Kavya Ganesan

NITRAM

SECURITY BUSINESS PROPOSAL

Prof Timothy “The GOAT” Suh

BOTTOM LINE UP FRONT

Nitram's overall risk is **High** due to high-value financial data, reliance on cloud platforms, and increasing phishing attempts.

Payment Fraud (Integrity): **High** risk, potential $4M+ in fraud and customer loss.

Cloud Breach (Confidentiality): Very **high** risk, up to $6M in fines, lawsuits, and brand damage.

Ransomware (Availability): **Moderate** risk, but downtime could cost $500K–$1M daily.

COMPANY OVERVIEW

Name: Nitram

Industry : Fintech (Personal Finance Management)

Revenue : $75M annually

Unique Cyber Qualities :

- Heavy use of third-party APIs for transaction aggregation
- All customer data stored in the cloud (AWS)
- Uses ML models for personalized insights

QUALITATIVE RISK ANALYSIS

CLOUD BREACH RISK

- Third-party dependencies and API exposure
- Attackers targeting weak links in partner integrations or exploiting API misconfigurations could gain access to sensitive financial data.
- Estimated breach cost: $6M+ including legal, regulatory, and forensic expenses

PHISHING AND CREDENTIAL STUFFING

- Caused by frequent user logins
- Users often reuse passwords across services, making credential reuse attacks highly effective
- Average phishing fraud loss per incident: $350K; up to $2M with regulatory penalties

DATA BREACH

- Handling sensitive financial and behavioral data that users expect to remain private and secure
- Can cause reputational harm that surpasses even the direct financial losses
- Resulting the loss of customer trust, regulatory scrutiny, and market confidence
- Projected cost after breach: estimated $1.5M–$3M drop in recurring revenue.

FAIR RISK ANALYSIS

The **most compelling scenario** is a **cloud breach impacting confidentiality** , with projected losses exceeding **$6M due to regulatory fines, legal action, and customer data breach.**

The **LEC curve** indicates both **high frequency and loss** of events from API(Application Programming Interfaces) or vendor-related vulnerabilities.

FAIR analysis reveals **Confidentiality** risks dominate, caused by data sensitivity and third-party exposure, followed by **Integrity** risks (payment fraud), and lastly **Availability** (security system downtime).

These findings support **urgent investment** in API security, vendor risk management, and cloud segmentation

NITRAM FINANCE

RECOMMENDATIONS

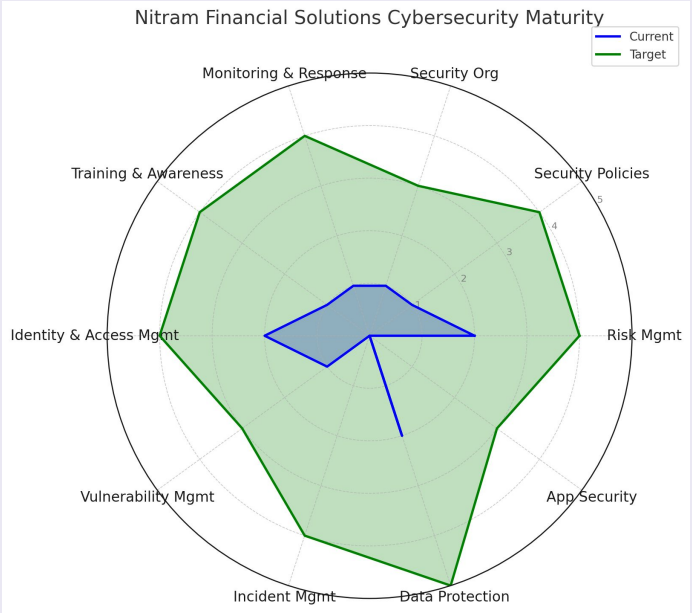
Avoidance:

- Stop using outdated, insecure web applications that aren't business critical
- Change to platforms with built-in security controls.

Mitigation:

- Create a formal incident response (IR) plan with defined roles, playbooks, and simulations. This will reduce downtime during a breach.
- Do regular code scans and basic input validation.
- Makes sure everyone follows the baseline and security policies
- Enable logging and monitoring tools for early detection of incidents. These are low-cost but high-benefit, especially with small IT teams.

RADAR CHART



RECOMMENDATIONS

Transfer :

- Purchase cyber liability insurance to reduce potential data breach. Budget around $2K–$5K/year for coverage
- Look into a managed detection and response (MDR) service (~$2.5K/month) for 24/7 monitoring and response

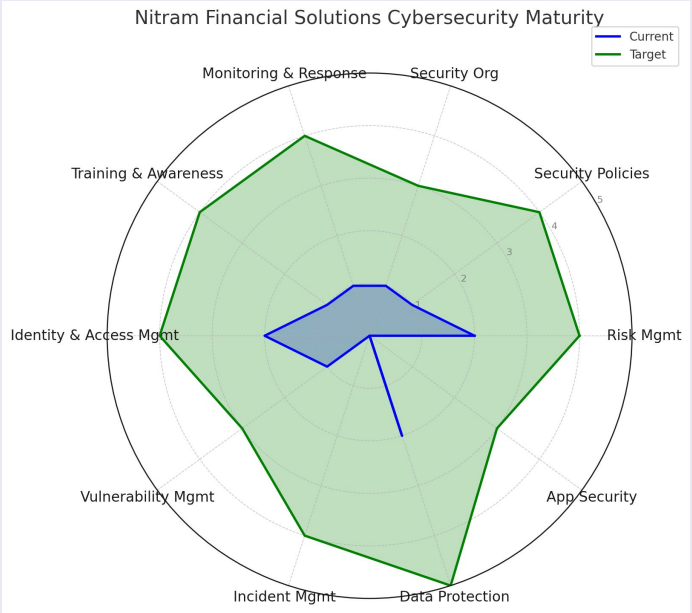
Accept:

- **Minor** risks like occasional phishing incidents without data loss
- Trying to eliminate all risk is unrealistic so focus budget where it matters most.

Cost vs Benefit:

- The cost of building an IR plan and basic app hardening is **low** compared to potential losses of $1M+ from a breach
- follow industry norms and bring Nitram closer to compliance and maturity standards without breaking your budget

RADAR CHART



THANK YOU

THANK YOU FOR YOUR ATTENTION AND PARTICIPATION. WE HOPE YOU FOUND THE PRESENTATION INSIGHTFUL AND LOOK FORWARD TO YOUR CONTINUED ENGAGEMENT.