IMPROVEMENT _ PLAN

Table of Contents

1.Immediate Actions (0–30 DAYS)

Action	Description & Justification	Responsible Party	Resources / Budget	Success Metric	Verification method
Emergency Credential Reset	Force password reset for all domain and privileged accounts to remove residual attacker access and prevent immediate re-entry.	IT Security Manager	Internal staff time.	100 % privileged accounts reset within 24 hours.	Reset confirmation validated through Active Directory audit logs and automated privilege account scan report.
Deploy Temporary MFA for Admin Accounts	Immediate Multi-Factor Authentication (MFA) deployment for all remote and privileged users to prevent reuse of stolen credentials.	CISO & IT Operations	$8K for MFA licenses	MFA enforced on all admin accounts.	IAM console report confirming MFA status across all admin accounts.
Network Segmentation Quick Fix	Create VLAN isolation between production, backup, and management networks to immediately inhibit lateral movement.	Network Engineer	$5K equipment	Segmented zones verified via scan.	Automatic network segmentation scan producing a baseline report confirming enforcement of new boundaries.

Air-Gap Backup Creation	Establish immutable/offline backups using external media until a permanent solution is implemented.	Backup Administrator	$12K hardware	Daily immutable copy successfully validated.	Automated backup integrity check confirming successful snapshot creation. Checksum validation ensuring no corruption.
IR Plan Hot Review	Conduct rapid tabletop review of existing Incident Response (IR) plan to correct role clarity gaps and decision-making bottlenecks noted during the event.	IR Manager & General Counsel	Internal workshop	Updated IR Plan v2.0 issued and approved.	Update IR plan version number and change log entry showing the applied correction. Attendance log confirming stakeholder participation.

2. Short - Term Actions (1–6 MONTHS)

Action	Description & Justification	Responsible Party	Resources / Budget	Milestones
Comprehensive security awareness program.	Redesign phishing-resistance training with simulated campaigns and quarterly testing.	HR & CISO	$4k content redesign and update $5k phishing simulation platform $3k training delivery $2k quality testing and evaluation $1k contingency Total :$15k	90 % of staff pass simulated phishing tests.
Privileged Access Management (PAM)	Implement PAM solution to control, rotate, and monitor administrator credentials, reducing the attack surface from internal threats.	IT Security Team	$30K software licenses $12k consulting & system integration $6k implementation &configuration $2k training for administrators &security team Total :$50k	PAM in production by Month 4.
Enhanced Monitoring & SIEM Tuning	Introduce advanced analytics for PowerShell command logging and lateral-movement	SOC Lead	$18K for SIEM software upgrade $5k log ingestion &storage expansion $5k implementation & tuning	New, validated alerts in pilot and full deployment.

	detection within SIEM platform.		$2k staff training on new SIEM features Total :$30k$18K for SIEM software upgrade $5k log ingestion &storage expansion $5k implementation & tuning $2k staff training on new SIEM features Total :$30k	
Incident Response Training & Exercises	Conduct semi-annual functional exercises and annual full-scale simulation to improve team cohesion and procedural adherence.	IR Manager	$3k tabletop and simulation planning $4k external facilitator $2k training materials & evaluation reports $1k team logistics Total:$10k	Two drills completed with post-exercise reports.
Legal & Regulatory Workflow Automation.	Integrate breach-notification templates and statutory timelines into GRC platform.	Compliance Officer	$4k automation tool licenses $2k configuration & workflow setup $1k compliance officer training Total:$7k	Automated reminders and reporting tested and functional.

3.Long - Term Actions (6–12 Months)

Action	Description/ Justification	Responsible Party	Estimated Budget	Key Metric	Quartely Checkpoints
Zero-Trust Architecture Adoption	Transition to identity-centric, least-privilege model across hybrid environment to minimize blast radius.	CISO & CTO	$120K	All critical applications placed behind Zero Trust (ZT) controls	Month 6: Identity centric access defined for 50% of high value applications. Month 9: 50% of systems migrated to Zero Trust controls. Month 12: Full Zero Trust policy enforcement across applications.
Immutable Cloud Backup Platform	Migrate to cloud-based, versioned, ransomware-resistant backup system with geo-redundancy.	IT Operations	$80K	Successful full quarterly restores tests achieved	Month 6: Immutable cloud storage platform deployed, and first successful versioned backup completed. Month 9: Geo redundancy configured and tested. Month 12: First full quarterly restore test completed.
Business Continuity and Disaster Recovery Enhancement	Establish alternate data center / cloud failover capability; update Business	COO & BC Manager	$60K	Recovery Time Objective (RTO) ≤ 4 hours for core systems.	Month 6: Failover capability and initial BCP Draft

	Continuity Plan (BCP) scenarios to include major cyber events.				Month 9: Full BCP Finalized and initial Testing Month 12:Final validation and RTO Achievement
Security Maturity Roadmap (ISO 27035 Alignment)	Advance Incident Response (IR) maturity from the “Developing” level to “Managed.” As per industry framework.	GRC Office	$25K consulting	Maturity level verified by external audit.	Month 6: Process development and Tooling. Month 9: Training, Procedure testing and optimization. Month 12: External Audit Readiness.

4.Root Cause Analysis

Primary Question: *Why did the ransomware attack succeed?*

Why #	Question	Answer
1	Why did the ransomware attack succeed?	Because a phishing email executed malicious code and no effective filter blocked it.
2	Why was the malicious email not blocked?	Email security controls were outdated and lacked essential features such as macro and sandboxing capabilities.
3	Why were controls outdated?	Patching and signature updates were not managed under formal change control.
4	Why was change control weak?	There were no dedicated Configuration Management Policy specifically governing security tools.
5	Why was policy missing?	Governance focus was compliance-driven (checking boxes) rather than risk-driven (managing threats) and budget was allocated only to easily auditable areas.

Effect: High security risk due to outdated controls and user susceptibility

Root Causes:

Governance: Lack of risk driven policies, no continuous security maturity

Process: Outdated technical controls

People: Users compensate for weak controls, increasing susceptibility

Process: Absence of periodic security reviews and risk assessments

Corrective Action: Adopt risk-based cybersecurity program aligned with NIST CSF and ISO 27035.

5. Improvement Recommendations

5.1 People (Training and Awareness)

- Launch **role-based security training** (IT admins, executives, customer-facing staff) tailored to specific risk profiles.
- Introduce **quarterly adaptive phishing simulations** that increase in difficulty based on user performance.
- Provide **executive crisis-communication workshops** for C-suite alignment during incident response.
- Establish an **annual incident response certification** requirement for CSIRT members.

5.2 Process (Policies and Procedures)

- **Update IR Plan** to include clear decision-authority matrix and mandatory legal review checkpoints.
- **Add a Comprehensive Breach Notification Runbook** defining state and federal (e.g. GLBA) timelines and templates.
- **Formalize a Change Management Policy** specifically for security tools configurations and architecture.
- Integrate a mandatory **post-incident review** to be completed within 15 days after any major incident.

5.3 Technology (Security Controls)

- Deploy **Next-Generation Email Gateway** with advance sandboxing and macro filtering capabilities.
- Implement **Network Segmentation** and internal firewall policy enforcement to restrict east-west traffic.
- Introduce an **EDR/XDR solution** for endpoint visibility, threat hunting and automated response.
- Establish an **immutable backup architecture** with secure offsite replication and mandatory monthly restore testing.
- Implement **centralized log management and SIEM correlation** for real-time alerting and proactive threat identification.

6. METRICS AND MEASUREMENT FRAMEWORK

KPI	DEFINITION	TARGET 2025
Mean Time to Detect (MTTD)	Average time from initial compromise to confirmed detection	≤ 4 hours
Mean Time to Respond (MTTR)	Average time from detection to containment	≤ 8 hours
Mean Time to Contain (MTTC)	Time required to isolate affected systems	≤ 2 hours
Mean Time to Recover (MTTR2)	Time required to restore critical operations post-containment	≤ 48 hours
IR Plan Testing Frequency	Tabletop / Full Simulation Rate	2 per year
Security Awareness Effectiveness	Percentage of employees passing stimulated phishing tests	≥ 90 %
Backup Validation Rate	Percentage of successful restore tests per quarter	100 %
Role based training Adoption Rate	Percentage of targeted personnel completing required role based training modules	100% of targeted roles(eg IT, Admins, Executives quarterly)
Security Awareness improvement score	Aggregate score combining stimulated phishing click Rate reduction and post Training knowledge/confidence surveys	20% improved in phishing click rate reduction and average score >=4/5 on surveys

IR Exercise decision clarity score	Average score from observers/evaluators regarding the speed and accuracy of critical decisions made during the exercise	Average score >= 4.5/5 for C-suite crisis communication and CSIRT incident handling decisions

7. IMPLEMENTATION OVERSIGHT

- **Governance:** Led by the CISO through the Cybersecurity Steering Committee.
- **Reporting:** Quarterly progress report will be submitted to the Board Risk Committee.
- **Budget Summary:** An estimated total of $400k will be allocated over the next 12 months (covering capital and operational expenditures).
- **Risk Integration:** project status updates, including residual risk levels and control effectiveness, will be formally logged as updates to the Enterprise Risk Register and aligned with the corporate Enterprise Risk Management(ERM) program
- **Review Cycle:** Formal Progress audit scheduled at Month 6 and final effectiveness assessment at Month 12.

8. CONCLUSION

The recent ransomware incident revealed systemic weaknesses in governance, controls and preparedness but also demonstrated FinanceFirst's capacity for rapid containment and executive coordination. By diligently executing this improvement plan. Focused strategically on People, Process and Technology. The Organization will progress from a developing to a managed incident response maturity, significantly reduce risk exposure and strengthen resilience against future cyber threats.