PREVIEW — SAMPLE DISCOVERY REPORT

What a Technology & Security Discovery finds

A preview of the real thing — one finding in full, and everything else it covers.

Below is a preview of a Discovery report written for a fictional 20-person professional services firm in Manhattan. The firm is invented. The findings are the ones we actually keep finding in businesses this size, written in the same format and the same plain language a real client gets.

The three things we led with

Every report opens with the small number of items that genuinely need attention first, before anything else. For this firm:

1. A 2024 email compromise was never fully closed. Two applications still hold standing permission to the company's mailboxes and files — permission a password reset does not remove.
2. Nothing stands between a stolen password and client work. The Microsoft 365 tenant has no access policies of any kind, and multi-factor authentication is optional.
3. If someone resigned tomorrow, company files would leave with them. Fourteen personal devices hold synced copies of company data, and disabling an account does not remove those copies.

The eight findings in this report

HIGH	The 2024 email compromise was never fully closed
HIGH	No access policies at all, and multi-factor authentication is optional
HIGH	Company data would leave with a departing employee
HIGH	Half the laptops are past end of life; seven run unsupported Windows
HIGH	One flat network, an unsupported firewall, and a port open to the internet
MEDIUM	No backup outside Microsoft 365
MEDIUM	No device management — no way to confirm, push, or wipe
MEDIUM	Anyone can send email that appears to come from the company

The next page shows one of them in full, exactly as a client receives it.

ONE FINDING, IN FULL

Finding 3 — Company data would leave with a departing employee

HIGH SEVERITY

What we found

This was the concern the owner raised at the outset, and the environment confirms it. SharePoint and OneDrive content synchronizes to any device someone signs into, and 14 of the devices currently holding synced copies of company files are personal machines not managed by the business. There are no controls preventing client material from being downloaded to a personal laptop, no alerting when someone downloads an unusual volume of files, and no classification distinguishing client deliverables from routine internal documents. The current offboarding process is to disable the account.

Why it matters

Disabling an account stops future access. It does nothing about the copies already sitting on someone's personal laptop, and the business has no record of what those copies contain. The period when this matters most — the weeks before someone resigns — is precisely when there is no visibility at all.

What we recommend

Restrict unmanaged devices to browser-only access with downloads blocked, enable alerting on unusual download volume, and apply data-loss prevention rules to client material. Rebuild offboarding so it includes revoking active sessions and removing company data from any device that holds it.

What's in the full report

All eight findings in this detail	Each with what we found, why it matters, and what to do
How we work during a Discovery	Read-only access to everything; nothing in your environment is changed
The remediation plan	Every item sequenced into immediate, short-term, and strategic phases
What happens next	How the findings meeting runs, and when cost enters the conversation

Read the full sample report

Six pages, free to request. It is the complete document a client receives; all eight findings, the remediation plan, and how the engagement runs.

Click here: Full Discovery Sample Report

Name, company, work email, and roughly how many people you have. That's it.

Or skip the reading. Start with a complimentary 20-minute IT Strategy Call — a conversation about how your technology is actually running, and our honest read on where your risk sits. No cost, no deck, no obligation to go further.

The company in this preview is fictional. The findings are representative of what we routinely find at professional services firms of this size.