AGIO

FROM PHISHING TO FORTIFIED

AGIO INCIDENT RESPONSE RESCUES PORTCO VALUE

PICTURE THIS...

You're a private equity CTO and see some sketchy behavior on a PortCo's email server. An employee took the bait on a phishing scam, allowing bad actors to compromise their account and infiltrate the company's systems. Now, your PortCo is at risk of reputational damage, financial losses, and possibly derailing your investment strategy.

A few months ago, this incident could have been catastrophic for your PortCo—they didn't have any cybersecurity or incident response measures in place. Fortunately, you had the foresight to recommend partnering with Agio to ensure proper governance and security were squared away ahead of a planned public offering.

You've worked with Agio for almost a decade and know you can count on them to mobilize swiftly and shut down the attack.

THE CHALLENGE

While Agio already has the PortCo's governance piece in place, they're onboarding cyber ops. The PortCo has met their assigned vCISO (virtual chief information security officer), and some detection tools have been deployed but not finalized, which means the PortCo isn't in a regular monitoring and alerting stage yet.

During this phase, an employee receives an email from a known contact within the company asking them to review and sign a seemingly legitimate document. The employee takes the bait, clicks the link, and boom—malware downloads. The bad guys trick the employee into handing over their Office365 credentials, which the employee readily provides, approving the multi-factor authentication (MFA) security check. The employee has no idea what they've set in motion.

You notice the suspicious activity and contact your PortCo's CTO to offer assistance. Unfortunately, this is the first he's heard about it because the company's technical team thought they resolved the issue days ago by resetting passwords. They were wrong.

Your PortCo is in trouble, and the reputational and financial fallout could tank your exit strategy for this investment.

NOT AT MONITORING STAGE

THE EMPLOYEE TAKES THE BAIT

RESETTING PASSWORDS WASN'T ENOUGH

THE SOLUTION

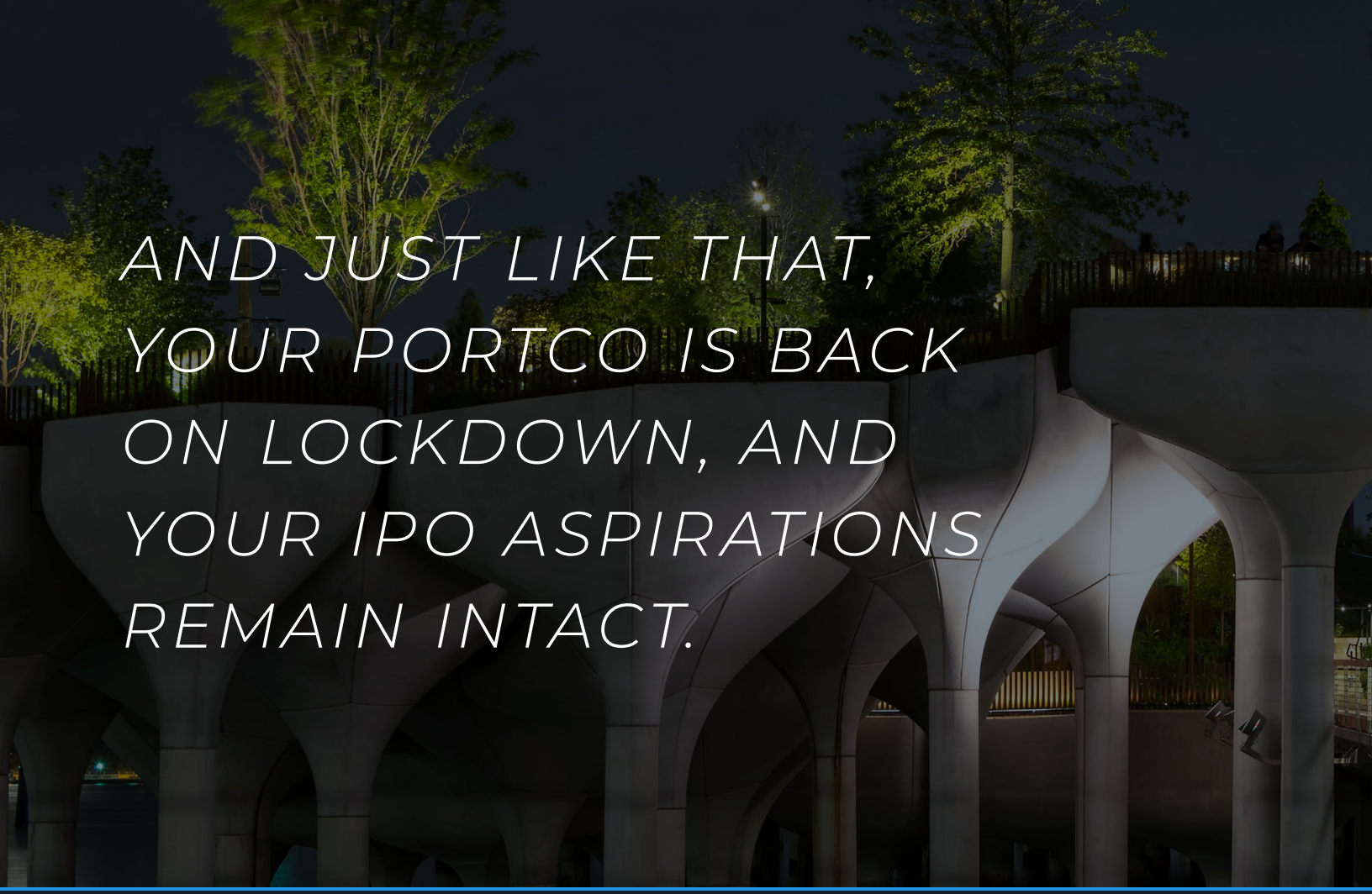
Your PortCo may not be in a regular monitoring and alerting stage yet, but the second Agio gets the call, all hands are on deck. Their security analysts immediately kick protocols into overdrive to stop the attack and get ahead of the hackers.

Within 15 minutes, you and your PortCo's CTO are on a call with the vCISO, Agio's director of cyber operations, and one of Agio's senior cybersecurity analysts, ready to kick off incident response.

Agio investigates what the PortCo's technology team has done so far while rolling out additional measures to scope the breach and lock it down. For the next few hours, Agio's cyber team works shoulder-to-shoulder with your PortCo's team to regain control of the situation.

During their deep dive, Agio discovers that two more employees were compromised when fake emails were sent from the initial victim's "trusted" address. Those staffers made the same mistake: They opened the malware, entered credentials, and approved the multi-factor authentication without realizing the criminals were the ones receiving everything.

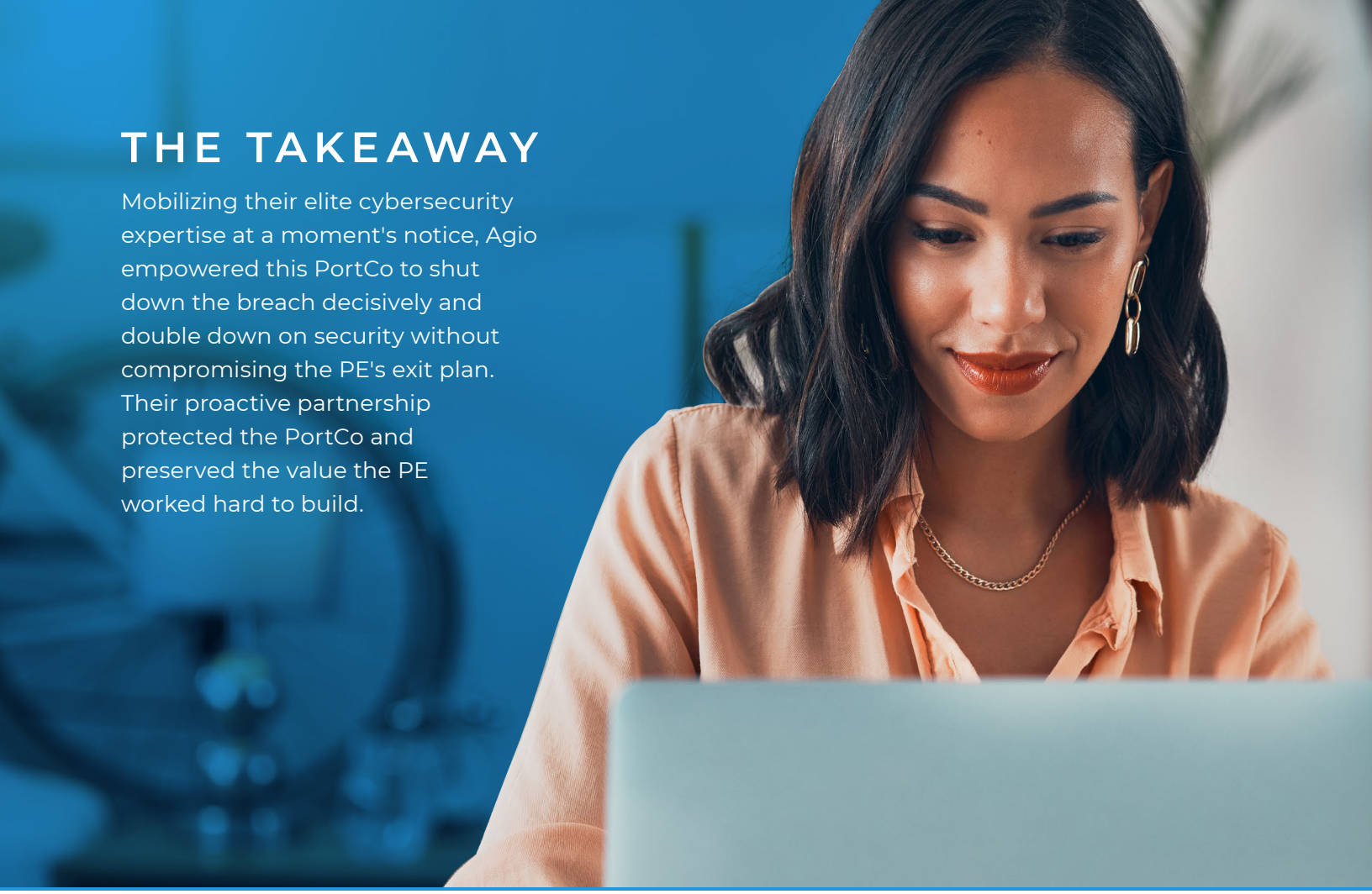
Agio’s director of cyber ops keeps your PortCo's CTO informed on important updates and next steps so he can manage the incident at the executive level and coordinate meetings with his legal and compliance teams, your team, and other stakeholders without missing a beat on the technical containment front.



THE OUTCOME

Thanks to Agio's swift, comprehensive incident response, the phishing attack is fully contained before any more damage is done. In their debrief, Agio prescribes some security improvements to prevent future incidents. With Agio's guidance, your PortCo's technical team quickly implements these updates, significantly enhancing the company's cybersecurity posture.

And just like that, your PortCo is back on lockdown, and your IPO aspirations remain intact.



THE TAKEAWAY

Mobilizing their elite cybersecurity expertise at a moment's notice, Agio empowered this PortCo to shut down the breach decisively and double down on security without compromising the PE's exit plan. Their proactive partnership protected the PortCo and preserved the value the PE worked hard to build.

THE AGIO DIFFERENCE

Agio's skilled cyber ops team, comprehensive incident response protocols, and swift action help private equity firms avert nightmare scenarios. Instead of reputational fallout and tanked financials, your PortCos and their value are safe and sound—and so is your exit strategy.

WHY AGIO?

#OneAgio

When you select Agio, you're investing in a relationship with everyone who's a part of this firm. Our teams operate in a symbiotic relationship based on deposits and withdrawals, creating a vehicle for delivering more than just service. We deliver an experience that reaffirms to our clients that we've got them covered. From clean, concise implementations to consistent support backed by automation and tools that work how they're supposed to, value-add reporting, accurate, timely invoicing, and content on the latest IT and cybersecurity trends, we bring the full breadth and depth of our talent to bear. We deliver #OneAgio.

Contact us today.