When Systems Fail: BCP/DR Best Practices from an IT Audit Perspective

REAL DISASTERS, REAL LESSONS, REAL ACTIONS

NOBLE W. ANTWI

11/03/2026

The Stakes - Why This Matters

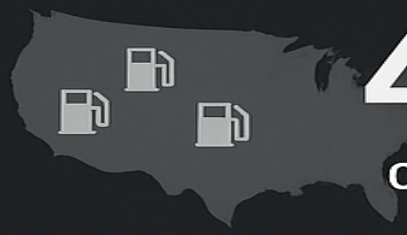
THE COST OF UNPREPAREDNESS

93%

of companies that lose data center for 10+ days filed for bankrupty within one year

$10–11 billion

Cost of NotPetya ransommere (most expensive cyberattack in history)



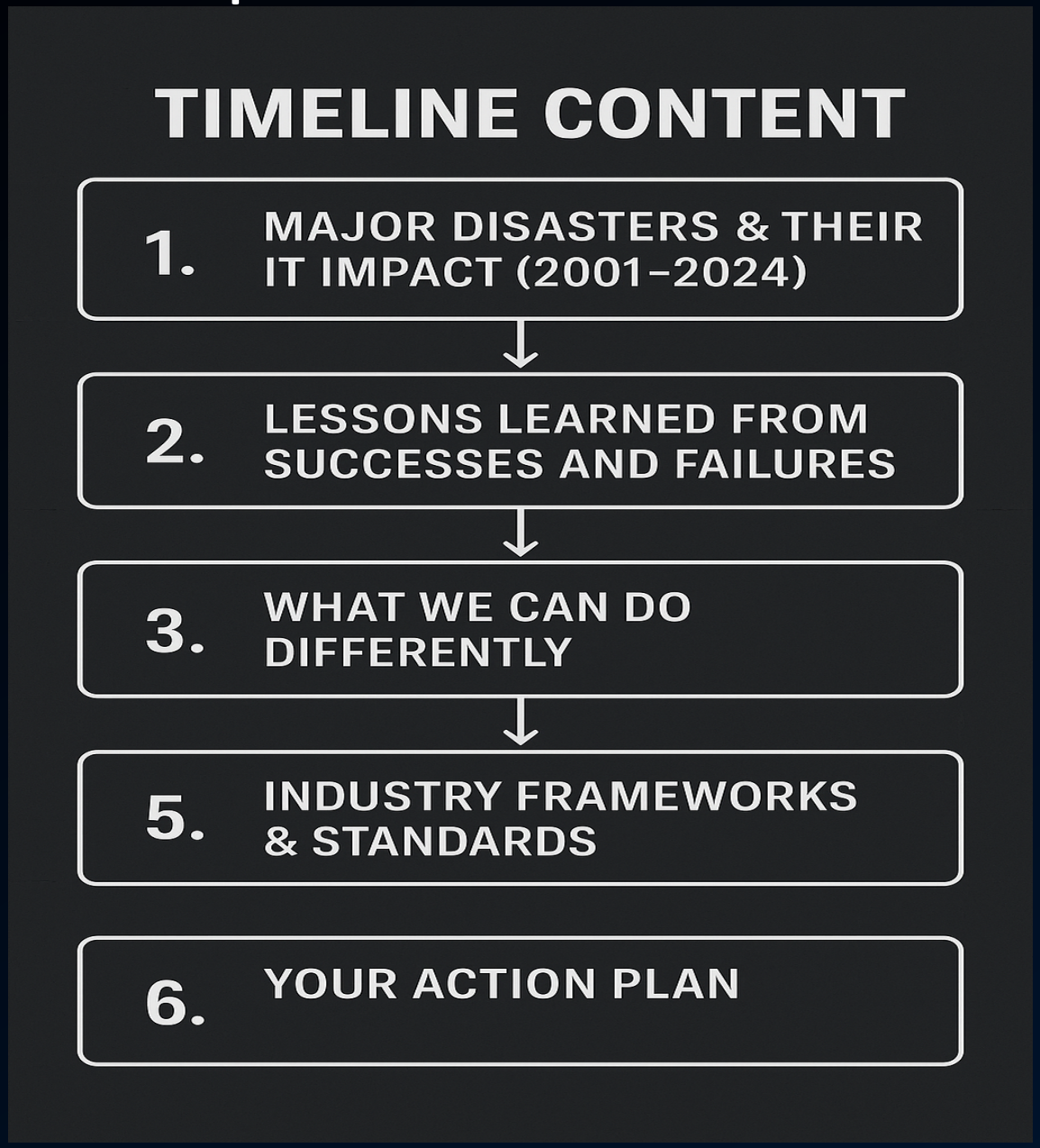
45%

of East Coast fuel supply offline for 5 days (Colonial Pipeline 2021)

8.5 million

devices crashed simultaneously (CrowdStrike 2024)

Session Roadmap



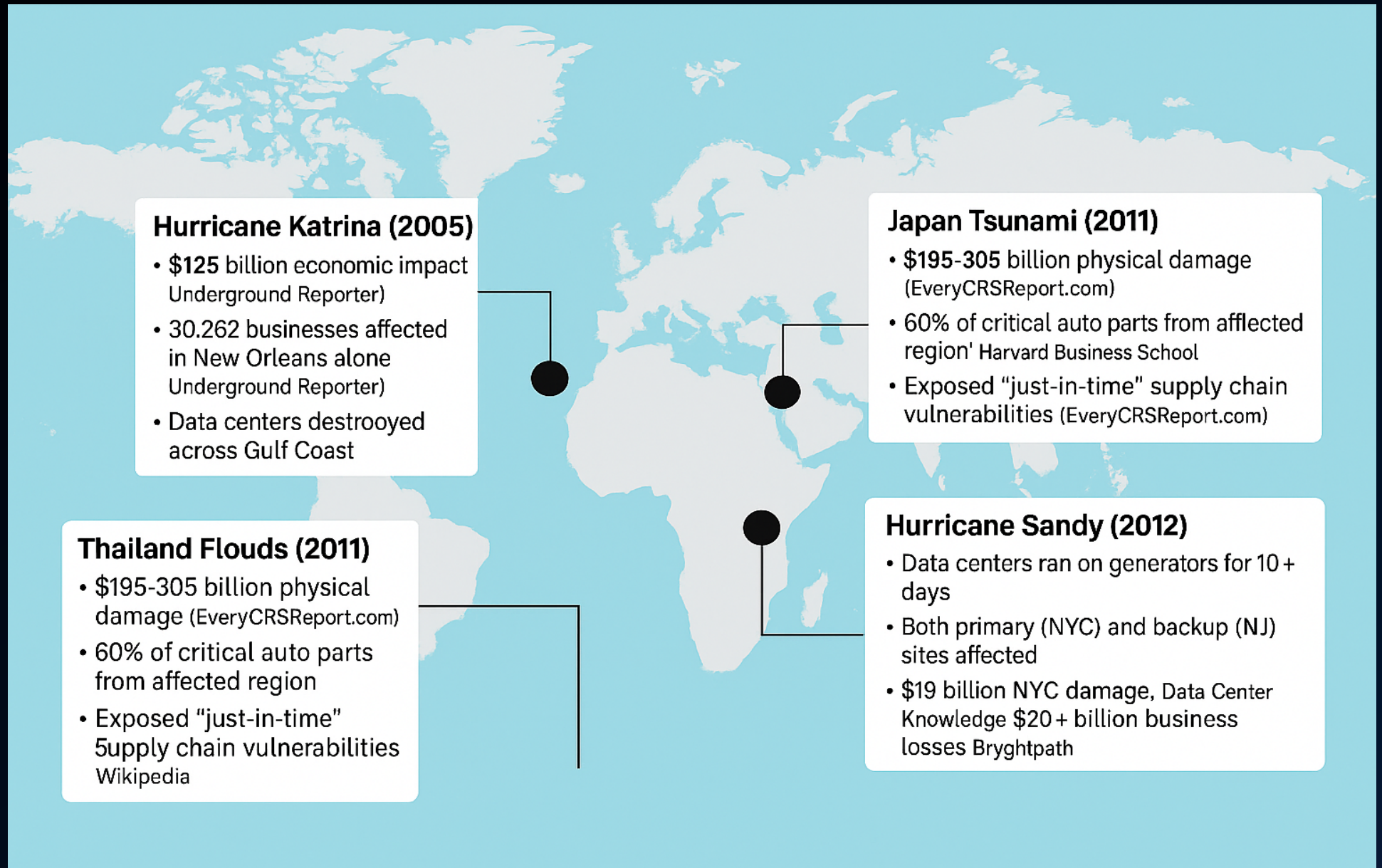
DISASTER EVENTS & SCALE OF IMPACT

- What Was the Disaster?

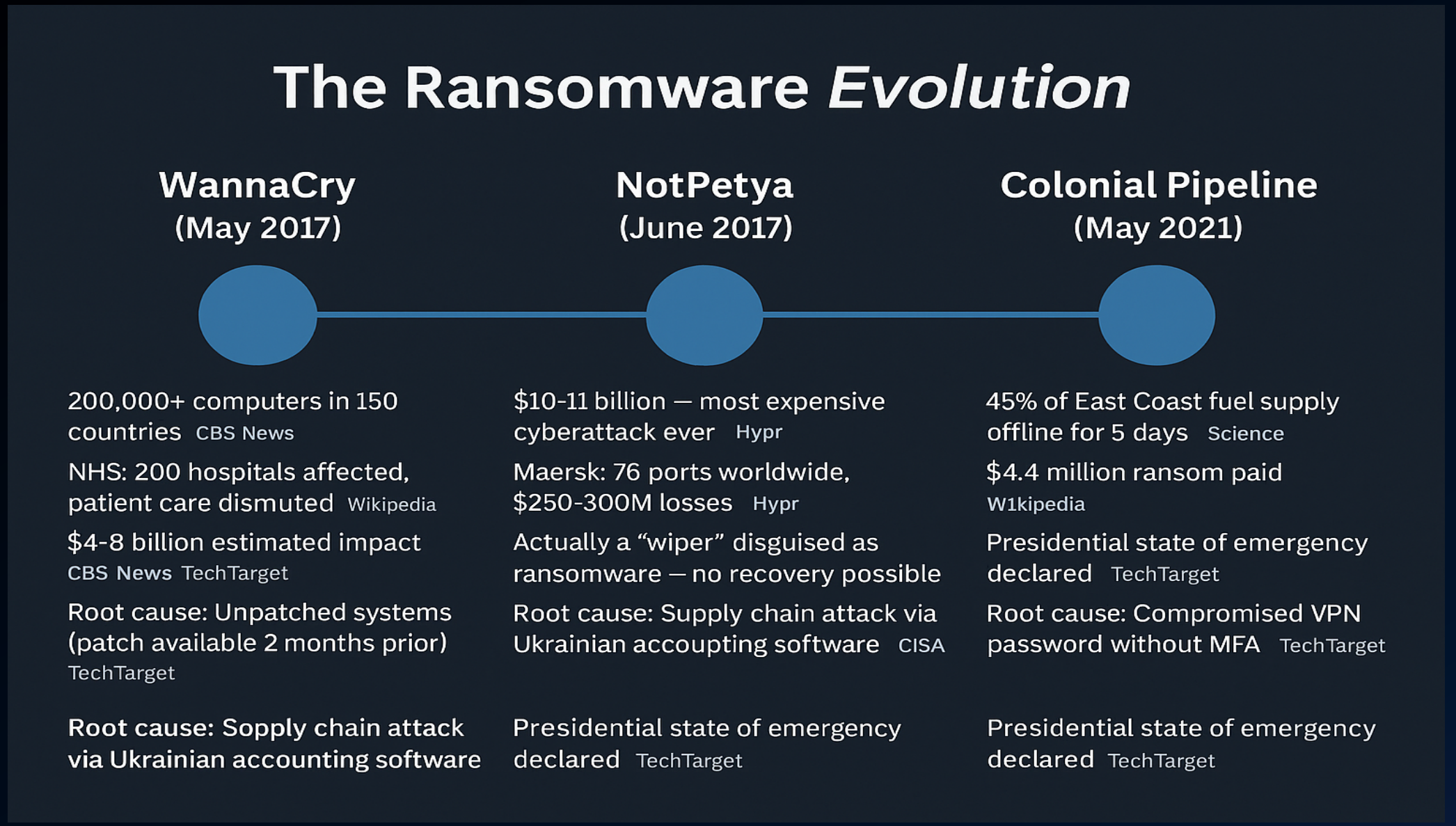
September 11, 2001 - The Paradigm Shift

Date:	September 11, 2001
Impact	World Trade Center towers destroyed
Organizations Affected	Cantor Fitzgerald (658 employees lost, primary data center destroyed) 430+ companies
IT Infrastructure:	Complete data center destruction, telecommunications severely damaged
Recovery Shift	From 24-72 hour recovery expectations to near-instant failover requirements
Key Statistic	Morgan Stanley evacuated 3,528 employees and activated backup site by 9:15 AM

Natural Disasters - When Geography Matters



The Ransomware Evolution



Supply Chain Attacks - The Trojan Horse

SolarWinds (2020)

- 18,000 organizations received compromised updates U.S. GAO
- Russian state actors (SVR)
- Undetected access for months
- 425 of Fortune 500 companies affected
- **Root cause:** Compromised software update mechanism + weak password ("solarwinds123")
- **Key Lesson:** Trusted software becomes weapon

The Pandemic - Business Continuity's Ultimate Test

•**40% of US workforce** moved to remote work

suddenly

•Pre-pandemic remote work: 2.9% (US), 2%

(Europe)

•Organizations with pre-existing remote capabilities significantly outperformed others

•Pre-existing cloud infrastructure Nutanix
•Remote work policies already in place Gartner
•Leadership trust and flexibility Gartner
•Investment in collaboration technologies

•VPN bandwidth expanded 10x

The Pandemic (**COVID-19**)- Business Continuity's Ultimate Test

COVID-19

- **40% of US workforce** moved to remote work suddenly
- Pre-pandemic remote work: 2.9% (US), 2% (Europe)
- Organizations with pre-existing remote capabilities significantly outperformed others
- VPN bandwidth expanded 10x in weeks
- Cloud costs skyrocketed

SUCCESS FACTORS:

•Pre-existing cloud infrastructure Nutanix

•Remote work policies already in place Gartner

•Leadership trust and flexibility Gartner

•Investment in collaboration technologies

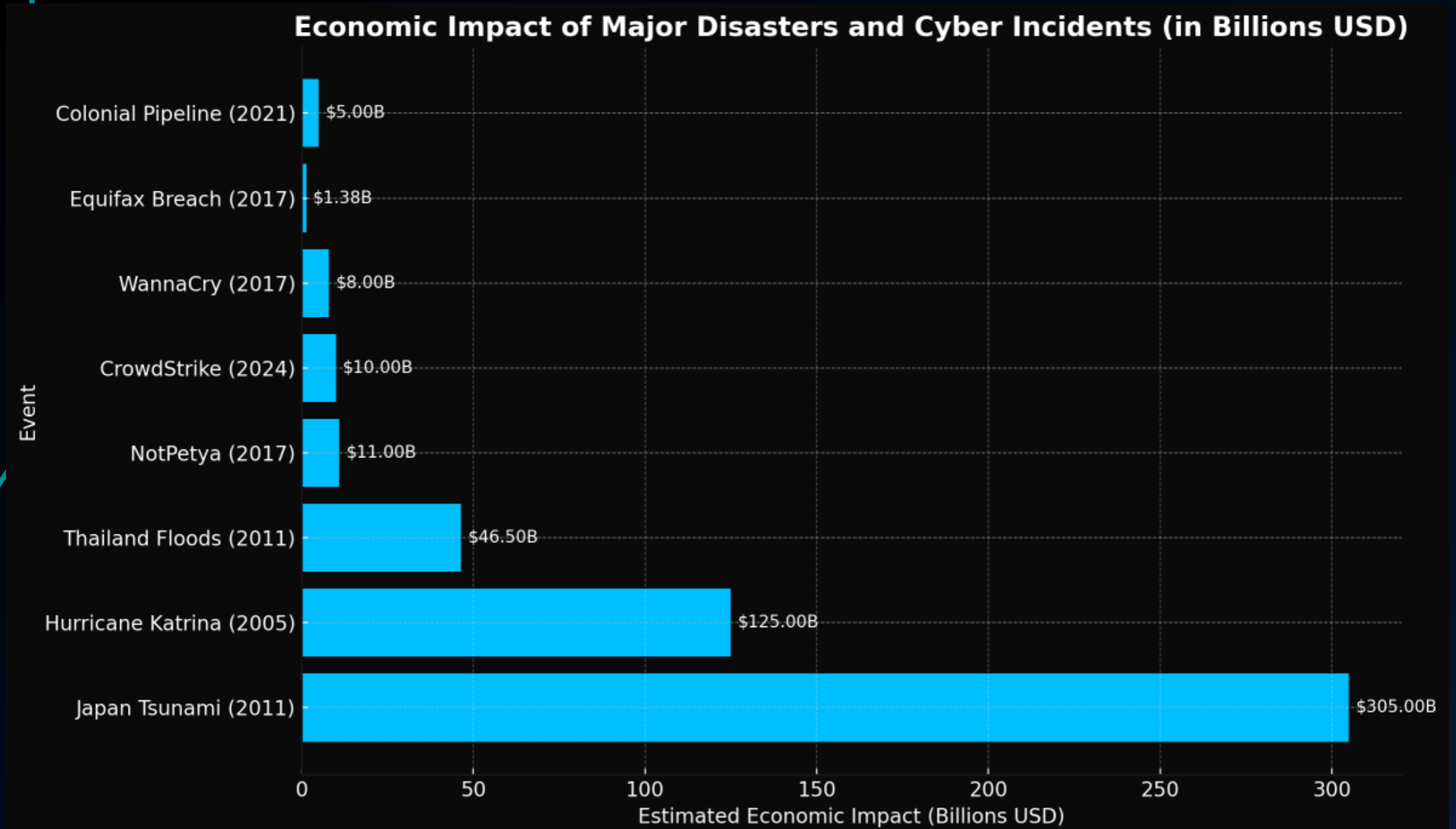
When Software Updates Go Wrong

CrowdStrike Global Outage (July 19, 2024)

- **8.5 million Windows devices** affected globally
- Fortune 500 impact: **$5.4 billion**
- 5,078 flights cancelled (4.6% of all flights)
- Hospitals reverted to paper systems

- **Root cause:** Faulty sensor update deployed without adequate testing

Financial Impact Summary



Fastest Spreading Incidents

- **CrowdStrike (2024):** 8.5 million systems in 78 minutes
- **WannaCry (2017):** 200,000 computers across 150 countries in days
- **NotPetya (2017):** 2,300+ organizations in 100+ countries in days
- **Maersk (NotPetya):** Full network compromise in 7 minutes

LESSONS LEARNED

LESSONS LEARNED: SUCCESS VS. FAILURE

Success Story - Morgan Stanley

WHAT THEY DID RIGHT

- Regular mandatory evacuation drills (despite employee resistance).
- Immediate action when first plane hit Tower 1
- Telecommunications redundancy (4-5 ISPs)
- Backup facilities operational and ready
- Strong security leadership empowered to act

RESULTS

- 2,937 lives saved (of 3,528 in building)
- Operations continued from backup sites within days
- Company survived and thrived

Key Lesson: Investment in drills and redundancy pays off when disaster strikes

Success Story - Maersk NotPetya Recovery

THE CRISIS

- 49,000 laptops destroyed
- 4,000 servers compromised
- Telecommunications redundancy (4-5 ISPs)
- 76 ports globally shut down
- 7 minutes to full network compromise

HOW THEY RECOVERED:

- One domain controller offline in Ghana (power outage) - became foundation for rebuid
- Immediate transparency with customers
- Rebuilt from scratch (10 days for core systems
- Procured 2,000+ devices immediately
- Manual operations maintained 80% capacity

Success Story - Maersk NotPetya Recovery (Contd)

KEY LESSONS

- Geographic redundancy saved them - offline backup was critical.
- All synchronized backups = single point of failure
- **3-2-1 backup rule essential:** 3 copies, 2 media types, 1 offsite
- Transparency builds customer trust

Failure Story - Equifax Data Breach

THE DISASTER

- 147.9 million Americans exposed (40% of US population).
- $1.38 billion total cost
- Executive casualties: CEO, CIO, CSO departed

Key Lesson: Basic security hygiene failure = billion-dollar disaster

WHAT WENT WRONG:

- Critical patch available March 7, not applied; breach began March 10 (3 days later)
- **Expired TLS certificate:** Network monitoring couldn't decrypt traffic for months.
- **Network segmentation failure:** Easy lateral movement.
- **Plaintext credentials** stored on servers
- **Delayed disclosure:** 41 days between discovery and public announcement

Failure Story - TSB Bank IT Migration

THE DISASTER

- 5.4 million customers affected
- 1.9 million locked out of accounts
- Issues lasted 8 months
- £330+ million cost
- CEO and CIO resigned

WHAT WENT WRONG:

- **Big bang approach:** All 1.3 billion records at once.
- **Testing failures:** No full-volume testing
- **Unrealistic timeline:** Announced date before assessment complete
- **No contingency plan:** No rollback capability
- Making live fixes during crisis

Failure Story - TSB Bank IT Migration (Cont’d)

KEY LESSONS

- Big bang migrations are high risk - phased approach essential.
- Full-volume testing is not optional .
- Rollback capability critical for all major changes

Cross-Cutting Lessons - What Works

TECHNOLOGY SUCCESS FACTORS

- Geographic diversity (truly separate regions).
- 3-2-1 backup rule with offline copies
- Network segmentation by data sensitivity
- Automated patch management with enforcement
- Multi-factor authentication everywhere
- Cloud infrastructure for flexibility

Cross-Cutting Lessons - What Works (Cont'd)

PROCESS SUCCESS FACTORS

- Regular testing (not just documentation)
- Phased implementations with rollback capability
- Comprehensive logging with 12+ month retention
- Realistic timelines based on actual work
- Documented, practiced incident response

Cross-Cutting Lessons - What Works (Cont'd)

CULTURE SUCCESS FACTORS

- Executive sponsorship and commitment
- Regular drills and training
- Empowered decision-making in crisis
- Transparency and communication
- Culture of preparedness

Cross-Cutting Lessons - What Fails

RED FLAGS (WARNING SIGNS)

- We're compliant so we're secure.
- Arbitrary deadlines without technical assessment
- Big bang implementations without phased approach
- Untested disaster recovery plans
- Single points of failure
- Legacy/unpatched systems
- Alert fatigue and ignored warnings
- Inadequate vendor oversight
- Backups in same location as primary systems
- No rollback capability for major changes

WHAT CAN BE DONE DIFFERENTLY

WHAT CAN WE DO DIFFERENTLY? FROM REACTIVE TO RESILIENT

Immediate Actions (Within 30 Days)

CRITICAL QUICK WINS

- **Implement MFA on all remote access systems** (Colonial Pipeline lesson).
- **Audit and deactivate unused accounts** (Basic access control)
- **Verify backup systems and test a sample restore** (Test, don't assume)
- **Review and update incident response contact lists** (Outdated contacts = delayed response)
- **Assess logging capabilities and retention** (SolarWinds lesson)
- **Identify systems without tested backups** (Create remediation priority list)

Owner: IT Security Team \ IT Operations **Timeline:** Complete by 12/10/2025

Short-Term Actions (Within 90 Days)

FOUNDATION BUILDING

1. **Conduct Business Impact Analysis (BIA)** for all critical systems
2. Implement network segmentation strategy
3. Deploy or enhance SIEM system
4. Establish patch management SLAs
5. Test disaster recovery procedures
6. Review geographic diversity of critical systems
7. Assess remote work capabilities and capacity

Long-Term Strategic Actions (Within 12 Months)

TRANSFORMATION INITIATIVES

1. Implement zero-trust architecture
2. Develop comprehensive BCP/DR program
3. Replace or isolate legacy systems
4. Establish supply chain security program
5. Conduct annual disaster recovery exercises
6. Implement automated recovery systems
7. Develop metrics for RTO/RPO by system criticality
8. Build redundancy into architecture
9. Establish relationships with incident response firms
10. Create executive-level cyber risk reporting

Technology Investments to Consider

INFRASTRUCTURE RESILIENCE

1. **Cloud-based DR solutions:** AWS DR, Azure Site Recovery, Google Cloud DR
2. **Backup automation:** Veeam, Commvault, Rubrik with air-gapped copies
3. **Network segmentation:** Micro-segmentation tools, zero-trust platforms
4. **SIEM/SOAR:** Splunk, IBM QRadar, Microsoft Sentinel
5. **Patch management:** Automated patch deployment with testing workflows

Technology Investments to Consider (Cont'd)

OPERATIONAL CAPABILITIES:

1. **Business continuity management platforms:** Fusion Framework, Castellan, MetricStream
2. **Incident management:** ServiceNow, PagerDuty
3. **Communication:** Emergency notification systems (Everbridge, AlertMedia)
4. **Collaboration:** Secure remote work infrastructure

Technology Investments to Consider (Cont’d)

TESTING AND VALIDATION:

1. **DR testing automation:** Zerto, Continuity Software
2. **Chaos engineering:** Controlled failure testing
3. **Backup validation:** Automated restore testing

Organizational Changes Needed

GOVERNANCE STRUCTURE

1. BCP/DR Steering Committee

1. Executive sponsor (C-level)
2. Cross-functional representation
3. Quarterly meetings minimum

2. Business Continuity Management Office

1. Dedicated BCP/DR Program Manager
2. Policy development
3. Testing coordination

3. Operational Teams

1. Crisis Management Team
2. IT Recovery Team
3. Business Unit Recovery Teams
4. Communications Team

4. Cultural Changes

1. Make security everyone's responsibility
2. Regular drills despite productivity cost (Morgan Stanley lesson)
3. Empower rapid decision-making in crisis
4. Transparency and communication priority
5. Learn from every incident

5. Metrics That Matter

1. Percentage of systems with documented, tested recovery procedures
2. RTO/RPO compliance rate
3. Testing completion rate
4. ime to recover in actual incidents

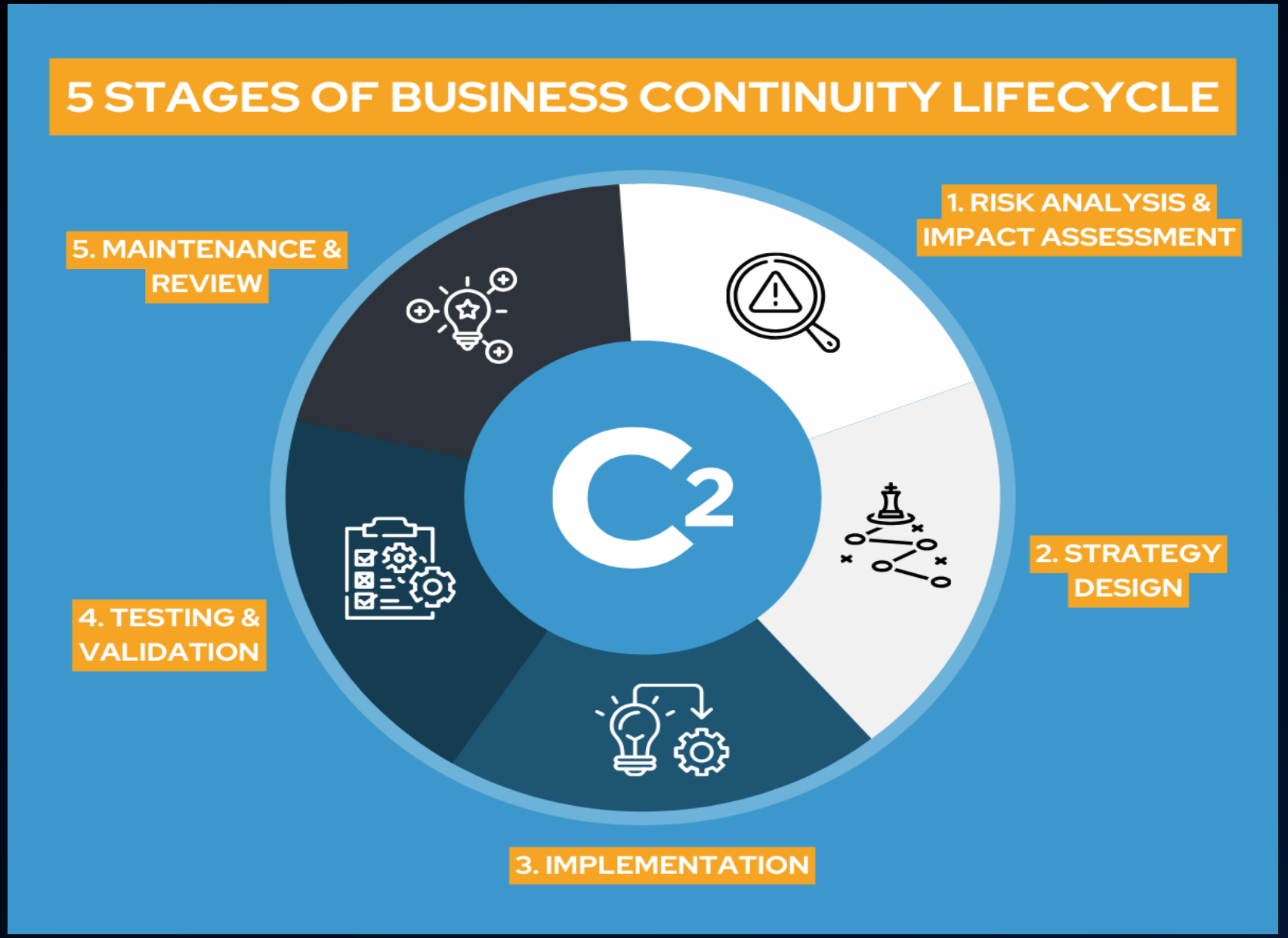
INDUSTRY STANDARDS AND BEST PRACTICES

INDUSTRY FRAMEWORKS: STANDING ON THE SHOULDERS OF GIANTS

NIST SP 800-34 - Contingency Planning Guide

- Develop contingency planning policy statement
- Conduct business impact analysis (BIA)
- **Identify preventive controls**
- Create contingency strategies
- Develop IT contingency plan
- Ensure plan testing, training, and exercises
- Ensure plan maintenance

ISO 22301 - Business Continuity Management



ISO 22301 - Business Continuity Management (Cont’d)

ISO 22301: International Standard for BCMS

PLAN-DO-CHECK-ACT CYCLE:

- **Plan:** Establish policy, objectives, processes
- **Do:** Implement and operate BC plans
- **Check:** Monitor, measure, evaluate
- **Act:** Maintain and improve

KEY REQUIREMENTS:

- Leadership and commitment
- Business continuity policy
- Business impact analysis
- Risk assessment
- Business continuity strategies
- Documented procedures

COBIT for Business Continuity

COBIT 2019: Governance and Management of Enterprise IT

DSS04: MANAGE CONTINUITY

- Ensure service continuity
- Test business continuity plans
- Manage backup arrangements
- Conduct post-resumption review

KEY PRACTICES:

- DSS04.01: Maintain business continuity
- DSS04.02: Develop and implement BC response
- DSS04.03: Test BC plans
- DSS04.04: Manage backups
- DSS04.05: Conduct post-event review

Cloud Disaster Recovery Best Practices

- **Elasticity:** Scale resources on-demand during recovery
- **Geographic distribution:** Deploy across multiple regions easily
- **Cost-effectiveness:** Pay for what you use, no idle infrastructure
- **Speed:** Rapid provisioning of recovery environments
- **Testing:** Easy to test without impacting production

RTO/RPO Industry Benchmarks

Industry	Tier 1 Systems	Tier 2 Systems	Tier 3 Systems
Financial Services	RTO: < 1 hour, RPO: < 15 min	RTO: < 4 hours, RPO: < 1 hour	RTO: < 24 hours, RPO: < 4 hours
Healthcare	RTO: < 2 hours, RPO: < 30 min	RTO: < 8 hours, RPO: < 2 hours	RTO: < 48 hours, RPO: < 8 hours
Manufacturing	RTO: < 4 hours, RPO: < 1 hour	RTO: < 24 hours, RPO: < 4 hours	RTO: < 72 hours, RPO: < 24 hours
Retail/E-commerce	RTO: < 1 hour, RPO: < 15 min	RTO: < 4 hours, RPO: < 1 hour	RTO: < 24 hours, RPO: < 8 hours
Government	RTO: < 4 hours, RPO: < 1 hour	RTO: < 24 hours, RPO: < 4 hours	RTO: < 72 hours, RPO: < 24 hours

Backup Strategy Best Practices

- **3 copies** of your data (1 primary + 2 backups)
- **2 different media types** (e.g., disk + tape, disk + cloud)
- **1 copy off-site** (geographic separation)

- Modern Enhancement: 3-2-1-1-0 Rule
- **3 copies** of data
- 2 different media types
- 1 off-site copy
- **1 offline/air-gapped copy** (ransomware protection)
- **0 errors** in backup validation

IT AUDIT GUIDANCE

IT AUDIT PERSPECTIVE: WHAT WE LOOK FOR

Common IT Audit Findings

- **Inadequate or outdated documentation** (Found in 68% of audits)
- **Insufficient testing** (Found in 61% of audits)
- **Incomplete Business Impact Analysis** (Found in 54% of audits)
- **Backup validation gaps** (Found in 48% of audits)
- **Weak governance** (Found in 45% of audits
- **Third-party risk not addressed** (Found in 42% of audits)
- **Lack of geographic diversity** (Found in 38% of audits)
- **Insufficient logging** (Found in 35% of audits)
- **No patch management process** (Found in 32% of audits)
- **Training gaps** (Found in 29% of audits)

IT Audit Control Frameworks

- Governance Control
- Risk Management Controls
- Recovery Strategy Controls
- Testing and Maintenance Controls
- Documentation Controls
- Audit Evidence Required

Testing Requirements - Progressive Approach

Testing Hierarchy (From Simple to Complex):

- Level 1: Tabletop Exercises
- Level 2: Walk-Through Testing
- Level 3: Simulation/Mock Testing
- Level 4: Parallel Testing
- Level 5: Full Cutover Testing

Regulatory Compliance Considerations

SOX (SARBANES-OXLEY ACT)

- **Applicability:** Public companies
- **Key Requirements:** Section 404 internal controls, DR for financial systems
- **Penalties:** Up to $5M fine, 20 years imprisonment
- **IT Audit Focus:** Financial system recovery capabilities

HIPAA (HEALTH INSURANCE PORTABILITY)

- **Applicability:** Healthcare providers, insurers, business associates.
- Key Requirements
  - Data backup plan (§164.308(a)(7)(ii)(A))
  - Disaster recovery plan (§164.308(a)(7)(ii)(B))
  - Emergency mode operations
- **Penalties:** Up to $1.5M per violation category per year
- **IT Audit Focus:** ePHI protection and recovery

Regulatory Compliance Considerations (Cont’d)

GLBA (Gramm-Leach-Bliley Act)

- **Applicability:** Financial institutions.
- **Key Requirements:** Safeguards Rule, information security program
- **Penalties:** Up to $100K per violation
- **IT Audit Focus:** Customer data protection

GDPR (General Data Protection Regulation)

- **Applicability:** EU data processing
- **Key Requirements:** 72-hour breach notification, data protection measures
- **Penalties:** Up to 4% of global revenue or €20M
- **IT Audit Focus:** Data processing resilience

Regulatory Compliance Considerations (Cont’d)

PCI DSS (PAYMENT CARD INDUSTRY)

- **Applicability:** Organizations handling card data
- **Key Requirements:** Requirement 12.10 incident response plan, annual testing
- **Penalties:** Fines + loss of card processing ability
- **IT Audit Focus:** Cardholder data environment recover

BCP/DR Maturity Model

ASSESS YOUR CURRENT STATE

- Level 1: Initial/Ad Hoc
- Level 2: Developing/Repeatable
- **Level 3: Defined/Consistent ← Target for most organizations**
- Level 4: Managed/Quantitative
- Level 5: Optimized/Adaptive

MATURITY ASSESSMENT TOOLS:

- ISO 22301 Business Continuity Maturity Model
- BCMM® (Business Continuity Maturity Model)
- COBIT 5 Maturity Scoring (0-5 scale)

CONCLUSION - Key Takeaways - What We Learned Today

- Disasters Are Inevitable, Recovery Is a Choice
- Basic Security Hygiene Prevents Most Disasters
- IT Audit Perspective = Business Survival