-users that are closest to a groups purpose to ensure each parts of a group's use is up-to-date and as secure as possible.

But, not every IT organization is this mature – so, what does group management today look like?

Do Groups Have Owners?

Assigning a group owner is much more than just filling out the Managed By field. Instead it is the initial step in putting a lifecycle management methodology in place. Owners should be the ones that approve membership changes, permissions assigned, and even a group's very existence in AD. As shown below, nearly one-third of organizations have less than **10%** of their groups assigned an owner.

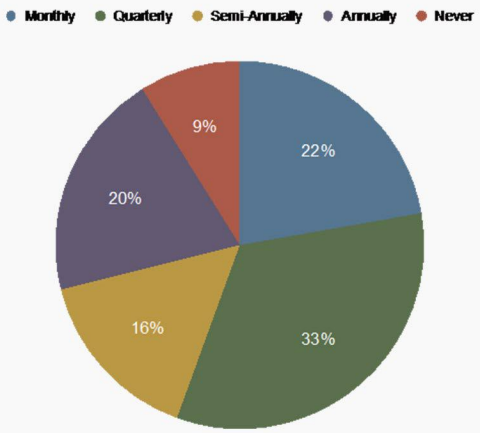
> *A majority of organizations (**60%**) have assigned owners in less than half of their groups.*



This lack of ownership isn't surprising, given the previously mentioned self-adoption by IT to take on the task of group management. What is surprising is the organization sizes that have the least ownership defined: two-thirds of mid-sized enterprises (those with **2500-5000** employees) have a defined owner in less than **10%** of their

Are Group Memberships Being Certified?

In a proper group management lifecycle, the members of a group should be reviewed and certified by a group owner, ensuring only those that should be members, are members. This is critical – given the vast number of security initiatives previously mentioned reliant upon group memberships being accurate – and should be done at least quarterly. We found that almost half of the organizations surveyed do not evaluate memberships at least quarterly – with **9%** of orgs never certifying group memberships.

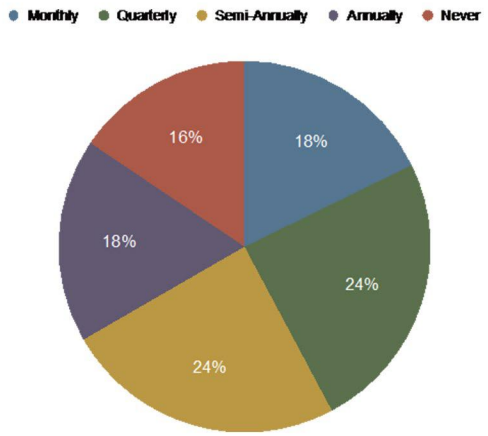


This is likely due to the lack of ownership, and the self-reliance upon IT to perform all management tasks, as indicated by the increase in-group membership certification frequency by those organizations embracing end-users or managers to assist with group management. Those utilizing end-users certified memberships monthly and over **2/3rd** of those utilizing managers did so monthly or quarterly.

Are Group Memberships Being Certified?

As with membership certification, group attestation is a necessary part of the group management lifecycle. Owners of groups should be attesting to a group's necessity to organization at least semi-annually, calling on a group to be deleted should it no longer be needed. As shown below, we found that one-third of organizations are not performing group attestation at least semi-annually – with **15%** of orgs never performing attestation.

Organizations performing attestation either annually or never ran the gambit of organization sizes, and those organizations utilizing end-users and managers did so at least semi-annually.

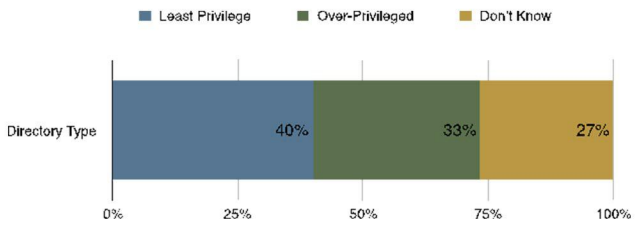


Are Your Groups Creating a State of Insecurity?

We've seen in this report the high number of security initiatives that rely on groups, and the lack of proper attention and management groups receive. Without assigned (and accountable) group ownership, along with membership certification and group attestation, organizations run the risk of leaving groups to evolve without review. The presence of empty groups, repurposed groups, the lack of process for assigning permissions to a group, and the absence of visibility into each of these circumstances puts the very foundation of the security found in AD – as well as every single security initiative that relies on AD groups – into question.

How Do You Characterize Your Access?

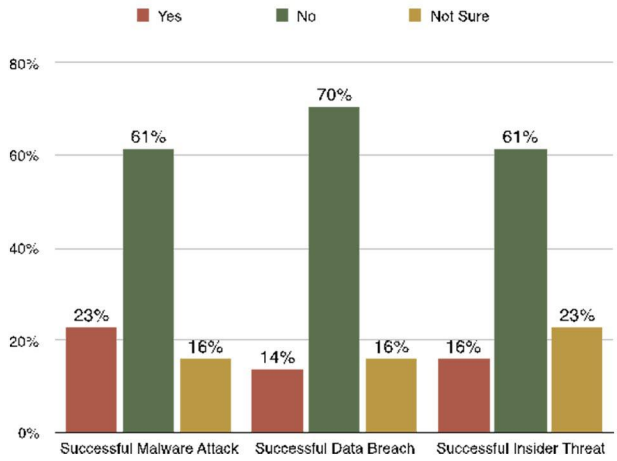
We asked respondents to characterize the access their users have, based on the frequency they manage groups. While **40%** believed themselves to be in a state of least privilege, the remaining **60%** considered their environment either over-permissioned, or were unsure.



Half of organizations that both certified group memberships and performed group attestation monthly characterized their environment as being in a state of least privilege – putting them above the average.

Putting Group Insecurity to the Test

Security is only as good as how well it stands up in the face of a threat. So, we asked organizations if they'd been a victim to three types of threats in the last **12** months – a malware attack, an external data breach, and an insider threat. As you can see below, the percentages of organizations experiencing these threats are relatively low.



But it's when you look at this data backwards and see just how secure any of the organizations experiencing an attack really are, you begin to understand just how important management of groups – and the influence on security they have – is to an organization.

Let's look at each threat and characterize the organizations experiencing them.

Threat 1: Malware Attack

Malware is simply the method by which an external attacker gains entry into your network. Once they've established a foothold by compromising an endpoint, the goal is to identify multiple sets of credentials and ways to gain elevated access, and jump from endpoint to endpoint until they've found some data of value they can exfiltrate. Because of the focus on obtaining elevated credentials, the need for groups to be configured correctly is critical.

Here's what the average organization experiencing a malware attack in the last **12** months looks like:

- ***60%*** are over-permissioned or unsure of the state of their security
- ***50%*** have group owners in less than half of their groups
- ***60%*** evaluate group memberships outside the recommend frequency
- ***30%*** perform group attestation outside the recommend frequency
- ***3 of the 16*** security initiatives reliant on groups are implemented

Threat 2: External Data Breach

This threat represents the sum of a number of attack vectors (which can include malware) culminating in a final action – the theft of data. This means they successfully navigated multiple endpoints, utilizing multiple sets of credentials, finding just the right one to access and steal the data they came for.

Here's what the average organization experiencing a data breach in the last **12** months looks like:

- ***67%*** are over-permissioned or unsure of the state of their security
- ***83%*** have group owners in less than half of their groups
- ***50%*** evaluate group memberships outside the recommend frequency
- ***50%*** perform group attestation outside the recommend frequency
- ***2 of the 16*** security initiatives reliant on groups are implemented

Threat 3: Insider Threat

The insider threat is the most difficult to spot, because the perpetrator is simply using the access granted them. So, if that access is incorrect – granting a user too much access – the risk of insider threat increases greatly.

Here's what the average organization experiencing an insider threat in the last 12 months looks like:

- ***57%*** are over-permissioned or unsure of the state of their security
- ***86%*** have group owners in less than half of their groups
- ***29%*** evaluate group memberships outside the recommend frequency
- ***29%*** perform group attestation outside the recommend frequency
- ***2 of the 16*** security initiatives reliant on groups are implemented

Conclusion

No matter how you look at it, each of the three scenarios above represent the current state of insecurity that exists today. Organizations just like yours are far less secure than they should have been. And, in many ways, they are the rea-world manifestation of all the data points brought forth in this report.

With rampant over-permissioning as a result of over-subscribing of group membership, no established process of owning and reviewing the state of groups, and with multiple enterprise initiatives resting their very security on an already rocky group foundation, this year's State of Group Insecurity report puts the spotlight squarely on the epicenter of one of your most critical security gaps – Groups.

By putting proper group lifecycle management processes in place – such as owners, certification, and attestation – and by leveraging users throughout the organization that can best determine whether this fundamental part of your security is correctly configured, organizations can quickly and easily shore up security and ensure it remains that way.