Real-World Security Breaches:

How They Happen and How to Stop Them

A Joint Planit & NRI Webinar I Tuesday 24 February 2026

Welcome & Introduction

Today we bring together two perspectives on real-world security incidents - offensive and defensive - to give you practical lessons you can apply immediately.

Your Hosts:

Ferd Hagethorn

Planit / Practice Director – Security Services

David Hawks

NRI / Head of Cyber

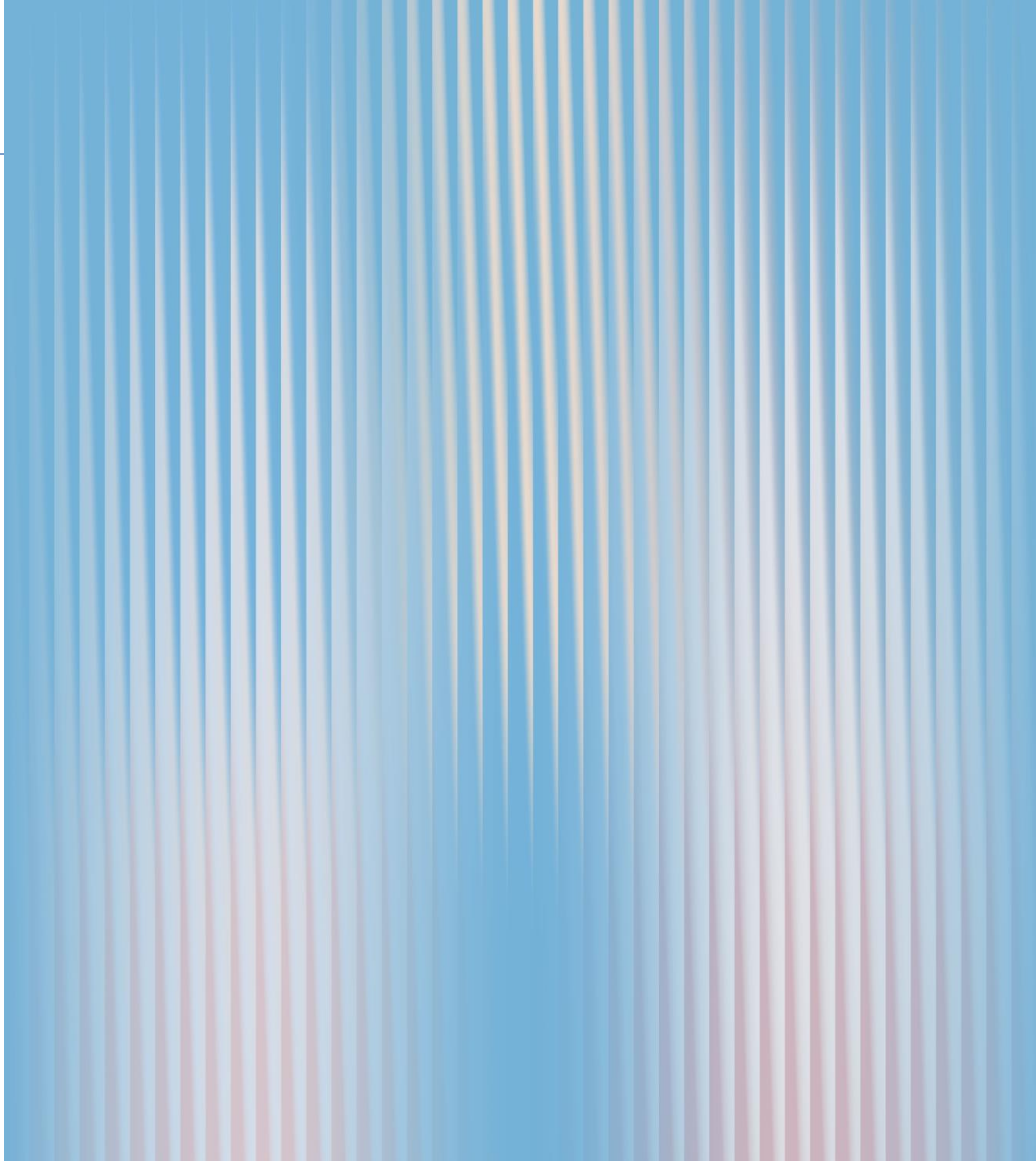
Today’s Agenda

Welcome & Introduction

Real-World Breach Analysis – Red Team Perspective

Defensive Design & Assurance – Blue Team Perspective

Q&A



About Planit & NRI

Planit

Australia and New Zealand's leading quality engineering and testing company. Decades of experience across QA, security testing, test automation and accessibility.

NRI

A global consulting and technology firm. NRI's Digital Trust practice helps organisations build, demonstrate, and sustain trust across cybersecurity, AI, data, and digital operations.

Together

Combining Planit's offensive security testing expertise with NRI's Digital Trust consulting and blue team assurance to deliver end-to-end security outcomes.

Why This Matters Now

Recent high-impact breaches across Australia and New Zealand have shown how quickly quality gaps and security blind spots escalate into serious, high-profile incidents.

Sectors affected in the last 18 months:

- Healthcare
- Aviation
- Higher Education
- Critical Infrastructure

Behind every breach is a chain of failures that could have been prevented

Ferd Hagethorn

Red Team Perspective – How Breaches Happen

What We'll Uncover

Four case-studies of publicly known incidents
'Post-mortems' to learn from

What went wrong

The impact

The prevention & Risks insights

Incident 1: University of Sydney (AU)

What Happened

Late 2023-2024: Attackers targeted students and staff using sophisticated **Adversary-in-the-Middle (AiTM)** phishing kits to bypass Multi-Factor Authentication (MFA).

What went wrong

The reliance on **"Legacy" MFA** (TOTP or Push notifications) which can be intercepted or "fatigued." Attackers sat between the user and the real login page, capturing the session token in real-time.

How to prevent

- **Phishing-Resistant MFA**: Implementing FIDO2/WebAuthn (YubiKeys or Passkeys).
- **Conditional Access**: Geofencing logins or flagging "impossible travel" logins at the identity provider level.

The Impact

Unauthorized access to internal research data and personal records; demonstrated that standard MFA (SMS/Push) is no longer a "hard" defence.

This highlights Intellectual Property (IP) and Continuity risks.

IP Theft: Universities are hubs for sensitive research and commercial partnerships. An MFA bypass isn't just about student emails; it's about losing millions in R&D value or proprietary data to state actors or competitors.

Cyber Insurance Eligibility: Insurers are increasingly denying coverage or hiking premiums for institutions that can't prove "effective" MFA. A "set and forget" approach could literally make the university uninsurable.

Operational Downtime: Account takeovers require massive IT labour hours to reset and audit, pulling staff away from maintenance tasks or other projects.

Incident 2: Qantas (AU)

What Happened

May 2024-2025: A "micro-outage" or system update caused the Qantas app to start serving incorrect session data. Users logging in were seeing other passengers' names, flight details, and boarding passes.

What went wrong

Likely a **server-side caching misconfiguration** (like a CDN or Load Balancer error) or a session-swapping bug (IDOR/Logic flaw) where user identifiers were incorrectly mapped during a high-traffic or recovery state.

How to prevent

- **Robust UAT/Staging**: Testing session persistence under "failure state" simulations.
- **Cache Invalidation Protocols:** Strict rules ensuring that PII is never cached at the edge or that session tokens are cryptographically bound to the hardware/IP.

The Impact

Massive PR embarrassment; immediate privacy breach for thousands of travellers; forced logouts for all app users.

Customer Experience and Brand Equity failure.

Brand Devaluation: Qantas is a premium brand. Seeing someone else's boarding pass on your app shatters the "premium/safe" feeling.

Operational Risk: The "fallout" into 2025 suggests that the underlying architecture is fragile. For a business, this often means long-term higher insurance premiums and lower investor confidence in their digital transformation roadmap.

Legal & Regulatory: Triggering the Australian Privacy Act (and potentially GDPR for international travellers) leads to massive legal fees and potential class-action lawsuits.

Incident 3: Manage My Health (NZ)

What Happened

Dec 2025-now: The ‘**Kazu**’ Hackers reportedly gained access through a **valid user account**, likely obtained via credential stuffing or automated login attempts.

Module-Specific Breach: The compromise was isolated to the "**My Health Documents**" module. The core GP clinical systems and live medical records remained secure, but this secondary module acted as a "soft door."

The Impact

108GB of data was stolen, consisting of approximately **428,337 files**. This included user-uploaded reports, hospital discharge summaries, and referral letters.
In total **125,000 affected users** (roughly 7% of their 1.8M user base) of which ~80,000 in Northland we caught in this breach. Secondary impact: identity theft.

Ransom: The group demanded **US$60,000** (approx. NZ$104,000). MMH followed police advice and did not pay .

What Went Wrong

June 2025 Warning: MMH has mentioned that the Office of the Privacy Commissioner (OPC) received an anonymous tip in **June 2025** about credential exposure on the platform. MMH investigated at the time but found "no breach," though they forced password resets as a precaution.

Authentication Weakness: The breach highlighted a lack of **phishing-resistant MFA**. While 2FA was available, it wasn't mandatory for the affected module at the time of the breach.

Incident 3: Manage My Health (NZ)

How to Prevent

- **Zero Trust for Legacy Modules:** Isolate older "bolt-on" components (like document storage) from the core network to prevent lateral movement.
- **BOLA Protection:** Implement strict Object Level Authorization checks to ensure a user can only access their specific ID, even if they guess a document URL
- **Anti-Scraping Controls:** Use rate-limiting and behaviour-based blocking to detect and stop automated data harvesting

Current Status

The Inquiry: The Privacy Commissioner’s inquiry is in "Phase One," investigating whether MMH took "reasonable steps" to protect the data.
Remediation: The "Health Documents" module was temporarily disabled and has since been re-secured with independent VAPT (Vulnerability Assessment and Penetration Testing) verification.

This is a **Trust and Compliance** loss.
Privacy Act 2020 Implications: In New Zealand, a breach of this scale triggers mandatory reporting and potential fines, but more importantly, it invites intense scrutiny from the Privacy Commissioner.
Reputational Churn: For a health platform, "trust" is the only product. If users (and the GP clinics that facilitate them) lose confidence, the platform risks a mass exodus to competitors.
Remediation Costs: Fixing legacy modules under the pressure of a live breach is exponentially more expensive than scheduled maintenance.

Incident 4: MediSecure (AU)

What Happened

2024-2025: A massive **ransomware** attack **exfiltrated 6.5TB** of data from a server environment. As a key link in the **national e-prescription chain**, the breach was catastrophic

What went wrong

A **supply chain failure** where a third-party server environment (likely a legacy data store) was compromised, giving attackers a "flat" path to a massive amount of PII and PHI.

How to prevent

- **Zero Trust Architecture**: Assuming the network is already breached and requiring verification for every movement.
- **Data Minimization:** If the data isn't needed for active operations, it should be archived offline or deleted, rather than sitting in a "live" environment.

Impact

Insolvency. The company could not cover the costs of the incident response and **entered voluntary administration** in mid-2025.

Customer Experience and Brand Equity failure.

Business Insolvency: This is the most potent warning for management. It demonstrates that a security failure isn't just a "cost centre" issue; it can be a "company-ending" event.

Supply Chain Contagion: You are only as secure as your weakest third-party vendor. For management, this means the business impact extends to legal liability for failing to conduct proper due diligence on partners.

Market Share Loss: When a company stops operating, competitors immediately absorb that market share, making recovery impossible even if the technical issues are eventually fixed.

Common Patterns & Themes

The Technical Trigger	*Leading to*	*The Business Impact*
Identity & MFA bypass	→	IP Theft & Insurance Uninsurability
Broken session management	→	Brand Devaluation & Operational Fragility
Legacy modules & technical debt	→	Privacy Compliance & Trust Erosion
Supply chain vulnerability	→	Business Insolvency & Existential Risk

NRI | planit
an NRI company

Defending Your Business

Core Principles

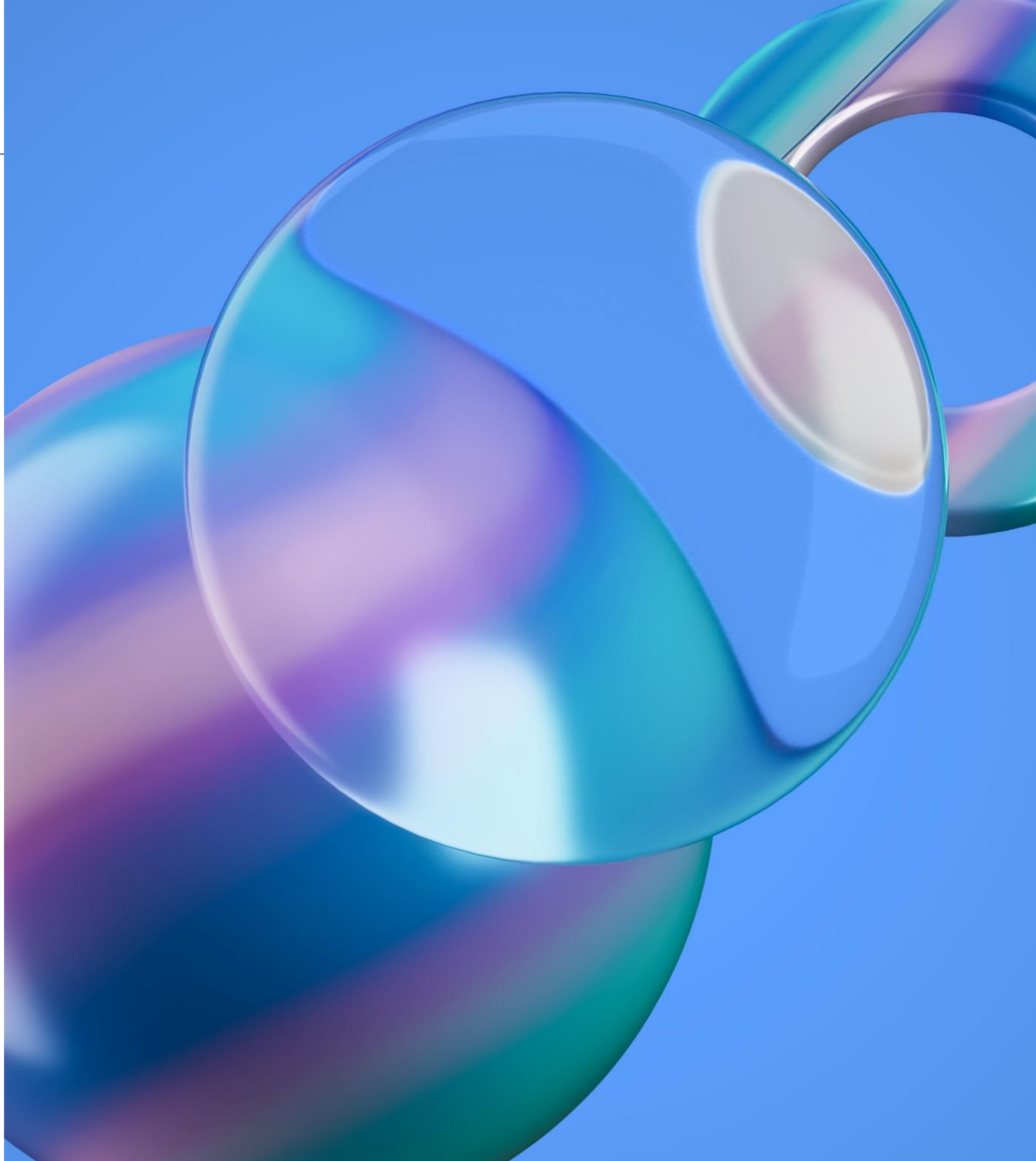
- Limit blast radius: Only hold what you need.
- Conduct Periodic Reviews: Include third parties in your assessments

Foundational Controls

- Phishing-proof MFA
- Monitoring, logging & alerting
- Vulnerability Management & patching

Security Mindset

- Security is a process, not a bolt-on
- Security is a strategic business pillar in 2026



Q & A

NRI | planit
an NRI company

Thank you!

WWW.NRI-ANZ.COM