



HITACHI

LATAM Partner Summit FY26

Built to Grow. Powered by Data.

HITACHI

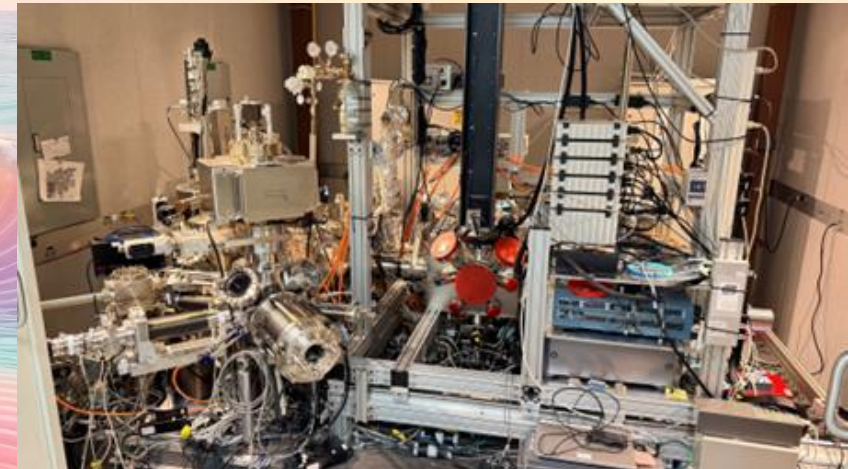
Achieving Operational Resiliency Mitigating the Risk

A Three-Lane Framework for Business Continuity and Rapid Recovery



- BJ Deonarain
- Global Quantum and Classic Cyber Security
- Cyber Security and Resiliency

Quantum (S) is the smallest possible piece of something, further describes as a single, indivisible particle or the smallest possible unit of something – 2 or More = Quanta



History

Hitachi is 116 Years old – 1910-Present

- 1910 the company was Founded in Ibaraki Prefecture, Japan, by electrical engineer Namihei Odaira
- 1911: Officially became an independent business entity focused on electrical machinery and name HTACHI
- 1920: The company-built Japan's first 4-kilowatt electric induction motor
- 1924: Produced Japan's first mainline electric locomotive.

Top 10 Threat Actors - 2026

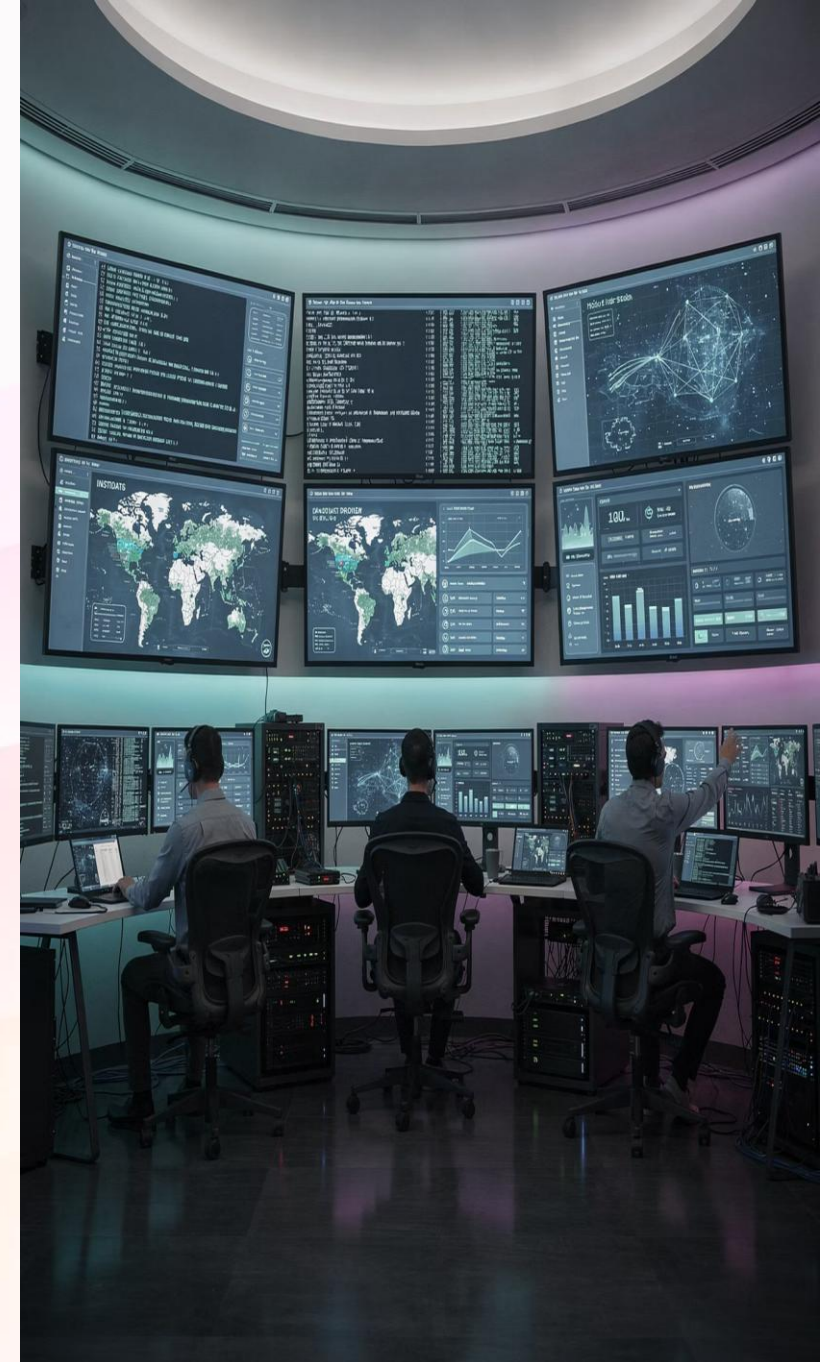
Rank	Masked Actors 2026	Rank	Ransomware Q1-Q2 2026
1	Scattered Spider - A decentralized group known for masterful social engineering and massive supply chain attacks.	1	Qilin - The most active ransomware group for 12 consecutive months, posting hundreds of victims.
2	Lazarus - A highly sophisticated, state-linked group responsible for over \$6.5 billion in cryptocurrency theft.	2	The Gentlemen - A rapidly rising RaaS group, often ranking #2 or #3 in Q1-Q2 2026.
3	MuddyWater - A state-aligned espionage group with a massive geographic reach (113 countries) and rapid malware development.	3	Akira - A consistent top-tier RaaS group that often ranks #2 or #3 in Q1 2026.
4	Tycoon 2FA - Dominates the Phishing-as-a-Service (PhaaS) market with an 89% market share.	4	LockBit - Made a major comeback with the launch of LockBit 5.0, re-emerging as a top-tier threat.
5	GoldFactory - A technically advanced group known for stealing biometric data to bypass mobile banking authentication.	5	DragonForce - A prominent RaaS group employing a "cartel" model and consistently ranking in the top five.
6	TX-NFC - Commercializes contactless payment fraud, offering its services via subscription models.	6	Siber - A new, rapidly growing group that reached #2 in May 2026 with 99 incidents.
7	Shadow Silk - A financially motivated group known for its ability to operate undetected inside critical infrastructure for over a year.	7	Chaos - A consistently active ransomware group, ranking in the top 10 in May 2026.
8	Bloody Wolf - A persistent group focused on long-term surveillance and intelligence gathering against government targets.	8	SafePay - A centralized, non-RaaS operation that has seen fluctuating activity but remains a significant threat.
9	Teste PHP - A fast-growing financial crime operation that uses malicious browser extensions to harvest credentials.	9	Inc_Ransom - An established RaaS group that has consistently been active throughout 2026.
10	DarkBlinders - An emerging, operationally agile group targeting aviation and telecom sectors in the Middle East.	10	Kairos / Nova / NightSpire - A group of other prominent ransomware operators that frequently appear in top-10 lists.

Masked Actor vs Ransomware:

The fundamental difference is that a **threat actor** is the **attacker** (the cybercriminal or group), while **ransomware** is the **tool** (the malicious software). Threat actors use ransomware to lock and encrypt data in order to extort a financial payment.

Navigating the Post-Quantum Future: A Overview of NIST 2.0

Understanding the Four Selected Algorithms and Architectural Implications

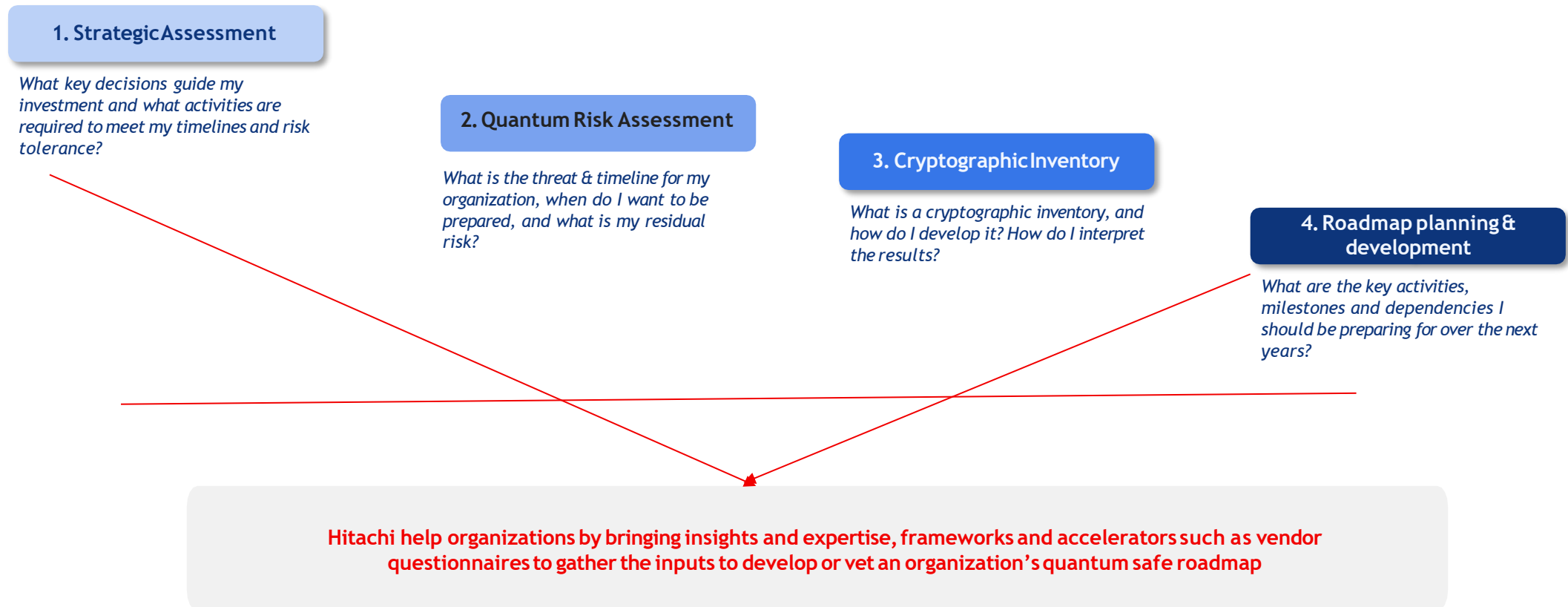


The NIST 2.0 Core: Two Signature Schemes, Two KEMs

Algorithm	Type	Mathematical Foundation	Key/Ciphertext Size	Primary Use-Case
CRYSTALS-Kyber	KEM (Key Encapsulation)	Module Learning with Errors (MLWE)	~1-2 KB	General-purpose key establishment (TLS, VPNs). The recommended default.
CRYSTALS-Dilithium	Digital Signature	Module Lattice-Based (MLWE + MSIS)	~2-4 KB	Primary digital signatures. Fast verification, suitable for most applications.
Falcon	Digital Signature	NTRU Lattices (Short Integer Solution)	~1-1.5 KB	Signatures where very small size is critical (e.g., code signing, blockchain).
SPHINCS+	Digital Signature	Hash-Based (Stateless)	~8-50 KB	Long-term backup / "paranoid" option. No hardness assumptions beyond hash function security.

- **The Big Trade-off:** Lattice-based (CRYSTALS, Falcon) offer performance & size efficiency but rely on newer mathematical assumptions. Hash-based (SPHINCS+) is bulky and slower but is a conservative, well-understood safety net.
- **Architectural Insight:** Kyber and Dilithium are designed to work well together, offering a cohesive suite for most systems.

Crafting a Quantum Safe Roadmap



From Theory to Implementation: Critical Considerations

Key Challenges:

1

Performance & Size Overheads

Expect 2-5x larger keys/signatures and higher computational cost than ECC/RSA. **This impacts TLS handshake latency, bandwidth, and storage.**

2

Hybrid Deployment is Mandatory (for now)

The interim strategy is **Hybrid Mode** – running new PQ algorithms *alongside* classical ones (e.g., ECDHE + Kyber). This maintains crypto-agility and security during the transition but doubles complexity.

3

Hardware & Ecosystem Readiness

Is your HSM ready? Do your provisioning and key management systems support larger key blobs? Library integration (OpenSSL, BoringSSL) is progressing but requires validation.

The Approach: Simplifying the Transition

- **Crypto-Agile Foundation:** Our solutions are built with algorithm abstraction, allowing you to plug in Kyber today and adapt tomorrow.
- **Hybrid Handshake Orchestration:** We manage the complexity of dual-algorithm negotiation and execution seamlessly within our stack.
- **Performance-Optimized Libraries:** We provide rigorously tested, hardware-accelerated implementations to mitigate performance impacts.
- **Lifecycle Management Tools:** For inventory, risk assessment, and phased migration planning of your cryptographic assets.

What customers and prospects are asking for

Demand

Boards and Regulators are Demanding



Tested & Predictable

Tested, proven, and predictable cyber recovery.



Catastrophic Scenarios

Under catastrophic scenarios (control plane loss).



Enterprise Scale

At enterprise scale for functional business services (MVCs).



End-to-End Workflow

For all steps of the cyber recovery workflow.

BUSINESS GOALS

- Lower RPOs
- Lower RTOs
- Evidence of recoverability
- Lower Cost
- Automation
- True Isolation
- Leverage Existing Investments

Cyber Recovery Workflow

Isolate



Rebuild



Recover



Eradicate

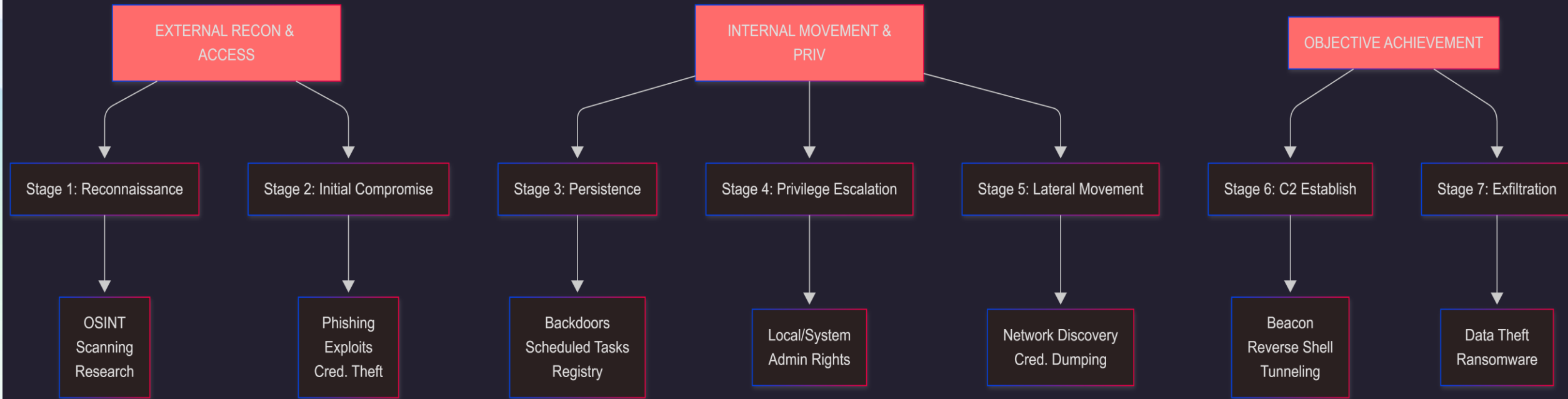
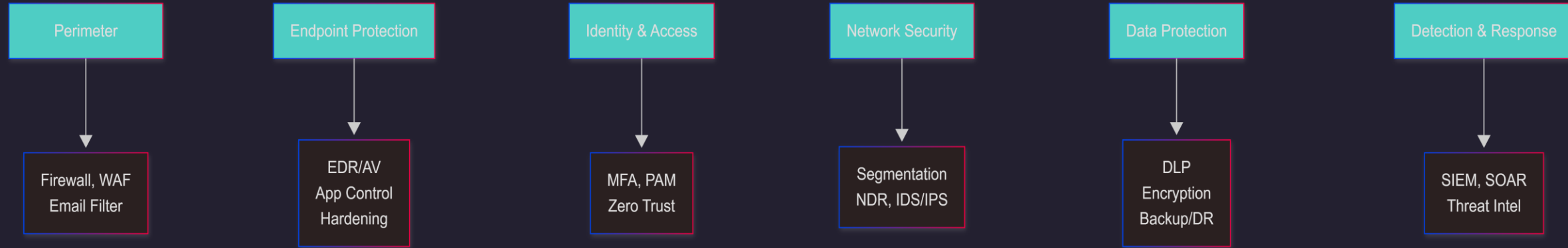


Harden



Reconnect

The Cyber Defense Sequence: Cyber Tools





The Three-Lane Response Framework

The Parallel Paths to Resilience: Our Three-Lane Framework

Lane 1: Operational Resiliency

Focus: Mission-critical systems & data.

Goal: Restore core operations in hours.

Lane 2: Cyber Security Response

Focus: Incident Response (IR), forensics, process.

Goal: Contain threat, investigate, meet audit reqs.

Lane 3: Cyber Recovery

Focus: Non-critical data & full restoration.

Goal: Complete recovery of all data/assets.

Monitoring, Planned Testing Frequency, and Governance Occurs Before an incident occurs.

Deep Dive: Lane 1 – Operational Resiliency

Lane 1: Operational Resiliency – The "Keep the Lights On" Lane

Key Objectives:

- **Primary Goal:** Restore mission-critical business functions within a short, defined period (e.g., 4-6 hours).
- **Mindset:** "Assess impact against our defined priorities." Prioritize service continuity over perfect security restoration.

Critical Actions:

- Activate failover systems and redundant infrastructure.
- Restore critical data from isolated, clean backups or last-known-good states.
- Focus on systems essential for revenue, customer service, and safety.

Outcome

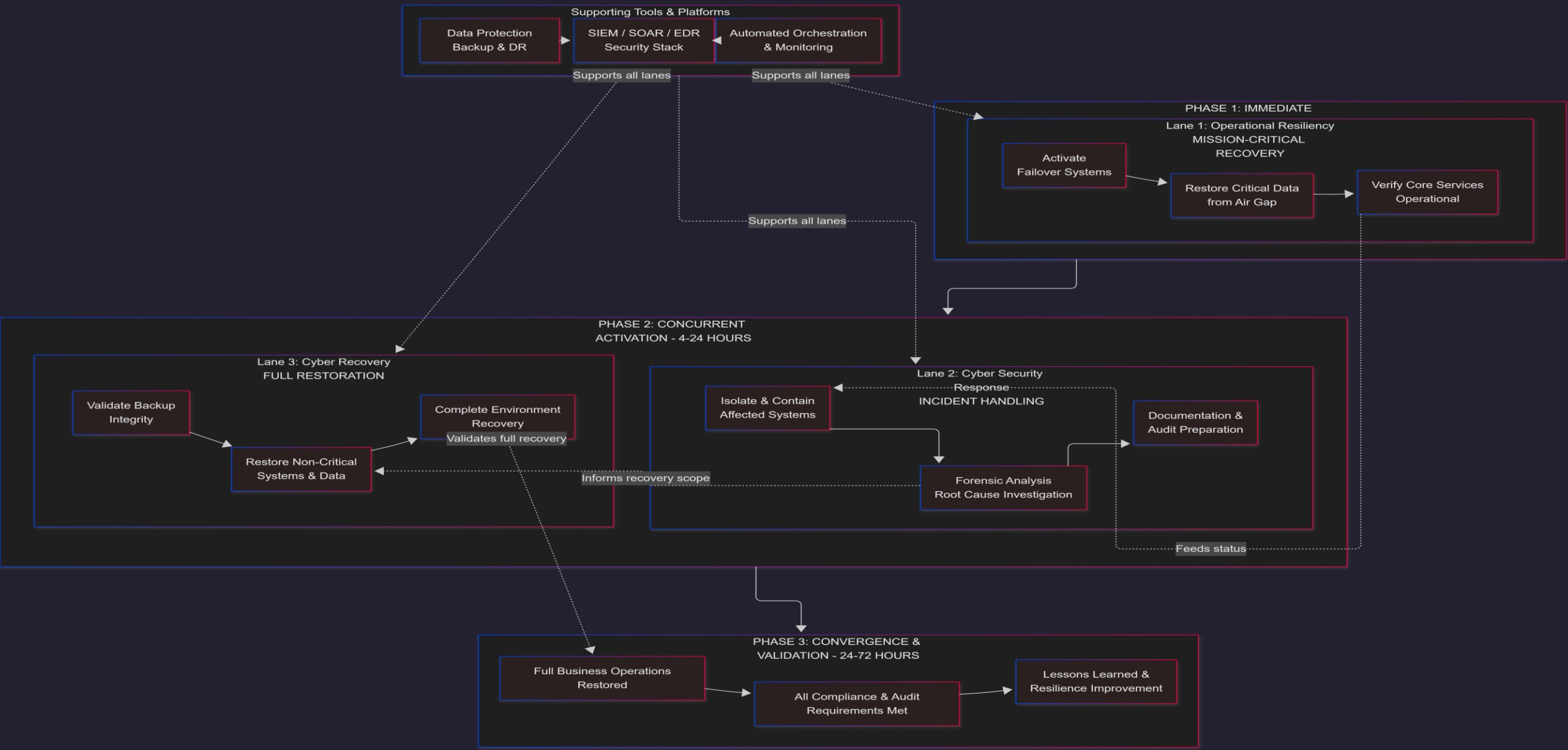
Core business operations resume with minimal customer impact.

Deep Dive: Lane 1 – Operational Resiliency Profile

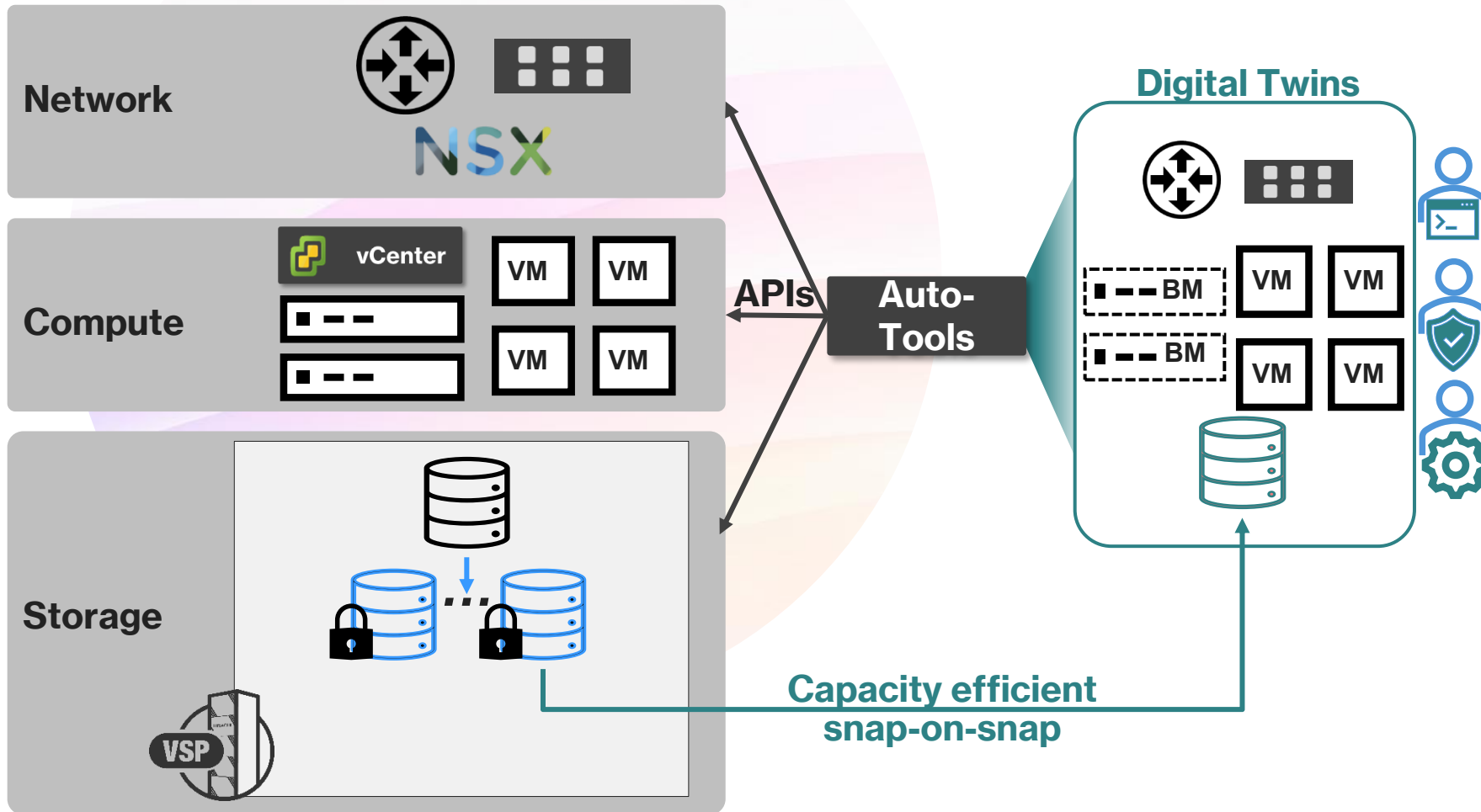
Solution Focus:

- Hitachi Vantara VSP 360 for Cyber Recovery – Provides isolated, immutable, and logically air-gapped recovery environments for mission-critical systems.
- Enables rapid restoration of core operations within defined RTOs (e.g., <1–6 hours) through secure, clean Continuous points.
- Supports failover to resilient infrastructure, ensuring business continuity even during active attacks.

Recovery Sequence – The anatomy of Operational Resiliency



Automated Recovery



Software solution with native API integrations

Single click automation

Virtual-Air-Gap isolation

Snap-on-snap recovery

VMware and BM recovery

Built-in RBAC and end-user access

Test upgrades, enable DevSecOps, and validate recovery at scale

Deep Dive: Lane 2 – Cyber Security Response

Lane 2: Cyber Security Response – The "Investigate & Fortify" Lane

Key Objectives:

- **Primary Goal:** Contain the threat, determine root cause, and strengthen defenses.
- **Mindset:** "Forensic & Procedural." Follow the IR playbook meticulously.

Critical Actions:

- Isolate affected systems to prevent spread.
- Conduct forensic analysis using EDR, SIEM, and threat intelligence (TIP).
- Document everything for audit, legal, and regulatory requirements.
- Execute incident response process: identification, containment, eradication, recovery.

Tools in Focus: EDR, SIEM, SOAR, TIP, UEBA/XDR.

Outcome: Threat neutralized, lessons learned, and audit trails validated.

Deep Dive: Lane 2 – Cyber Security Response profile

Solution Focus:

Hitachi Cyber Incident Response Services – Delivers end-to-end incident response, from containment to forensic investigation.

Hitachi Cyber Security Services – Includes 24/7 monitoring, threat intelligence, and managed detection and response (MDR) for IT/OT environments.

Provides documented IR playbooks, audit trails, and regulatory compliance support.

Integrated Operational Resilience Architecture

A Full-Spectrum Portfolio to Secure and Support Your Organization

Virtual CISO & Advisory Services

- Virtual CISO, Architect and/or Security Team
- Strategic Planning
- Risk Management
- Policy Development
- Compliance Assurance
- Vendor Management

Cyber Threat Intelligence

- External Attack Management
- Digital Risk Protection Services
- Brand Exposure Protection
- Data Leaks Identification
- Dark Web Monitoring

Penetration Testing

- Infrastructure Penetration Testing
- Application Penetration Testing
- Mobile Web Application Testing
- Wireless (WiFi) Penetration Testing
- Hardware Testing
- Static Code Analysis
- Code Review
- Objective-Based Testing
- Attack Surface Hunting

Architecture Security

- Network Architecture & Configuration Assessment & Design Support
- Cloud Migration - Security Architecture Design Support
- M365 Security Configuration Assessment + Deployment Support
- Azure Security Configuration + Virtual Architecture Assessment & Deployment Support
- Application Security Architecture & Risk Assessment
- OT Network Security Assessment - ISA/IEC 62443 Guidelines
- Identity Access Management Assessment
- Network Infrastructure Security
- Cloud Computing Considerations
- Application Security
- Endpoint Device Protection
- Data Security Measures
- User Authentication and Access Controls
- Addressing Security Challenges Across Domains
- Malware Resiliency Assessment

Governance, Risk & Compliance (GRC)

- Enterprise Security Program Development
- IT/OT Risk Management
- Security Controls Gap Assessment (ISO, NIST, COBIT, SANS)
- Compliance Assessments (HIPAA, SOC 1/2, NIST CSF, CSA CCM, CAN CIOSC, CIS) & Attestation (PCI DSS, ISO2700x, SWIFT)
- Secure AI Frameworks
- Security Policy & Procedures Development
- Training and Awareness
- Business Continuity and Disaster Recovery Advisory
- Business Impact Assessment
- Cybersecurity Governance
- Vulnerability Risk Management Program
- Threat Risk Assessment
- Cybersecurity Insurance Compliance

Virtual DPO & Privacy Services

- Virtual DPO Services/Support to Internal DPO
- Compliance Assurance
- Privacy Frameworks
- Data Protection Policies
- Privacy Impact Assessments
- Data Breach Response
- Vendor Management

Vulnerability Assessment

- Vulnerability Scanning
- Risk Assessment for IT and OT/IoT Technologies
- Vulnerability Patching Plans

Training, Social Engineering & Simulations

- Tailored Cybersecurity, Privacy & GRC Training
- Executive & Board Training
- Middle Management Empowerment
- Security-by-Design Training for Technical Staff
- General Employee Awareness
- Social Engineering & Phishing Campaigns
- Agency-Wide Simulations & Tabletop Exercises (Red Team-Blue Team and Purple Team Scenarios).

Cyber Resilience & Business Continuity

- Proactive Resilience Strategies
- Business Continuity Planning
- Disaster Recovery Planning
- Trusted Defense Enhancement
- Incident Response Process and Playbook Development
- Vulnerability Management Audit
- Firewall Policy Audit
- Endpoint Protection Configuration Audit
- Environment Monitoring/Logging Audit
- Cyber Resiliency Assessment

24/7 Managed Security & Incident Response Services

- Managed Detection and Response
- IT/OT/IoT Event Monitoring
- Vulnerability Management
- Managed Security for PCI-DSS Compliance, Including ASV Scanning
- Endpoint Detection and Response
- Network Detection and Response
- Cloud Security Monitoring: Managed Security for AWS, Azure, and M365
- Security Incident Response (Retainer or Post-breach)
- Compromise Investigation and Assessment (May Include Subcontracted Digital Forensics)

Deep Dive: Lane 3 – Cyber Recovery

Lane 3: Cyber Recovery – The "Full Restoration" Lane

Key Objectives:

- **Primary Goal:** Achieve complete, verified recovery of all data and critical*** and non-critical systems.
- **Mindset:** "Comprehensive & Verified." Ensure data integrity and completeness.

Critical Actions:

- Utilize dedicated data protection tools to restore certain critical*** and non-critical data.
- Perform backup and out-of-band integrity checks to ensure recovery points are clean.
- Execute the full recovery of file servers, archives, production and development environments, etc.
- Support the long-tail recovery process that follows the initial emergency.

Tools in Focus: Industry Strength Data Protection and Recovery Tools and Products



Outcome: Full business environment restored with verified data integrity.

Deep Dive: Lane 3 – **Cyber Recovery – “Full Restoration”**

Solution Focus:

Hitachi Vantara Backup and Recovery with VSP 360 – Leverages recovery tools for fast, scalable, and searchable backup cataloging to accelerate recovery.

Hitachi Vantara Data Protection Partner Solutions – Integrated ecosystem for comprehensive data protection, integrity validation, and full restoration of critical*** and non-critical data and systems. Ensures complete, verified recovery with minimal data loss (RPO-driven).

Be prepare to Adopt and Recover

Remember:

***If you are not at the table, you are
on the menu***

Contact Me

BJ Deonarain: bj.deonarain@hitachivantara.com

+1-647-330-0039

Trivia Question

What year was HITACHI commercially founded, and the first commercial product built and what year

Trivia Prize





Gracias