CORE SECURITY

Assessing the Risk of Identity and Access

Assessing the Risk of Identity and Access

March 2016

CORE SECURITY

Table of Contents

Foreword

Here at Core Security, our mission is to help customers succeed in a world of open access and increasing threats. We want to make sure that the right people have the right access to the right resources and that they are doing the right things with those resources. The question becomes, how does an organization assess those threats and gauge the risk it faces from both internal and external forces? Moreover, how do you plan for that risk and put in place processes to help detect identify and manage the risk?

Most Common Risks

With an increasing number of computers and other devices and an increase in the ways in which users access resources, access rights and the monitoring and managing of complex user access rights becomes harder every day. The stresses and strains of access can come from all over but the most common offenders are:

- **Routine changes** such as hiring, promotions or transfers
- **Business changes** such as reorganizations, the addition of new products, or new partnerships
- **Infrastructure changes** such as mobility, cloud adaptation, system upgrades, or new application rollouts

In addition to the stresses from business change, there are an increasing number of government regulations that require compliance, regardless of industry. From healthcare to bantling, these regulations climb into the hundreds and assuring that you are fully compliant is more difficult than ever. This increase in regulations along with the increase in complexity of access rights matles identity and access governance a red hot priority.

Routine Changes

Hiring

Promotions

Transfers

Termination

Project Teams

Customer Acquisition

Customer Management

Business Changes

Reorganization

New Product Intro

Union StriRes

Merger & Acquisitions

Geographic Expansion

New Partnerships

Infrastructure Changes

Mobility

Cloud App Adoption

Virtualization

New App Roll Outs

System Upgrades

New Infrastructure

What is Identity and Access Governance?

Identity and access governance tools establish an entire lifecycle process for identities in an organization, providing comprehensive governance of not just the identities but also their access requests. These lifecycle decisions are developed through real time intelligence and are informed by an organization's processes. When we are preparing for an audit we have to ask questions we had never been asked before Who has access to what? What does that access allow them to do? And why do they need that access? IGA helps to answer those questions up front to ensure that every identity has the right access, to the right things, at the right time.

When the internet was brand new, an organization had one room with only two to three people having access to resources. As a result, there was a pretty low risk of anyone hacking their way in. Now, our data centers are everywhere from a server room in a remote location to the cloud of everywhere-ness.

The result is that we have a broader and ever exploding attack surface and diversity of infrastructure. You've heard of the "Internet of Things" and these "things", that is, Internet-enabled devices and resources, such as a building thermostat or a household appliance, have increased the attack surface ten fold.

Unfortunately, we also are faced with a super sophisticated attacker ecosystem. Hackers are now working collaboratively, looking for weakness in your infrastructure and are armed with increasingly sophisticated and specialized tools and services. It may only take a hacker a few minutes to get into your system, but now they know that the payoff is worth waiting days or even months for the perfect time to strike.

The Issue of Compliance

If you look at the most recent Verizon PCI Compliance Report you will see that the average organizational compliance is at 93.7%. However, when you break that number down into the number of fully versus partially compliant firms, you will see that only 20% are 'fully' compliant. So if as organizations we collectively are compliant at 93.7%, then why have the total number of security incidents detected increased 48% since 2013? The answer is that we need more visibility into our systems. The top audit findings for the reasons behind these attacks are:

- **Excessive** access rights
- **Excessive** developers' access to production systems and data
- **Lack of** removal of access Following a transfer or termination
- **Lack of** sufficient segregation of duties

The biggest risk here is credentials. The number of stolen credentials is no surprise when you consider the number of transfers and terminations and accounts with excess access to sensitive systems that may remain active.

The Issue of Compliance

According to the Verizon Data Breach Investigations Report 2015 when asked if their organization is able to detect if access credentials are misused or stolen, 42% of companies surveyed in the report said they are not confident in their ability. Even worse, according to CSOOnline, 66% of board members are not confident of their companies' ability to defend themselves against any cyberattack. For those of us on the information security team, that shows a lack of boardroom trust in our capabilities.

42% of companies are not confident in their ability to detect if access credentials are misused or stolen.

Why do board members have so much trouble trusting our cybersecurity measures? Consider the fact that in 60% of cases, attackers are able to infiltrate the system within minutes and it typically takes information security around 225 days to find the breach. Just recently, the US government Office of Personnel Management was hacked and more than 24 million current and Former government employees may be affected. While investigators have known about the breach since April, they are still trying to determine what was hacked and what information was leaked since it could have been up to six months since the attackers initially gained access into the system.

66% of board members are not confident of their companies' ability to defend themselves against any cyberattack.

Preparing for an Attack

This attack makes us think about the elements of an attack and where our federal government's systems may have broken down. The elements of an attack are:

- Malware, Phishing
- Command & Control
- Lateral Movement
- Access Target
- Package & Exfiltrate

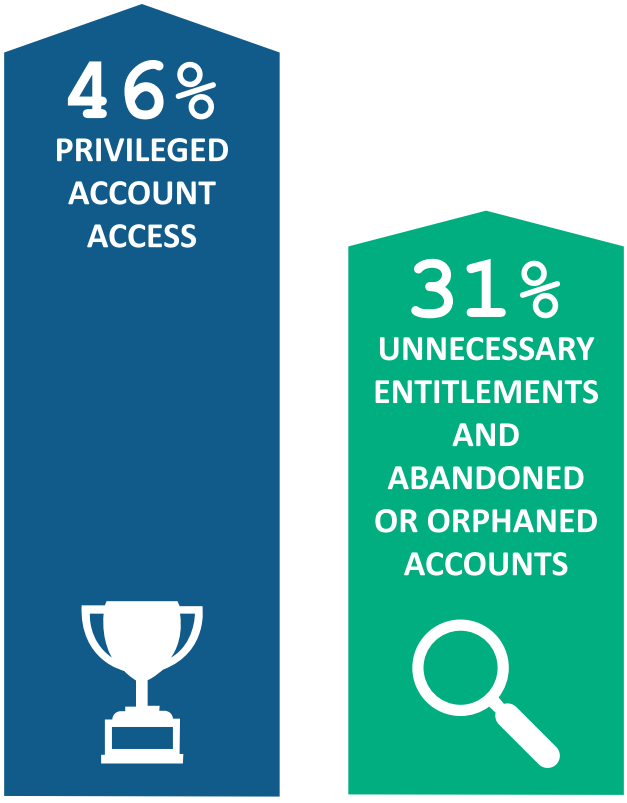
While we have anti-virus and anti-malware to fend off some of these attacks, and DLP and SIEM processes in place to fend off or detect others, we do not have the ability to fully defend against access targets and lateral movement once access is gained. What this means is that even though we are spending money, sometimes up to 85% of our budget on defending the perimeter, we have little to no security on the inside stopping hackers once they have penetrated our networks.

Typical time it takes information security to find the breach

Identity and Access Management Controls

When we look at provisioning identities or certifying access for governance, it quickly becomes a rubber-stamping process. You want to make sure the right people have the right access but what if you don't know what that person needs for his or her job? Do you reject or approve? Other than a slow down in productivity, there is no bad outcome if you don't approve access, but instead request additional sign-offs. After all, with hundreds of thousands of people and identities, access rights and roles, policies and regulations, actions, and resources, you have trillions of access relationships to manage

In a survey conducted by Core Security about the access risks that cause the most anxiety, number one on the list-at 46 percent-was privileged account access; that is, accounts such as those used by administrators that have increased levels of permission and elevated access to critical networks, systems, applications, or transactions. Other anxiety causing access issues that accounted for 31 percent were unnecessary entitlements and abandoned or orphaned accounts. What this tells us is that over half of the anxiety in your organization is based on provisioning.

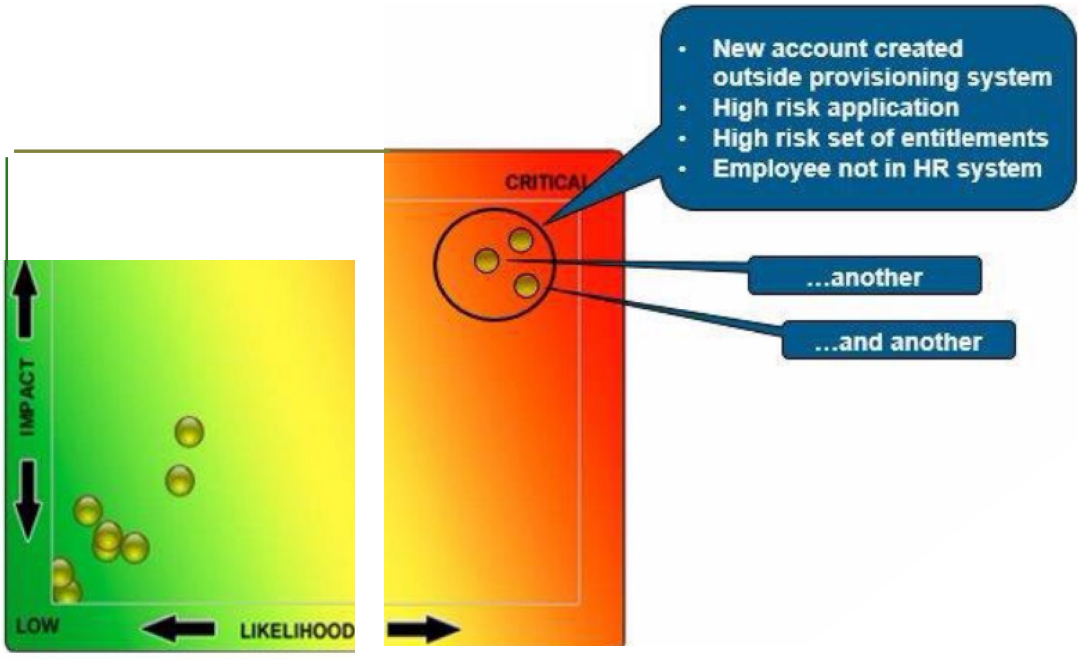


Identity and Access Management Controls

To effectively address this issue, we need to start looking at not just passing our audit at the end of the year but also at the true impact of risks created through increased or inaccurate access credentialing on an ongoing basis.

But what if with each request you received you also knew the perceived risk of approving or rejecting it? What if you could take a look at all of your credentials across your system and see who was the greatest risk? That's where an intelligent or risk-aware identity and access management tool comes in.

With risk-aware 1AM you have the ability to automate your provisioning process to keep your backlog at a minimum and still ensure that you are provisioning the correct access to your employees without just rubber-stamping an approval. With intelligence driving your provisioning and governance you can see risks long before you have an issue. Imagine if you were able to log in and see access credentials listed like this:

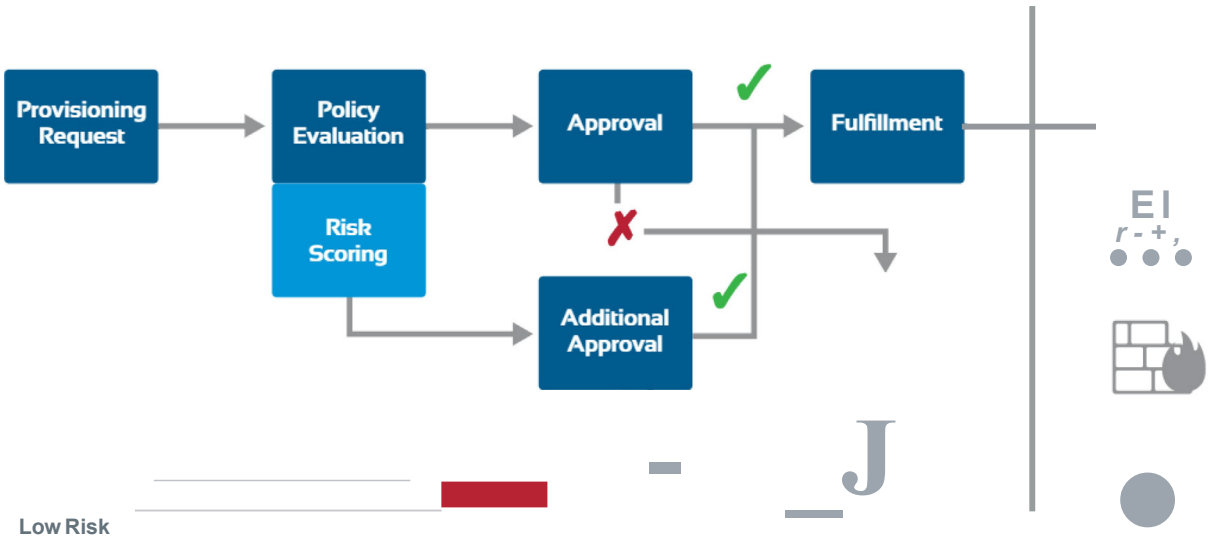


Identity and Access Management Controls

We need to understand these access risks on a scale from low risk to high. Provisioning today includes a request, a policy evaluation, and a quick approval or rejection of the request. At Core Security, we see things differently. If the request is seen as a low risk item, then it gets passed through and fulfilled in our automated system.

But for other access requests which may represent some risk, the access request will require an approval or both an approval and a micro certification.

This micro-certification , or risk-based certification review, provides holistic context around the information being examined, thus allowing an IS manager to make an informed decisions on whether a user's access is suitable or not before granting access. By performing these narrowly focused, micro-certifications, organizations can reduce access risk in a smarter more efficient way on the front end of the request to guard against over- or under-privileged accounts.



Intelligent IAM

Intelligent IAM is the next-level evolution of traditional IAM. Each process is led with intelligence with front end approvals and risk assessments that allow near real-time decisions that manage and mitigate risk to the company. According to Gartner, "By year-end 2020, identity analytics and intelligence tools will deliver direct business value in 60 percent of enterprises, up from less than 5 percent today ".

Through continuous monitoring and analytics applied to your provisioning and governance activities in real time, you are able to see the most up-to-date information thus allowing your company to truly mare data-driven decisions. With intelligence driving policy, provisioning, and access decisions, you can mitigate risk in real time and have better visibility into your organization.

Are you looking for more visibility into your company's identity and access risk? With a Quick Scan assessment of your organization's access risk we can help you take a quick look into your security measures and provide you with a plan of what you can do to mitigate those risks.