The Ultimate M&A Checklist for Retailer IT Leaders

With an accelerated consumer shift toward digital channels, retailers look to buy versus build to keep pace. But this strategy comes with risks and must be assessed carefully.

Mergers and acquisitions (M&A) in the retail industry have always been supercharged, and the last few years are no different. 60% of the aggregate transaction value of retail and consumer services dominated Australia compared to other industries in 2020. With an accelerated consumer shift toward digital channels, retailers look to buy versus build to keep pace. But this strategy comes with risks and must be assessed carefully.

The pandemic made it harder for retailers to fund their growth, transforming an urgent and strategic imperative. Retail executives highlight a more significant revenue and profit decline than the cross-industry average in 2020, with 92% of global retailers stating their company has experienced a substantial decrease in revenues vs. 87% of executives across all industries.

The Risk for Retail

Buying a company means you buy their data, endpoints and assets. With disparate security and IT operation practices between companies, there is a considerable risk when bringing them onto your network. Threats that have infiltrated their endpoints will leave you exposed to data compromise, fines and loss of trust with customers.

Acquiring companies face many risks that must be assessed and carefully accounted for during due diligence: financials, litigation, intellectual property and regulatory matters represent the potential inherited impact on a business.

Stakeholders involved in the M&A process include CEOs, CFOs, lawyers and accountants. However, they lack the expertise needed to understand the cyber risks they may potentially acquire.

They need security expertise and due diligence on user access. The stakeholders need to know how the company plans to handle software patches and understand what assets they are buying plus what is on them. Unfortunately, this is usually an afterthought.

But these challenges will be put in the shade by the reputational damage, deal value discounting, and operational disruption the company will suffer if a cyber breach is discovered during or after the acquisition.

You only have to reflect on recent prominent hacks to grasp the magnitude of the consequences of neglecting thorough IT due diligence. Verizon cut its purchase price for Yahoo by $350 million in 2017 after the web portal disclosed widespread cyberattacks under its watch.

Marriott International acquired Starwood Hotels but was subsequently fined 18.4M pounds in GDPR fines. Cyber-criminals had been in Starwood Hotel's systems for years and were effectively thrown into the merger deal without Marriott having a clue.

Many acquirers only pay lip service to protect their targets from hackers despite these risks and high-profile cases. Few conduct a thorough review of a target's security posture, and many neglect their target's risk profile altogether.

IT Operation Challenges

Not only does an IT team find that overnight they have thousands more assets to manage, but they need to work out how to save money to reduce duplicated tools and redundant processes.

Traditional tools don't provide anywhere near enough visibility and control over retailers' IT environments, so a platform that offers these capabilities is critical. GenesisCare fortuitously chose to bring on the Tanium Platform for asset management and vulnerability management just before the company acquired 21st Century Oncology in the United States. Very quickly, the company added another 400+ clinics to its organisation. It was a significant acquisition expanding GenesisCare's reach across the globe. The endpoints Mike Kleviansky, Head of IT Security and his team, had to manage jumped from 6,000 to 16,000 overnight. Thankfully, GenesisCare achieved complete visibility and control across multiple regions on a single platform.

“My initial thinking was that we needed a security tool,” Kleviansky says. "But we realised we required more than a security tool. A lot of our use cases are operational efficiency." With this guidance in mind, he sought out help, and he found Tanium.

> Once Kleviansky saw how Tanium equally supported security and IT operations, he said his “decision was a no-brainer.”

Alexandra Scott, Vice President at Tanium for Australia and New Zealand, points out that the success of M&A deals will significantly depend on how well technology is used. "To put it bluntly, IT is the engine room of any modern company, and its PCs, servers, virtual machines, containers and cloud infrastructure not only keep the lights on but drive essential growth through innovation and business agility."

Align Teams

Aligning two organisations' IT operations and security functions can be massive. But with the right tools in place to gain real-time insight into all digital assets, organisations can accelerate the whole process at speed and scale while minimising the cost of doing so.

Acquiring companies can begin to rationalise IT assets, identify critical synergies and bring exposed endpoints back into compliance—speeding up time-to-value.

Asset Visibility is Critical

Acquiring firms need a complete picture of all assets to price their target accurately and manage potential cyber risk.

Governance and oversight policies, processes and procedures, and the technology that identifies and enforces everything is a business imperative. Delivering a C-level administrative dashboard with a single unified view enables rapid understanding and visualisation of how all the systems fit together is desired. With this capability, there is complete visibility and control, and it heightens cybersecurity risk prevention and aids in discovering breaches.

> "I know from personal experience that comprehensive insight into digital assets is a pre-requisite of effective due diligence and key to the success or failure of deals."
>
> Alexandra Scott, Vice President, Tanium, Australia and New Zealand

If a target company doesn't know where its crown jewels are located, it is a disaster waiting to happen. Unfortunately for the acquirer, this problem sometimes becomes apparent only during breach investigations when the organisation cannot clarify its prized assets and where they are stored.

Before an acquiring company follows through on its purchase, it must be confident that the target has an established risk-management program and a set of cybersecurity controls and standards in place that monitor and safeguard its most precious assets.

Consider an example in which an organisation reports 500 endpoints, but in reality, it is more like 10,000. If valued at the 500-mark, this could be a good deal for the acquiring company. But these IT blind spots could also soon turn into a liability if it turns out that many of the unmanaged endpoints are riddled with unpatched vulnerabilities.

Shawn Keve, Forbes Councils Member shares that, unfortunately, "most companies lack a cohesive solution that seamlessly integrates multiple diverse tools." Source

For More Information Read: M&A success boils down to clear visibility into IT assets.

The Ultimate M&A Checklist for IT

Aligning two companies' IT operations and security functions is a massive operation, and the goals are generally universal. IT leaders must find synergies that drive cost reduction and understand and contain the acquired company's threat matrix.

The following is a checklist of the top ten priorities IT teams should immediately focus on when performing M&A due diligence:

Identify synergies

- Inventory hardware and software assets to drive machine and license consolidation strategy
- Consolidate servers and ensure full server utilisation
- Distribute new software and required applications
- Eliminate redundant point solutions at both organisations in favour of a platform that can simplify
- Streamline infrastructure

Containing threats

- Proactively identify rogue machines and malicious actors, and bring all assets under management.
- Reduce risk by scanning endpoints to ensure that vulnerabilities don't already exist on acquired endpoints and investigate and remediate exposures
- Standardise data centre management tools
- Ensure all VMs are under proper management
- Ensure vital security hygiene of the acquired company's endpoints

Additional questions to ask about the organisation being acquired during the M&A process are:

- Does it use the top cybersecurity engineering (CSE) controls?
- Does it use the NIST standard (National Institute of Science and Technology) or ACSC's Essential Eight?
- Details of the cybersecurity steering committee?
- What is the operating model for identity and access management?
- How does it mitigate identified cybersecurity risks?
- What is in place to quickly remediate those risks?
- Does it have ISO certification?

Tanium for Mergers & Aquisitions

Tanium can help accelerate the due diligence process and reduce risk by rapidly deploying 10,000 endpoints per day on average. This rapid deployment means that when the board asks you to outline your plan to quickly audit, manage and protect a substantial number of new endpoints, you can be confident you have it under control.

Customers can ask simple or complex questions about their networks' current or historical state, get fast responses from all their endpoints, and take actions to secure and manage their environment. When M&A is on the table, IT teams often have limited time to prepare and act. It is, therefore, reassuring that Tanium could be deployed in a matter of hours if critical.

After implementing Tanium primarily for security, the GoDaddy team found that Tanium was also very effective in addressing many IT operations use cases, from end-user support to IT asset management and M&A consolidation - Source.

Summary

Tanium is a game-changer during M&A for both IT operations and security teams. Customers can easily and quickly identify synergies and rationalise assets in their environment to drive substantial resource and cost savings. Organisations can eliminate redundant point solutions and streamline infrastructure.

> "Don't only look at it through security eyes," recommends Kleviensky when speaking about the Tanium Platform. "I can tell you our operational guys are probably more excited than I am, which is saying a lot." "Tanium is very smart technology."

The Tanium platform enables proactive risk assessment, remediation and quick application of policies to newly added endpoints. Ultimately retailers will benefit from unparalleled visibility and control across their new organisation whilst achieving substantial ROI. Scott said it best, “M&A can be a tough business: every day lost through costly integration is a day when the organisation is failing to maximise its market potential. With comprehensive insight into digital assets, more of these deals have a better chance of succeeding.”

Request a risk assessment →