

TECH & AI CASE STUDY - LAW FIRM - 2026

Zero-Trust Security That Protected a 4-Office Law Firm

Based on a delivery engagement with Blackwood & Reyes LLP

64 to 19

PRIVILEGED ACCOUNTS

zero

CRITICAL AUDIT FINDINGS

3 weeks to 4 days

ACCESS REVIEW CYCLE

-38%

PASSWORD-RESET TICKETS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Blackwood & Reyes LLP case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Blackwood & Reyes LLP - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Blackwood & Reyes LLP is a litigation firm of 240 attorneys operating from offices in four cities. The firm's work product is confidential by definition: case strategy documents, settlement positions, deposition materials and client communications that opposing counsel would pay a great deal to see. Its document management system is the true vault of the business, and its network connects four offices, hundreds of attorneys and staff, expert consultants, co-counsel and court reporting vendors into a single working fabric.

Law firms sell judgment and discretion, and their clients increasingly audit both. Institutional clients with their own security programs send outside-counsel security questionnaires before engagement — long forms covering identity management, encryption, network architecture and incident response — and the answers decide whether the firm can accept the work. The partnership's economics add a constraint most businesses do not have: every hour spent on security process is an hour not billed, so a program that made daily work slower would be resisted quietly and abandoned loudly. Any security model the firm adopted had to assume breach, protect privileged files, and do it all without adding friction to court deadlines and client calls.

02 Where Things Stood

The firm's technical foundation contradicted its confidentiality obligations. Office networks were flat, so a laptop compromised in one practice group could reach systems across the firm. Remote access ran on always-on VPN, which granted broad network trust to whatever device connected — including the growing population of unmanaged personal devices that remote work had multiplied. A maze of shared service accounts held the whole structure together, none of them individually owned, none of them rotated on any schedule. Auditors found departed employees whose access had never been revoked, some months after their departure, because offboarding ended at the farewell email.

Law firm operations made each of those habits harder to break than they would be elsewhere. Case teams formed and dissolved with every matter, so access grants accumulated the way teams do; co-counsel and expert consultants were granted network access by whoever sponsored them, on whatever terms the case required; and the four offices had grown their own local conventions for file shares and admin accounts over fifteen years of mostly independent administration. Nobody had ever drawn the full picture, and the firm's part-time approach to security governance had never asked for one.

The reckoning arrived through a prospective client's outside-counsel security questionnaire, which returned 41 gaps and put a \$12M annual engagement on hold until the firm could prove its controls. The managing partners did not need a security education to understand the exposure: one stolen credential could expose privileged case files, trigger malpractice claims and force breach notification to hundreds of clients. IBM Security's 2024 research puts the average US breach cost at \$9.36 million — a figure that lands hardest on data-dense professional-services firms — and the Verizon Data Breach Investigations Report finds 68% of breaches involve a non-malicious human element such as a phishing click or mishandled credential, which described the firm's shared-account and over-privileged habits precisely. The firm needed security built on the assumption of breach, and it needed the \$12M engagement back.

03 The Challenge

The challenge was architectural and cultural at once. Architecturally, the firm needed to move from implicit network trust — once you are on the VPN, you belong — to continuous, per-session verification of identity, device and privilege, which is the model NIST's zero-trust architecture standard, SP 800-207, prescribes. That transition touches every login, every file access and every remote session in a 240-user partnership, so sequencing and change management mattered as much as the controls themselves.

Culturally, the program had to earn the partnership's consent by visibly protecting billable work. Attorneys work to court deadlines from courtrooms, client offices and airports; a security rollout that interrupted trial preparation in any office would have killed the program politically. The 41 questionnaire gaps also carried a clock: the prospective client wanted evidence within two quarters, which meant the controls that answered the questionnaire had to land first, and the deeper architecture had to follow without renegotiating attention. The firm's size was actually an advantage — small enough to move in quarterly waves, large enough to need real engineering — but only if every wave left daily work measurably easier, not harder.

04 Discovery and Diagnosis

Emerson Technology began with a five-week discovery across all four offices, combining network mapping, an identity census and workflow interviews with partners, associates and the support staff who keep litigation operations running. The identity census was the foundational exercise: employees, contractors, vendors and service accounts across all systems, each catalogued with its owner, its privilege level and its last use. It confirmed the auditors' findings about departed employees and produced the number that anchored the program's goal — 64 privileged accounts, most of them blanket admin rights accumulated over years, none of them justified by a current business need.

Network mapping showed the flat office topology and traced exactly which systems an attacker could reach from a single compromised laptop, a blast-radius analysis partners found more persuasive than any abstract risk score. Workflow interviews mapped how attorneys actually access case files — from the document management system, on managed desktops in offices and unmanaged laptops at home, sometimes through co-counsel sharing arrangements negotiated case by case. The diagnosis organized the findings into a NIST SP 800-207-aligned target state with a quarterly wave plan: identity first, segmentation and privilege second, monitoring and recertification third, with the outside-counsel questionnaire's 41 gaps mapped onto the earliest waves so the \$12M engagement's evidence requirements were met on schedule.

05 The Solution

The program followed the NIST SP 800-207 zero-trust model, delivered in quarterly waves so that no office lost a billable day.

Identity as the perimeter

Identity became the firm's perimeter. A centralized single sign-on platform federated every application the firm operates, with enforced authentication policies, so each application moved inside the monitored boundary instead of carrying its own local password — every app left outside the identity provider is an unmonitored side door attackers probe first. Phishing-resistant MFA rolled out to all 240 users, beginning with administrators and finance staff, because this single control defeats most credential-stuffing and phishing attempts at minimal cost.

Device-health checks now gate access to the document management system: unmanaged personal laptops can still reach email, while the vault of case files stays protected from unknown endpoints. Password-reset tickets fell 38% as single sign-on spread, which turned the security change into a daily convenience attorneys noticed positively.

Segmentation and the least-privilege reset

Micro-segmentation split each office network into practice-group zones with explicit firewall rules, restricting east-west traffic so one compromised laptop could no longer reach everything — segmentation designed around data sensitivity rather than office floor plans. Every shared service account was vaulted, rotated automatically and tied to a named owner, ending the anonymous credentials that make lateral movement easy. Least-privilege role reviews replaced blanket admin rights across the firm, cutting privileged accounts from 64 to 19, each of the remaining accounts justified, scoped and monitored. The privilege reduction was performed with department by department review rather than fiat, so no attorney lost access they could demonstrate needing.

Watching sessions, recertifying access

A managed SIEM with identity-threat detection watches every session for impossible-travel and privilege-escalation patterns, converting the firm's sign-in activity from an unaudited stream into an analyzed one. Quarterly access recertification now runs through automated workflow approvals instead of email chains — managers approve or revoke each entitlement on a schedule, and the cycle that once consumed three weeks of chasing closes in four days. Vendors and co-counsel enter through brokered, time-boxed remote sessions recorded end to end, so external collaborators keep their access while the firm gains an audit trail and instant revocation for every engagement that ends.

06 The First 90 Days

The first quarter executed the identity wave end to end. Weeks one through four completed the identity census and deployed single sign-on in audit mode, federating the first tranche of applications. Weeks five through eight rolled phishing-resistant MFA across all 240 users — administrators and finance first, then attorneys by office — with enrollment sessions timed to avoid trial calendars and a support channel staffed through each wave. The device-health gate went live for the document management system in the same window, with a pre-enrolled managed device fleet so no attorney lost file access on rollout day.

Weeks nine through twelve delivered the first segmentation wave in one office as a template, the vaulting and automatic rotation of the shared service accounts, and the launch of the SIEM's identity-threat detection with a two-week tuning period. The first quarterly access recertification cycle ran on the new workflow tooling and closed in four days instead of the historical three weeks, giving the firm its first reproducible evidence artifact. By day 90, departed-employee access was revoked same-day by construction, the second office's segmentation wave was scheduled, and the outside-counsel questionnaire's identity-related gaps had been answered with system-generated evidence rather than assertions — the difference between a claim and a proof.

07 The Results

Privileged accounts fell from 64 to 19, and the outside-counsel questionnaire now returns zero critical findings — the \$12M engagement was signed in the first quarter after rollout. Quarterly access reviews that once took three weeks close in four days, and password-reset tickets dropped 38% as single sign-on spread. The firm renewed cyber-insurance coverage at a lower premium after its first clean control audit, and partners report no measurable friction in daily court or client work.

METRIC	BEFORE	AFTER
Privileged accounts	64	19
Critical audit findings	-	zero
Access review cycle	3 weeks	4 days

METRIC	BEFORE	AFTER
Password-reset tickets	-	-38%

The zero-trust posture changed the firm's risk arithmetic in ways the metrics only sketch. A compromised laptop now yields an attacker one session to one zone instead of a network; a departed employee's credentials die the day the departure is recorded; and every co-counsel session produces a recording that would settle any later dispute about what was accessed and when. Institutional clients noticed — the firm's security answers went from a liability in vendor reviews to a credential that shortens them. The clean control audit also did something quietly important inside the partnership: it demonstrated that rigorous security and a billable practice are compatible, which makes the next wave of controls a routine decision instead of a negotiation.

08

What Your Business Should Do

The Blackwood & Reyes sequence works for any professional organization with confidential data and limited security staff. Inventory every identity before buying anything — list employees, contractors, vendors and service accounts across all systems, and name an owner for each, because zero-trust programs stall on unknown service accounts, not on tool selection. Make phishing-resistant MFA your first move, rolling hardware keys or platform authenticators to administrators and finance staff first and everyone else next; this single control defeats most credential-stuffing and phishing attempts at minimal cost. Federate applications behind one identity provider with enforced authentication policies, since every app left outside it is an unmonitored side door attackers probe first. Segment by data sensitivity rather than office floor — split the network into zones around systems like document management and finance, with explicit rules restricting east-west traffic so one compromised laptop cannot reach everything.

Vault and rotate all service accounts, moving credentials into a secrets vault with automatic rotation and named ownership to remove the shared-password habits that make lateral movement easy. Gate your most sensitive applications on device health, requiring managed, patched devices for core data while unmanaged personal laptops still reach email — a compromise that protects the vault without surveilling everyone's personal machine. Automate quarterly access recertification with workflow tooling that prompts managers to approve or revoke each entitlement on a schedule, catching orphaned accounts that manual reviews miss. Finally, broker and record vendor remote access through a jump host with time-boxed credentials and full session recording, so third parties keep their access while you gain an audit trail and instant revocation. Carry these eight steps through your own rollout with the action checklist in this practice book, and let the reflection questions frame each quarterly partner review: if a partner's laptop were compromised tomorrow, how many other systems could an attacker reach from it, when did you last verify that every departed employee lost access the same day, and how long would it take your team to detect privilege escalation on an admin account — hours, days, or never?

REAL-WORLD PROOF & BENCHMARKS

IBM's 2024 Cost of a Data Breach report finds the average US breach now costs a reported \$9.36 million — a figure that lands hardest on data-dense professional-services firms. - IBM Security, 2024

The Verizon Data Breach Investigations Report finds 68% of breaches involve a non-malicious human element such as a phishing click or mishandled credential. - Verizon DBIR, 2024

NIST's zero-trust architecture standard, SP 800-207, advises organizations to grant access per session with continuous verification rather than trusting any single network perimeter. - NIST SP 800-207

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐

1. Inventory every identity before buying anything

List employees, contractors, vendors and service accounts across all systems. Zero-trust programs stall on unknown service accounts, so name an owner for each before any tooling purchase.

OWNER

TARGET DATE

STATUS

--	--	--

☐

2. Make phishing-resistant MFA your first move

Roll out hardware keys or platform authenticators to administrators and finance staff first, then everyone else. This single control defeats most credential-stuffing and phishing attempts at minimal cost.

OWNER

TARGET DATE

STATUS

--	--	--

☐

3. Federate applications behind one identity provider

Move every application you can onto single sign-on with enforced authentication policies. Every app left outside the IdP is an unmonitored side door attackers probe first.

OWNER

TARGET DATE

STATUS

--	--	--

☐

4. Segment by data sensitivity, not office floor

Split the network into zones around sensitive systems such as document management and finance. Restrict east-west traffic with explicit rules so one compromised laptop cannot reach everything.

OWNER

TARGET DATE

STATUS

--	--	--

☐

5. Vault and rotate all service accounts

Move service credentials into a secrets vault with automatic rotation and named ownership. Rotated, owned accounts remove the shared-password habits that make lateral movement easy.

OWNER

TARGET DATE

STATUS

--	--	--

☐

6. Gate sensitive apps on device health

Require managed, patched devices for access to your most sensitive systems. Unmanaged personal laptops can still reach email while core data stays protected from unknown endpoints.

OWNER

TARGET DATE

STATUS

--	--	--

☐

7. Automate quarterly access recertification

Replace email-based access reviews with workflow tooling that prompts managers to approve or revoke each entitlement on a schedule. Automated reviews catch orphaned accounts that manual processes miss.

OWNER

TARGET DATE

STATUS

--	--	--

☐

8. Broker and record vendor remote access

Route third-party sessions through a jump host with time-boxed credentials and full session recording. Vendors keep their access; you gain an audit trail and instant revocation.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. If a partner's laptop was compromised tomorrow, how many other systems could an attacker reach from it?

Q2. How many shared service accounts exist in your environment, and can you name the owner of each one?

Q3. When did you last verify that every departed employee and ended contractor lost access the same day?

Q4. Would your largest client's security questionnaire return critical findings today — and would you know before they send it?

Q5. Which applications sit outside your single sign-on platform today, and who still logs into them with local passwords?

Q6. How long would it take your team to detect privilege escalation on an admin account — hours, days, or never?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Blackwood & Reyes LLP's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact