WHITE PAPER

How to limit risk in mergers and acquisitions

LUCIDUM

NOW PART OF cyberes

Mergers and acquisitions pose unique challenges for companies.

Buyers need to know as much as possible before closing the deal, yet the company up for purchase can't provide some details that could have a significant impact on the merger process. It's possible, however, to reduce the risk for buyers with AI-driven tools designed to automate the exploration process.

Manually auditing target companies is a slow and tedious process. Identifying security threats and other vulnerabilities can come with difficulties, and audit teams often have to sift through multiple cloud and app platforms. They also must decide on the critical pieces of information, which can prove hard when they may not know how all of the data points relate to each other.

The phases in the M&A process – due diligence,sign and announce, and integration (transition to operations) – each has its own security threats. Finding and mitigating those threats plays a crucialpart in successfully navigating the process and acquiring the target company.

THE DUE DILIGENCE PHASE:

Auditing the Target Company

Once a target company has been identified for potential acquisition, the due diligence phase starts. The buying company needs as much information as possible to determine show-stopping issues and prepare as best as possible to merge the target's technology assets with their own systems.

For the acquiring company, the process is challenging because the target may not have the ability to share all of the information needed to assess vulnerabilities and other red flags before moving forward to the next phase. Should the deal fall apart, the target doesn't want its proprietary intellectual property in someone else's hands. If the acquiring company walks away from the deal, not having access to that information serves as a protection from the possibility of IP theft accusations.

> *"That process today involves a lot of bodies doing a lot of manual inventory to pull together a document that says, 'Here's what we know about what we have.' And it's going to have a lot of human errors."*
> *Jeremy Sherwood, **Chief Product Officer, Lucidum***

An audit relying solely on human research takes ample time and increases the likelihood of overlooking network, software, data, and other assets. An automated audit system using AI and Machine Learning can catalog network and data assets more efficiently and uncover potential security risks that might otherwise go unnoticed. In essence, the target requires auditing to discover security problems such as improperly secured data, misconfigured networks and servers, out-of-date software, and unmanaged network assets to address them.

Jeremy Sherwood, Lucidum's Chief Product Officer, called out the risks in human-only discovery audits, saying, "That process today involves a lot of bodies doing a lot of manual inventory to pull together a document that says, 'Here's what we know about what we have.' And it's going to have a lot of human errors."

In many cases, only about 60% of the information they report will be accurate, but that leaves a lot of room for inaccuracies. "You have about 40% of the data that's people's best guess, or it may be stale," he added. "There may be a lot of things wrong with that information."

Incorporating a system that uses AI and Machine Learning into the process gives the humans the data they need to make well-informed decisions before moving on to close the deal, cutting out as many of the unknowns as possible. It also saves a considerable number of hours, potentially cutting weeks off the discovery process.

THE SIGN AND ANNOUNCE PHASE:

Preparing for Possible Attacks

After completing the due diligence phase and announcing the deal, the race against attackers begins. The merger announcement immediately makes the target company's infrastructure a security risk because attackers see this as a window of vulnerability. If they find any weaknesses to exploit, the company's network and data are at risk.

The buying and target companies must move quickly to reduce the risk of a security or data breach. That means working with as much information as possible to secure the target company's network and assets before falling victim to overlooked vulnerabilities. With the target company's necessary need for secrecy gone, the buying company has more information with which to work. In theory, that should make it easier to lock down security threats, but it takes time for humans to analyze the data.

"Until sign and announce, the target company must keep confidential data that includes intellectual property, trade secrets, and even vulnerabilities," according to Lucidum CEO Joel Fulton. "That's a big gap in the acquiring company's visibility that isn't closed until long after sign and announce – long after it's desperately needed to protect the newly combined company."

"The moment of greatest threat from the outsiders is the moment of least visibility to the combined company."
Joel Fulton, CEO, Lucidum

Fulton also warned that the window after the announcement of the merger but before the companies have found and acted on the potential security risks makes for an especially dangerous time. "The moment of greatest threat from the outsiders is the moment of least visibility to the combined company," he said.

Relying only on people to make any necessary changes poses its own risks. First, the IT and security teams tasked with addressing the issues may not have the ability to move as quickly as attackers trying to break in. Second, they could accidentally misconfigure critical security settings or miss making essential updates.

This misconfiguration offers another place where a comprehensive automated system based on AI and Machine Learning can prove valuable. Since the system can identify addressable security weaknesses so much faster than humans, it can apply the necessary fixes – such as correcting server and network configurations or repairing outdated user permissions – quickly and without missing any necessary changes.

THE INTEGRATION / TTO PHASE:

Hardening the Defenses

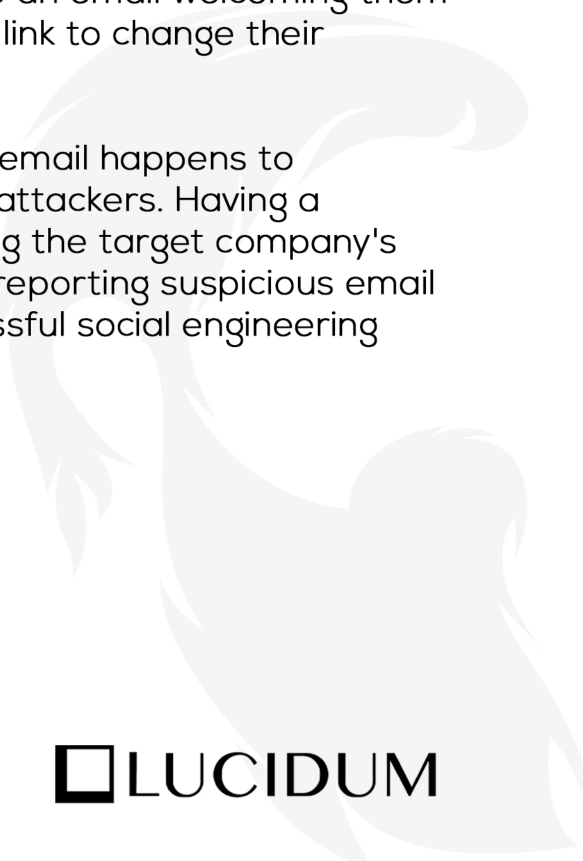
As the combined companies work to merge their resources fully, the race against attackers kicks into high gear. To successfully merge the technology and data assets, the teams from the buying and target companies must cooperate. For the highest efficacy, they need accurate information from the post-merger security audit.

Like the pre-merger audit, AI-based tools look for potential security threats, such as data encryption issues, poorly secured networks and weak security practices, much faster than their human counterparts. With those resources supplementing the human teams, it's easier to see where vulnerabilities can crop up and keep the combined company's overall security issues in mind.

"The transition part is tricky," said Brian Spanswick, CISO and Head of IT at Cohesity. "When you're going through this process, it's easy for the security teams to get a little bit confused because it's easier to be thinking about the in-state security requirements. And sometimes we forget that we have to actually securely manage the transition."

Security and IT teams also need to ready themselves for security threats targeting people instead of tech resources. "The merger provides a rich opportunity for social engineering attacks," according to Fulton. "Employees receive an email welcoming them to the company with instructions and a link to change their password, but it's a phish email."

Falling victim to a well-crafted phishing email happens to everyone, and it's a common tactic for attackers. Having a well-documented process for integrating the target company's employees, along with a procedure for reporting suspicious email messages, can help cut down on successful social engineering attempts.



MOVING FORWARD:

After the M&A is Complete

Protecting the combined company's assets doesn't end with the completion of the M&A process. Attackers always work to find new ways to break through the company's security measures, and devices the IT team doesn't know about get added to the network. Humans cannot constantly watch for suspicious activity and unauthorized devices accessing the network, at least not reliably. However, the AI platform that cataloged all the devices, network settings, permissions, and apps during the merger can do that much more effectively.

"Stuff sneaks into the environment all the time. Where Lucidum adds value is through aggregating multiple data sources and developing Machine Learning models over time for what should be there," explained Quincy Castro, CISO at Redis. "Then when someone plugs in a Windows XP vending machine on a shop floor somewhere, that pops up as something that doesn't seem like it's supposed to be here."

The AI platform then alerts the appropriate team so they can find the mystery device, determine its legitimacy, and ensure its proper configuration or remove it from the network.

Attackers have created a sort of AI arms race, too. They use AI systems to probe for vulnerabilities and launch attacks more efficiently, making the company's own AI and Machine Learning security tools a critical part of their defensive arsenal. IT and security teams can stay a step ahead of attackers by finding and fixing potential weak points before attackers exploit them much faster than they could without the help of the AI platform.

Ultimately, it all depends on preventing cybersecurity threats before exploitation, both during and after the M&A process. Fulton added, "AI does the smart things faster so you can do the important things faster and in the right order."

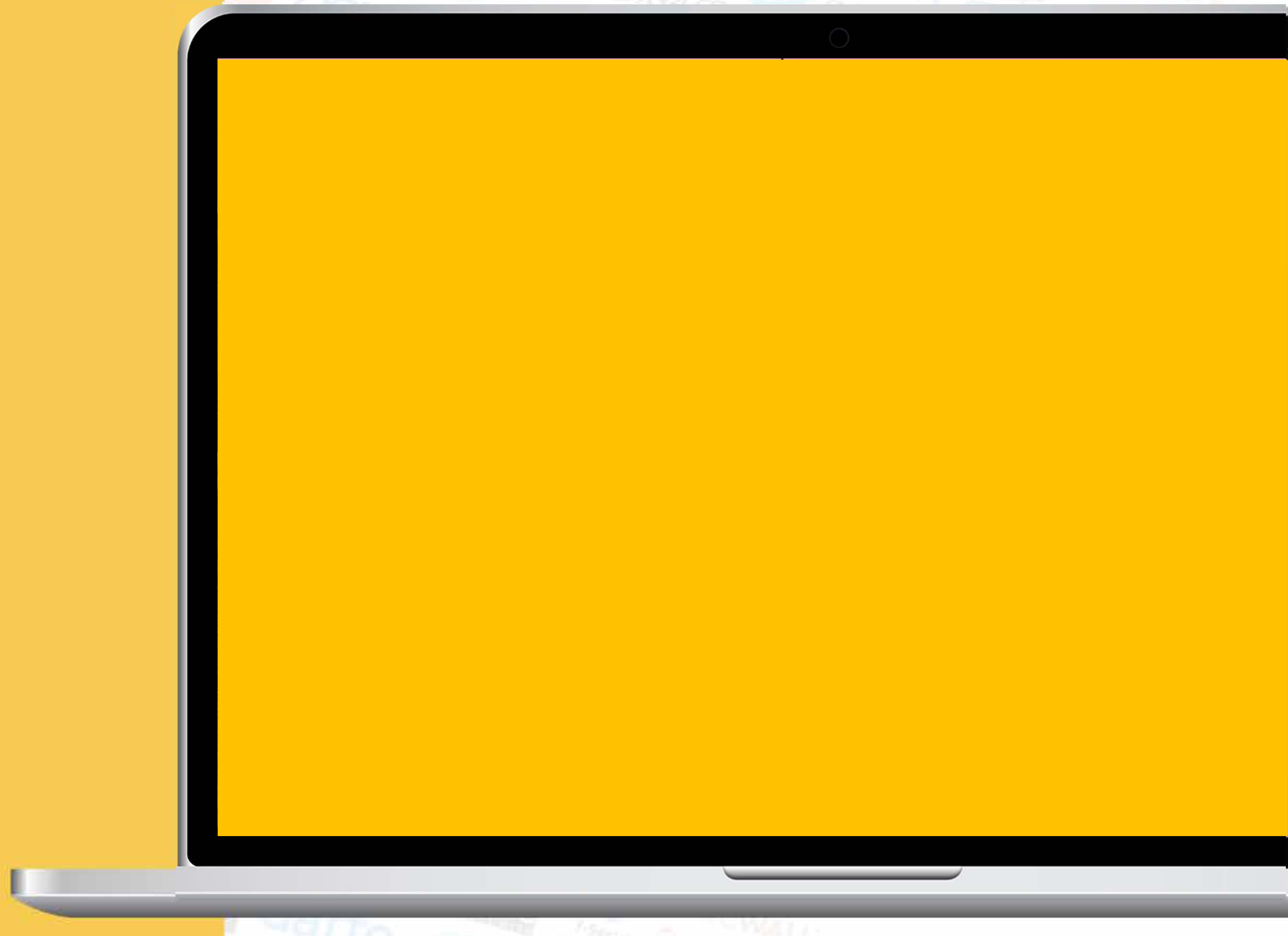
> *"Stuff sneaks into the environment all the time. Where Lucidum adds value is through aggregating multiple data sources and developing Machine Learning models over time for what should be there."*
> ***Quincy Castro, CISO, Redis***

LUCIDUM

Schedule a demo

with us to see how we can assist with your next merger or acquisition project.

Ready To Go!



LUCIDUM

studio/ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Ready To Go!

LUCIDUM