Cyolo

A GUIDE TO ACCELERATING MERGER & ACQUISITION SUCCESS WITH ZERO-TRUST ACCESS

INTRODUCTION

Mergers and acquisitions (M&As) are a massive undertaking for everyone involved, from the owners down to the business-level employees transitioning from one company's set of systems and expectations to another.

For CISOs and their security teams, M&As present a heavy workload and a host of potential risks. They must anticipate the expectations and needs of the business while also accounting for the risk of a mass onboarding of new users, whose devices and security hygiene are largely unknown and present potential vulnerabilities.

With a cybersecurity landscape that is continuously evolving, managing an M&A transition is no simple feat. Many security challenges arise during an organizational change of this magnitude, including issues related to technical debt, mass onboarding, shadow IT, unfamiliar systems, and more.

Executives overseeing M&As have seen this increased vulnerability to cybercrimes play out repeatedly. An IBM Institute for Business Value (IBV) survey found that, "More than one in three executives surveyed said they have experienced data breaches that can be attributed to M&A activity during integration. Almost one in five experienced such breaches post-integration."

Yet, one of the likeliest areas of vulnerability for an organization acquiring a new company goes beyond the technology they're using—to the users themselves.

PEOPLE ARE THE NEW SECURITY ACCESS PERIMETER

While you can and should fully assess your systems before and during an M&A (more on this below), you can't necessarily know what to expect when onboarding new employees. These users present new vulnerabilities as they transition to new systems, processes, and policies— and they may or may not be bringing bad security habits with them.

According to a recent **Deloitte study**, "During integration, unclear roles and responsibilities, disgruntled employees, modifications in the operating model, language barriers, and changes in location may prove to be a challenge." All of these factors can lead to increased cybersecurity risks.

This is not to say that a majority of acquired users are coming in with malicious intent. However, by their very nature M&As are a period of organizational chaos in which errors are bound to happen, despite everyone's best intentions. This requires security teams to consider their approach to trust and access when shoring up the cybersecurity risks users bring with them.

Integrating new users during an M&A also takes time, which means the risks are prolonged and value is lost.

On average, it takes 18 months to merge systems, apps, data, users, and other critical assets. When organizations fail to maximize the time-to-value of acquisitions and mergers, it leads to avoidable consequences and ultimately destabilizes the company.

55% of M&As don't realize their full value because of poor integration.

In today's landscape of rapid digital transformation, the disparity between new and legacy systems is growing and the risks security teams face during a merger period are higher than ever. Perimeter-focused "castle and moat" security systems aren't capable of mitigating the risks that arise before, during, and after an M&A. They simply aren't flexible or granular enough to harmonize two independently formed infrastructures.

THE SOLUTION TO M&A RISK IS ZERO TRUST ACCESS.

Zero trust is a modern security model that operates on the premise of “never trust, always verify.” It works by continuously identifying and authenticating every device, user, and identity before providing them with access to network resources. This means users are validated each and every time they want to access a network component, and would-be cybercriminals can’t exploit the company’s entire network of sensitive data through a single user’s vulnerability.

During an M&A and beyond, people should be treated as the new security access perimeter. With zero-trust access, organizations can onboard new users and systems more rapidly while drastically reducing risk.

TRUST AND ACCESS CHALLENGES

Although the company being acquired has been vetted by the CISO and security team, this doesn't mean implicit trust should be given once the formal paperwork is signed.

Managing an influx of new employees will always come with challenges and unknowns. Leveraging the acquired organization's identity source (such as Active Directory) to set user groups and necessary permissions isn't always straightforward. The challenge is to reduce risk while making the process as simple as possible. It can be a substantial task to merge directories and deconflict policies that might deny resources to someone who typically requires them, or worse – grant access to resources the user doesn't need and increase your attack surface.

There are several steps you can take to securely connect users during an M&A.

Vetting should include **examining users' existing security measures**. Check that they're in compliance with current regulations, look at their access policies, and identify all tools and technologies being used. Having both the IT and security teams perform an assessment will lead to the most thorough accounting of the situation on the ground.

By the time the M&A closes, the acquiring company should have a roadmap to integrate, migrate, or keep separate resources. A third-party consultant can help outline the risks associated with both infrastructures and propose a structured approach to risk management. At a minimum, the acquiring organization should recognize that accepting some unknown risks is itself a risk and thus plan accordingly.

The fact is that an acquired company's employees should be seen as **third-party, high-risk users** when it comes to trust, security, and access. If users refuse or struggle to adapt to new systems and procedures, they may end up taking shortcuts, which can quickly lead to risk. This is compounded by user error, which is likely to arise when learning new systems and procedures.

USER DEVICES AND SOFTWARE CHALLENGES

User devices and software present a serious challenge following an M&A, especially when new employees are not (yet) using company-owned or monitored devices. It's perfectly understandable to want acquired employees to get to work immediately, but this means they may be connecting to your internal systems on devices and tools that exist outside your security perimeter or practicing bad security habits that you cannot control or even monitor.

This can easily lead to **shadow IT**, where users leverage practices and tools that don't align with the parent company's approved systems, processes, and policies. Shadow IT increases the risk of cyberattacks because of unknown vulnerabilities and conflicting security hygiene practices that increase the attack surface for bad actors.

It may seem like the obvious solution here is to provision incoming employees with new laptops as quickly as possible. Unfortunately, this too is not without complication. Your IT team must configure these new devices and install the proper applications and agents – all while attending to the normal, day-to-day technological issues that employees face. At the end of the day, preparing devices for a large number of new employees comes at a significant cost, in terms of both money and time.

PERFORMING AN ASSESSMENT OF YOUR POST-M&A SECURITY POSTURE

A **security assessment** is an important tool that enables teams to assess their level of preparedness against potential cyberattacks. Completing a full security assessment following your M&A can help identify areas of vulnerability to be shored up and make your onboarding process run as smoothly as possible.

Here are some of the basic steps for a successful security assessment.

1. PERFORM AN ASSESSMENT OF ACCESS RIGHTS.

This assessment should include users inside and outside your organization. Use this opportunity to identify and assess who currently has privileged access rights and whether these rights are truly needed. Then, use the principle of least privilege to optimize access permissions for all user groups.

2. CHECK FOR EVIDENCE OF BREACHES AND LEAKED DATA IN THE PAST.

In all likelihood (and according to the zero-trust principle of "assume breach"), past breaches occurred and the acquired company is insecure. If security incidents did occur, examine the measures the company took to reduce exposure and improve security posture afterward. Note that as you integrate, you can use zero-trust security posturing to prevent and limit the potential damage of future incidents, breaches, or data exposures.

3. RUN A VULNERABILITY ASSESSMENT.

Use tools like vulnerability scanners to inventory software and assess patch management practices. The fact is that all companies and all software have vulnerabilities, and it's important to determine what these are for all devices and software levels. For instance, operational technologies, such as software and hardware used at off-site manufacturing facilities, may have common vulnerabilities because the manufacturer has not released a patch or it is not feasible to patch these systems. A vulnerability assessment lets you develop a plan for restricting access to these systems and mitigating the associated risks.

- Check for redundancies, workarounds, shadow IT, and systems that don't talk to each other.
- Check for modern identity infrastructure, such as multi-factor authentication (MFA), single sign-on (SSO), or password vaults.
- Block risky actions and don't allow users to make risky downloads.
- Use pinpoint access, not full network access. Network convergence is a challenge because IP address ranges may overlap. Solve this by connecting users, not networks.
- Check endpoint health before allowing a user to connect to sensitive applications.

4. EXAMINE IF THE COMPANY IS USING ANY VULNERABLE SECURITY TOOLS.

Consider the example of **LastPass**, a password management tool that has recently suffered a number of high-profile breaches. Tools should be assessed to ensure they are as effective as they need to be and don't present preventable vulnerabilities that can be costly in the long run.

Another example would be Virtual Private Networks (VPNs), which can allow attackers to take advantage of security flaws that make the network's entry points vulnerable. Additional weak security points include outdated antivirus software.

5. LOCATE ALL LEGACY APPLICATIONS TO BUILD UP A LEGACY APPLICATION PROFILE.

Be sure to extend your discovery exercise to legacy and homegrown applications. Many organizations seem willing to accept the risk these systems present because upgrading them to modern security and authentication standards feels impossible. Fortunately, there are now tools, like Cyolo's zero-trust access control platform, that can retrofit legacy applications with MFA and SSO without disrupting service or requiring **change management**. After cataloging all legacy systems in your environment, develop a plan to modernize their identity infrastructure.

6. MANAGE IDENTITY PROVIDER (IDP) SPRAWL THROUGH FEDERATION.

This exercise should also include legacy applications and is intended to ensure IdPs work together correctly and integrate with all applications. A zero-trust access platform will seamlessly authenticate users from a single interface and, at the same time, achieve a more secure access control setup.

7. USE YOUR RESULTS TO BUILD A ZERO-TRUST ACCESS IMPLEMENTATION PLAN.

Once you have completed the previous six steps of your security assessment, you can aggregate the results and build a remediation plan for the acquired company to implement. This includes mapping user access to the applications they need across both companies, deciding which applications should be eliminated, and configuring access to new applications.

Implementing ZTNA requires a high level of visibility, and performing these tasks can assemble a lot of critical data.

- Analyzing user accounts and access roles can give you a clearer picture of identity and access management.
- Vulnerability scans can give you a clearer picture of software inventory and patch management practices.
- Identifying legacy systems and their limitations informs ZTNA implementation needs.

SECURING M&A USERS WITH ZERO TRUST

As any C-level leader who's overseen an M&A will tell you, a primary goal is always to increase the time-to-value. Yet, the sheer scale and difficulty of managing security concerns across both companies' user groups and devices can make the process slow and laborious.

The answer is Zero Trust ~~Network~~ Access with Cyolo. In addition to providing secure connectivity to all approved resources for all verified users, Cyolo's trustless zero-trust access solution:

- **Enforces access controls that minimize entry points that attackers could exploit.**
- **Strengthens connectivity controls to remove the keys that enable unauthorized connections.**
- **Improves oversight controls by understanding the details needed to generate compliance reports.**

Zero trust helps organizations adhere to least-privilege access principles whether the user is an M&A employee or not, and regardless of whether they are using a managed or unmanaged device. This is because each user is verified according to their identity and only granted access to necessary applications for their role.

Zero trust enables you to connect users instantly without needing to migrate either users and networks. At the same time, zero-trust access enforces the purchasing company's security controls according to the highest security standards. By creating policies that determine which devices and users can access which systems and applications, zero trust can enable new users to connect and get to work in days instead of months.

In this way, zero trust improves your time-to-value while also letting your business-level users be more productive quickly. Using zero-trust security posturing allows newly on-boarded employees to start working immediately on the equipment they already have and continue using their regular routines.

Simply put, zero trust simplifies and streamlines the M&A integration process on every level.

While users likely will not even notice a difference in how they approach their workflows within the network, a zero-trust access solution like Cyolo helps you accelerate the adoption of new processes and pick which processes are best, thus achieving better economy of scale, accelerating growth, and more easily meeting the technical goals of an M&A.

THE CYOLO SOLUTION

Cyolo aims to improve the security practices of organizations like yours by offering a unique, fully trustless zero-trust access solution. Unlike other ZTNA providers, Cyolo does not require the implicit trust of its customers and cannot become a single point of failure.

The Cyolo platform includes valuable features like the ability to monitor, record, and audit all activity for full visibility. These capabilities not only serve as important controls but they also help to achieve and maintain compliance with industry and geographic regulations.

At Cyolo, we believe that the employee onboarding process that follows an M&A can be both painless and secure. For more information about how Cyolo can help simplify security as your business expands and evolves, wherever you are in your M&A process or zero-trust journey, **schedule a demo** or visit **our website**.

Cyolo

ABOUT CYOLO

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running.

Cyolo provides the only trustless zero-trust access solution, giving organizations visibility and access control over the users who leave them most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications.

cyolo.io