GRC105 - Incident Management and Business Continuity

Week 20: Practical Simulation Lab Assignment

Ransomware Incident Response Simulation

Course: GRC105 - Incident Management and Business Continuity
Institution: International Cybersecurity and Digital Forensics Academy (ICDFA)
Week: 20 (December 1-7)
Topic: Incident Response Planning
Assignment Type: Practical Simulation Lab
Total Points: 100
Estimated Time: 6-8 hours
Due Date: End of Week 20

Assignment Overview

This practical simulation lab provides hands-on experience responding to a realistic ransomware incident affecting a financial services organization. You will assume the role of **Incident Response Manager** and lead your team through all phases of the NIST Incident Response Lifecycle, making critical decisions under time pressure while documenting your actions and rationale.

The simulation is designed to replicate the complexity, ambiguity, and stress of real-world incident response operations. You will work with incomplete information, face competing priorities, navigate organizational politics, and balance business continuity needs against security imperatives. Your performance will be evaluated based on the quality of your decisions, thoroughness of your documentation, and adherence to incident response best practices.

This assignment bridges the gap between theoretical knowledge and practical application, preparing you for real-world incident response responsibilities in cybersecurity and GRC roles.

Learning Objectives

Upon completion of this simulation, students will be able to:

1. **Execute incident response procedures** across all phases of the NIST Incident Response Lifecycle in a realistic scenario

2. **Make time-sensitive decisions** balancing security, business continuity, legal, and regulatory considerations
3. **Coordinate incident response activities** across multiple stakeholders including technical teams, executives, legal counsel, and external parties
4. **Document incident response actions** maintaining chain of custody and creating defensible records for regulatory and legal purposes
5. **Conduct post-incident analysis** identifying lessons learned and developing actionable improvement recommendations

Simulation Scenario: FinanceFirst Credit Union Ransomware Attack

Organization Background

You are the **Incident Response Manager** at **FinanceFirst Credit Union**, a regional financial institution serving 85,000 members across the Southeastern United States. The organization has the following characteristics:

Organizational Attribute	Details
Industry	Financial Services (Credit Union)
Member Base	85,000 active members
Employee Count	320 employees across 12 branch locations and 1 headquarters
Assets Under Management	$1.2 billion USD
Services Offered	Checking/savings accounts, mortgages, auto loans, business banking, online/mobile banking
Regulatory Requirements	NCUA, FFIEC, GLBA, state banking regulations
IT Infrastructure	Hybrid environment with on-premises core banking system, cloud-based CRM, and member portal
Security Posture	Moderate - basic security controls, annual penetration testing, security awareness training
Incident Response Maturity	Developing - IR plan exists but has not been tested in real incident

Your Role and Authority

As **Incident Response Manager**, you have the following authority and responsibilities:

Authority:

- Direct authority over the Computer Security Incident Response Team (CSIRT) including IT security staff, system administrators, and network engineers
- Ability to request resources and support from other departments (IT operations, legal, communications, branch operations)
- Authority to recommend business decisions to executive leadership including system shutdowns, service disruptions, and external notifications
- Budget authority up to $50,000 for immediate incident response needs (forensics, external consultants, emergency equipment)

Responsibilities:

- Lead all incident response activities from detection through post-incident review
- Coordinate with executive leadership, providing regular status updates and recommendations
- Ensure compliance with regulatory notification requirements
- Maintain documentation and chain of custody for potential legal proceedings
- Protect member data and maintain business continuity to the extent possible

Reporting Relationships:

- You report directly to the **Chief Information Security Officer (CISO)**
- The CISO reports to the **Chief Executive Officer (CEO)**
- You coordinate with **Chief Operating Officer (COO)**, **General Counsel**, and **Chief Communications Officer**

Simulation Timeline and Inject Sequence

The simulation unfolds over a compressed timeline representing **72 hours** of incident response operations. You will receive information "injects" at specific points in the timeline, requiring you to make decisions and take actions. The simulation is divided into **four phases** corresponding to the NIST Incident Response Lifecycle.

Phase 1: Detection and Initial Response (Hour 0-4)

Inject 1.1 - Initial Alert (Monday, 6:45 AM)

You receive an urgent call from the **Night Shift System Administrator** who reports the following:

> *"We're seeing something very strange. Starting about 20 minutes ago, our monitoring system started showing massive file activity on several file servers. Users are calling the help desk saying they can't access shared drives. When I checked one of the servers, I found a text file on the desktop that wasn't there before. It's called 'READ_ME_NOW.txt' and it says all our files have been encrypted and we need to pay Bitcoin to get them back. This looks like ransomware."*

The administrator forwards you the ransom note, which reads:

```
YOUR FILES HAVE BEEN ENCRYPTED

All your important files including databases, documents, and backups have been
encrypted with military-grade encryption. You cannot recover them without our
decryption key.

WHAT HAPPENED?
Your network security is weak. We have been inside your systems for 3 weeks,
stealing your data and preparing for encryption. We now have:
- Complete member database (names, SSNs, account numbers, balances)
- Employee records and payroll data
- Internal communications and emails
- Backup systems (also encrypted)

WHAT DO WE WANT?
Payment of 75 Bitcoin ($2.8 million USD at current rates) within 72 hours.

If you pay within 24 hours: 50 Bitcoin ($1.9 million USD) - 32% discount
If you pay within 72 hours: 75 Bitcoin ($2.8 million USD)
If you do not pay within 72 hours: 150 Bitcoin ($5.6 million USD) + we publish
your member data on the dark web

DO NOT:
- Contact law enforcement (we are monitoring your communications)
- Attempt to decrypt files yourself (you will corrupt them permanently)
- Restore from backups (we encrypted those too)

TO PAY:
Contact us at: [TOR hidden service address]
Bitcoin wallet: [Bitcoin address]

```

```
You have 72 hours. The clock is ticking.
```

Your Task - Inject 1.1:

6 **Immediate Actions** - What are your first three actions in the next 15 minutes? List them in priority order with brief justification.

7 **Initial Assessment** - Based on the information provided, answer the following:
   - Is this a confirmed security incident? Why or why not?
   - What is your preliminary severity assessment (Critical, High, Medium, Low)?
   - What incident type and attack vector are you dealing with?

8 **Stakeholder Notification** - Who needs to be notified immediately, and what will you tell them? Draft brief notification messages for:
   - CISO (your direct supervisor)
   - CEO
   - CSIRT members

9 **Evidence Preservation** - What immediate steps will you take to preserve evidence and maintain chain of custody?

Inject 1.2 - Scope Assessment (Monday, 7:30 AM)

Your security team has completed an initial assessment and reports the following findings:

Affected Systems:

- 8 of 12 file servers encrypted (Windows Server 2019)
- Primary database server encrypted (member account database)
- Email server encrypted (Microsoft Exchange)
- Backup server encrypted (Veeam backup repository)
- 45 workstations encrypted across headquarters and 3 branch locations

Systems NOT Affected (so far):

- Core banking system (IBM AS/400 mainframe - isolated network segment)
- Online banking portal (cloud-hosted by third-party vendor)
- Mobile banking app (cloud-hosted by third-party vendor)
- Network infrastructure (routers, switches, firewalls)
- ATM network (separate isolated network)

Additional Findings:

- Ransomware appears to be **REvil/Sodinokibi** variant based on file extensions (.sodinokibi)
- Encryption started at approximately 6:25 AM
- Security logs show suspicious PowerShell activity starting 3 weeks ago
- Evidence of lateral movement using compromised domain administrator credentials
- Backup server was encrypted 2 hours before production systems

Business Impact:

- Employees cannot access email, shared files, or internal systems
- Branch operations can continue using core banking system for basic transactions
- Online and mobile banking operational (members can access accounts)
- Headquarters administrative functions severely impaired
- Payroll processing scheduled for Wednesday is at risk

Your Task - Inject 1.2:

10. **Containment Decision** - Do you recommend immediate containment actions that may disrupt business operations? Specifically, address:
    - Should you disconnect affected systems from the network?
    - Should you shut down the entire network to prevent further spread?
    - Should you close branch locations or limit operations?
    - Provide justification for each decision considering business impact
11. **Containment Strategy** - Develop a short-term containment plan including:
    - Specific technical actions to isolate the threat
    - Timeline for implementation
    - Expected business impact
    - Mitigation measures to maintain critical operations
12. **External Support** - Do you recommend engaging external resources? Consider:
    - Forensic investigation firm
    - Ransomware negotiation specialist
    - Legal counsel specializing in cyber incidents
    - Cyber insurance carrier
    - Provide cost-benefit analysis for each
13. **Communication Strategy** - The CEO is asking if you should notify members about the incident. What is your recommendation and why? Consider:

- Legal and regulatory obligations
- Reputation and trust implications
- Timing considerations
- What information to disclose (if any)

Inject 1.3 - Executive Pressure (Monday, 9:00 AM)

You are called into an emergency meeting with the executive leadership team. The following stakeholders are present:

- **CEO** - Concerned about reputation damage and member trust
- **COO** - Focused on maintaining business operations and branch functionality
- **CFO** - Worried about financial impact and insurance coverage
- **General Counsel** - Concerned about regulatory compliance and legal liability
- **Chief Communications Officer** - Managing media inquiries (local news has somehow learned about the incident)

The **CEO** makes the following statement:

> *"I understand we have a serious situation, but I need to understand our options. Our cyber insurance policy has a $5 million coverage limit for ransomware payments. The attackers are demanding $2.8 million, or $1.9 million if we pay within 24 hours. That's less than half our coverage limit. If we pay quickly, we can restore operations, protect our members' data from being published, and avoid regulatory scrutiny. I know the FBI says don't pay ransoms, but we have a fiduciary duty to our members. What's your recommendation?"*

The **General Counsel** adds:

> *"We have notification obligations under GLBA and state breach notification laws. If member data was actually exfiltrated, we may need to notify 85,000 members, state regulators, and federal agencies. That's going to be extremely expensive and damaging to our reputation. If paying the ransom prevents data publication and allows us to avoid breach notification, that might be the lesser of two evils."*

The **COO** interjects:

> *"Our branches can operate on the core banking system for basic transactions, but we can't process loan applications, open new accounts, or handle complex transactions. Every day we're down, we're losing business to competitors. We need to restore operations as quickly as possible, whatever it takes."*

Your Task - Inject 1.3:

14 **Ransom Payment Recommendation** - Provide your professional recommendation on whether to pay the ransom. Your response must address:
   - Technical considerations (likelihood of successful decryption, reinfection risk)
   - Legal and regulatory implications (FBI guidance, regulatory expectations)
   - Ethical considerations (funding criminal enterprises, encouraging future attacks)
   - Business considerations (cost-benefit analysis, operational impact)
   - Alternative options (recovery from backups, system rebuilding)

15 **Regulatory Notification Analysis** - Analyze whether the organization has a legal obligation to notify regulators and members at this point. Address:
   - What evidence exists of data exfiltration vs. encryption only?
   - What are the specific notification triggers under GLBA and state laws?
   - What is the timeline for notification if required?
   - What are the consequences of premature vs. delayed notification?

16 **Media Response Strategy** - Local media is calling asking about "computer problems" at FinanceFirst. Draft a brief holding statement for the Communications Officer to use, considering:
   - What can/should be disclosed at this stage?
   - How to maintain member confidence?
   - How to avoid admitting facts not yet confirmed?

17 **Next 24-Hour Action Plan** - Present a clear action plan for the next 24 hours including:
   - Immediate priorities
   - Resource requirements
   - Expected outcomes
   - Decision points requiring executive approval

Phase 2: Containment and Investigation (Hour 4-24)

Inject 2.1 - Forensic Findings (Monday, 2:00 PM)

You engaged an external forensic investigation firm (cost: $35,000 for initial 48-hour engagement). They have completed preliminary analysis and provide the following findings:

Attack Timeline Reconstruction:

Date/Time	Event
Nov 10, 3:42 PM	Initial compromise via phishing email to HR employee
Nov 10, 4:15 PM	Malicious macro executed, TrickBot malware installed
Nov 11-17	Lateral movement, credential harvesting, network reconnaissance
Nov 18	Domain administrator credentials compromised
Nov 19-Dec 1	Data exfiltration (estimated 340 GB transferred to external server)
Dec 1, 4:25 AM	Backup server encrypted
Dec 1, 6:25 AM	Mass encryption of production systems initiated

Data Exfiltration Evidence:

- Network logs show 340 GB of outbound data transfer to IP address in Romania over 2-week period
- Exfiltrated data appears to include:
    - Member database (full copy including SSNs, account numbers, balances, transaction history)
    - Employee records (SSNs, salary information, performance reviews)
    - Email archives (executive communications, board meeting minutes)
    - Loan application documents (financial statements, tax returns, credit reports)
    - Internal audit reports and security assessments

Backup Status:

- Primary backup server encrypted and unusable
- Offsite backup tapes exist but are 45 days old (last successful offsite backup was October 15)
- Cloud backups of email exist and are intact (Office 365 retention)
- Core banking system has separate backup process and is recoverable

Attacker Persistence:

- Multiple backdoors identified in the network
- Compromised credentials still active
- Forensic team recommends complete network rebuild to ensure eradication

Your Task - Inject 2.1:

18 **Breach Notification Determination** - Based on the forensic evidence, has a reportable data breach occurred under GLBA and state laws? Provide detailed analysis including:
   - What data elements were compromised?
   - Does this meet the legal definition of a breach?
   - What are the notification obligations and timelines?
   - Who must be notified (members, regulators, credit bureaus, law enforcement)?

19 **Eradication Strategy** - The forensic team recommends complete network rebuild. Do you agree? Address:
   - Can you safely eradicate the threat without full rebuild?
   - What is the estimated timeline and cost for full rebuild vs. targeted remediation?
   - What is the business impact of each approach?
   - What is the risk of reinfection with each approach?

20 **Recovery Planning** - Develop a recovery strategy considering:
   - What systems should be restored first (prioritization)?
   - Can you use 45-day-old backups for some systems?
   - How will you validate systems are clean before restoration?
   - What is the estimated timeline to full operational recovery?

21 **Ransom Payment Reconsideration** - Given the data exfiltration evidence, does this change your recommendation on ransom payment? The attackers claim paying will prevent data publication. Address:
   - Is there any guarantee they will delete exfiltrated data if paid?
   - Does payment address the breach notification obligations?
   - What is the total cost comparison: ransom payment vs. breach notification and recovery?

Inject 2.2 - Regulatory Contact (Monday, 4:30 PM)

Your General Counsel reports that the **National Credit Union Administration (NCUA)** regional examiner called asking about "rumors of a cybersecurity incident" at FinanceFirst. The examiner stated:

> *"We've heard through industry channels that FinanceFirst may be experiencing a significant cyber incident. As you know, federal credit unions are required to notify NCUA within 72 hours of any reportable cyber incident. We consider ransomware attacks affecting member data or critical systems to be reportable incidents. I need to know the status of your situation and whether you've filed a Suspicious Activity Report (SAR) with FinCEN as required for cyber incidents involving potential fraud or theft."*

Additionally, the General Counsel notes that under the **Gramm-Leach-Bliley Act (GLBA)**, you are required to notify affected members "as soon as possible" after discovery of unauthorized access to sensitive customer information. Several state breach notification laws also apply, with varying timelines ranging from "without unreasonable delay" to specific deadlines of 30-45 days.

The **FBI Cyber Division** also contacted you, stating they are aware of REvil ransomware operations and would like to coordinate with your investigation. They reiterate their position that paying ransoms is not recommended as it funds criminal enterprises and provides no guarantee of data recovery or deletion.

Your Task - Inject 2.2:

22 **NCUA Notification** - Draft the notification you will provide to NCUA including:
- Incident description and timeline
- Systems and data affected
- Response actions taken
- Estimated impact and recovery timeline
- Compliance with notification timeline requirements

23 **SAR Filing Analysis** - Determine whether a Suspicious Activity Report (SAR) must be filed with FinCEN. Address:
- Does this incident meet SAR filing criteria?
- What is the filing deadline?
- What information must be included?

24 **Member Notification Plan** - Develop a comprehensive member notification plan including:
- Notification timeline (when will you notify?)
- Notification method (mail, email, website, media?)
- Notification content (what will you disclose?)

    - Credit monitoring and identity theft protection offerings
    - Call center preparation for member inquiries
    - Estimated cost of notification process
25. **Law Enforcement Coordination** - Decide whether and how to coordinate with FBI. Consider:
    - Benefits of FBI involvement (threat intelligence, investigation support)
    - Risks of FBI involvement (potential publicity, investigation delays)
    - Impact on ransom payment decision
    - Evidence sharing and coordination procedures

Phase 3: Recovery and Restoration (Hour 24-48)

Inject 3.1 - Recovery Decision Point (Tuesday, 6:00 AM)

After 24 hours of intensive incident response, you must make critical recovery decisions. Your team has provided the following status update:

Current Situation:

- All affected systems remain offline and isolated
- Forensic investigation ongoing with multiple backdoors identified
- No additional systems encrypted since initial containment
- Business operations continue at reduced capacity using core banking system
- Member inquiries increasing due to limited service availability

Recovery Options Analysis:

Option A: Pay Ransom and Decrypt

- Cost: $1.9 million (24-hour discount expired, but attackers agreed to extend)
- Timeline: 24-48 hours for decryption keys and system restoration
- Risks: No guarantee of working decryption, reinfection possible, data may still be published
- Additional costs: $200,000 for Bitcoin acquisition and negotiation services

Option B: Rebuild from 45-Day-Old Backups

- Cost: $150,000 for external consultants and emergency equipment

- Timeline: 7-10 days for complete rebuild and validation
- Risks: 45 days of data loss, extensive manual data reconciliation required
- Additional costs: $500,000 estimated for data reconciliation and member account corrections

Option C: Complete Network Rebuild (Forensic Recommendation)

- Cost: $400,000 for complete infrastructure rebuild
- Timeline: 14-21 days for new infrastructure deployment and migration
- Risks: Extended business disruption, potential member attrition
- Benefits: Clean environment, improved security posture, no reinfection risk
- Additional costs: $300,000 for temporary infrastructure and business continuity measures

Option D: Hybrid Approach

- Pay ransom to decrypt critical systems immediately
- Simultaneously rebuild network infrastructure in parallel
- Migrate to new infrastructure once validated clean
- Cost: $2.1 million (ransom) + $400,000 (rebuild) = $2.5 million total
- Timeline: 48 hours to restore operations, 21 days to complete migration
- Benefits: Minimizes business disruption while ensuring long-term security

Business Impact Analysis:

The CFO provides estimated daily revenue loss:

- Day 1-3: $150,000/day (reduced operations, transaction fees lost)
- Day 4-7: $250,000/day (member attrition begins, loan origination halted)
- Day 8+: $400,000/day (significant member attrition, competitive disadvantage)

The COO reports that three large commercial members (representing $45 million in deposits) have indicated they will move their accounts to competitors if full service is not restored within one week.

Your Task - Inject 3.1:

26 **Recovery Strategy Recommendation** - Select one of the four recovery options (or propose an alternative) and provide comprehensive justification addressing:
    - Total cost analysis (direct costs + business impact costs)
    - Timeline and business continuity considerations

    - Risk assessment for each option
    - Long-term security implications
    - Regulatory and legal considerations
    - Recommendation with detailed implementation plan
27. **Executive Briefing** - Prepare a concise executive briefing (1-2 pages) for the Board of Directors explaining:
    - Current situation summary
    - Recovery options with pros/cons
    - Your recommendation and rationale
    - Expected timeline and costs
    - Long-term implications and lessons learned
28. **Implementation Plan** - Develop a detailed implementation plan for your chosen recovery strategy including:
    - Phase-by-phase restoration sequence
    - Resource requirements (personnel, equipment, budget)
    - Validation and testing procedures
    - Rollback procedures if issues arise
    - Communication plan for stakeholders

Inject 3.2 - Complication (Tuesday, 2:00 PM)

As recovery operations proceed, you encounter a significant complication. The **Chief Communications Officer** urgently reports:

> *"We have a major problem. A cybersecurity news website just published an article titled 'FinanceFirst Credit Union Suffers Massive Ransomware Attack, Member Data Stolen.' The article includes screenshots of what appear to be actual member account records posted on a dark web leak site. The attackers are claiming we refused to pay and are now publishing member data as promised. Our phones are ringing off the hook with media inquiries and panicked members. We need a response immediately."*

You verify that the leak site does contain what appears to be legitimate FinanceFirst member data including:

- 500 sample member records with names, SSNs, account numbers, and balances
- A statement claiming the full database of 85,000 members will be published in 24 hours unless payment is received

- Screenshots of internal emails between executives discussing the incident response

The **General Counsel** notes that this public disclosure significantly changes the legal landscape:

- Member notification is now urgent due to public disclosure
- Regulatory notification timelines are accelerated
- Potential class action lawsuits are likely
- Reputational damage is severe and immediate

The **CEO** is furious and demands to know:

- Why the attackers published data despite ongoing negotiations
- Whether paying now will prevent further publication
- How to manage the public relations crisis
- Whether executives should resign to demonstrate accountability

Your Task - Inject 3.2:

29 **Crisis Communication Response** - Draft immediate crisis communication materials including:
    - Public statement for media and website (what will you say publicly?)
    - Member notification letter (required by law, now urgent)
    - Employee communication (internal messaging to staff)
    - Talking points for executives and call center staff

30 **Damage Control Strategy** - Develop a comprehensive damage control plan addressing:
    - Immediate actions to support affected members (credit monitoring, fraud alerts, account monitoring)
    - Media management strategy (press conference, interviews, social media response)
    - Member retention initiatives (fee waivers, enhanced security, relationship management)
    - Regulatory coordination (proactive outreach to NCUA and state regulators)

31 **Ransom Payment Reconsideration** - The attackers are offering a "final chance" to pay $3.5 million (increased from $2.8M) to receive decryption keys and prevent publication of the remaining 84,500 member records. Provide updated recommendation considering:
    - Is there any reason to believe payment will prevent further publication?
    - Does payment provide any value at this point given partial publication?
    - What message does payment send to members, regulators, and future

attackers?
    - Are there better uses of those funds (member support, security improvements)?

32 **Legal and Regulatory Strategy** - Work with General Counsel to develop strategy for:
    - Regulatory notifications and coordination (NCUA, state banking regulators, state attorneys general)
    - Law enforcement coordination (FBI, Secret Service, state law enforcement)
    - Potential litigation defense (class actions, regulatory enforcement)
    - Insurance claims (cyber insurance, D&O insurance)

Phase 4: Post-Incident Activity (Hour 48-72)

Inject 4.1 - Lessons Learned Session (Wednesday, 10:00 AM)

You are conducting a preliminary lessons learned session with the CSIRT and key stakeholders. The following issues and observations have been identified:

What Went Wrong:

33 **Initial Compromise** - Phishing email bypassed email security controls; employee clicked malicious link despite security awareness training

34 **Lateral Movement** - Attacker moved freely through network for 3 weeks undetected; insufficient network segmentation

35 **Credential Compromise** - Domain administrator credentials were compromised and used for lateral movement; no privileged access management (PAM) solution

36 **Detection Delay** - No alerts triggered during 3-week dwell time; SIEM rules insufficient to detect subtle reconnaissance activity

37 **Backup Failure** - Backup server was accessible from production network and encrypted; no air-gapped or immutable backups

38 **Incident Response Plan Gaps** - IR plan existed but had never been tested; confusion about roles and decision-making authority during actual incident

What Went Right:

39 **Core Banking Isolation** - Core banking system on isolated network segment was not affected; business continuity maintained

40 **Cloud Service Resilience** - Online and mobile banking hosted in cloud were unaffected; members could still access accounts

41. **Rapid Containment** - Once detected, containment actions were swift and effective; no additional systems encrypted after initial response
42. **Executive Support** - Leadership provided clear authority and resources for incident response; no bureaucratic delays
43. **External Expertise** - Rapid engagement of forensic firm provided critical intelligence and guidance
44. **Documentation** - Incident response team maintained detailed logs and documentation throughout incident

Stakeholder Feedback:

CISO: "We need to completely overhaul our security architecture. Network segmentation, privileged access management, improved detection capabilities, and immutable backups are non-negotiable going forward."

CEO: "This incident will cost us millions in direct costs, lost business, and reputation damage. I want to understand how we prevent this from ever happening again. What investments do we need to make?"

General Counsel: "We're facing potential regulatory enforcement actions and class action lawsuits. Our incident response and breach notification processes need to be bulletproof going forward. We need clear legal review points built into the IR plan."

COO: "We need better business continuity planning. We were lucky the core banking system wasn't affected, but we had no good options for maintaining operations if it had been. We need redundancy and failover capabilities."

Your Task - Inject 4.1:

45. **Root Cause Analysis** - Conduct a structured root cause analysis using the "Five Whys" methodology for the initial compromise. Start with "Why did the ransomware attack succeed?" and work backwards to identify systemic root causes, not just proximate causes.
46. **Lessons Learned Documentation** - Create a comprehensive lessons learned document including:
    - Incident timeline and key events
    - What worked well (sustain these practices)
    - What didn't work well (improve these areas)
    - Specific recommendations for improvement
    - Responsible parties and implementation timelines
47. **Improvement Recommendations** - Develop prioritized recommendations across three categories:

48 **People (Training and Awareness):**
    - What training gaps were identified?
    - How should security awareness be improved?
    - What incident response training is needed?

49 **Process (Policies and Procedures):**
    - What IR plan updates are needed?
    - What new policies or procedures should be implemented?
    - How should decision-making authority be clarified?

50 **Technology (Security Controls):**
    - What technical security improvements are needed?
    - What detection and response capabilities should be enhanced?
    - What backup and recovery improvements are required?

51 **Metrics and Measurement** - Propose key performance indicators (KPIs) to measure incident response effectiveness going forward:
    - Mean Time to Detect (MTTD)
    - Mean Time to Respond (MTTR)
    - Mean Time to Contain (MTTC)
    - Mean Time to Recover (MTTR)
    - Incident response plan testing frequency
    - Security awareness training effectiveness

Inject 4.2 - Final Incident Report (Wednesday, 4:00 PM)

You must prepare a comprehensive **Final Incident Report** documenting the entire incident for multiple audiences including:

- Executive leadership and Board of Directors
- Regulators (NCUA, state banking authorities)
- Cyber insurance carrier
- Legal counsel (for potential litigation defense)
- Internal audit and compliance

This report will serve as the official record of the incident and will be subject to regulatory review and potential legal discovery.

Your Task - Inject 4.2:

Create a comprehensive Final Incident Report including the following sections:

52. **Executive Summary** (1 page)
    - High-level overview of incident
    - Business impact summary
    - Response actions taken
    - Current status and resolution
    - Key lessons learned
53. **Incident Details** (3-4 pages)
    - Detailed timeline of events from initial compromise through resolution
    - Attack vector and methodology
    - Systems and data affected
    - Attacker tactics, techniques, and procedures (TTPs)
    - Forensic findings and evidence
54. **Response Actions** (2-3 pages)
    - Detection and initial response
    - Containment measures
    - Eradication activities
    - Recovery and restoration
    - Stakeholder communications
55. **Business Impact Assessment** (1-2 pages)
    - Operational impact (systems down, services affected, duration)
    - Financial impact (direct costs, lost revenue, remediation costs)
    - Reputational impact (media coverage, member attrition, brand damage)
    - Regulatory impact (enforcement actions, compliance costs)
56. **Regulatory Compliance** (1-2 pages)
    - Notification obligations and timeline compliance
    - Regulatory coordination and reporting
    - Compliance with GLBA, state breach laws, and banking regulations
    - Outstanding compliance requirements
57. **Lessons Learned and Recommendations** (2-3 pages)
    - Root cause analysis
    - What worked well / what didn't work well

- Specific improvement recommendations (people, process, technology)
- Implementation plan and timeline
- Resource requirements and budget

58 **Appendices**

- Incident timeline (detailed)
- Evidence inventory and chain of custody
- Communications sent (notifications, public statements)
- Forensic reports (summary)
- Regulatory correspondence

Report Requirements:

- Professional formatting with table of contents, page numbers, and version control
- Factual, objective tone appropriate for legal and regulatory review
- Clear documentation of decision-making rationale
- Proper citations and references to supporting evidence
- Executive summary suitable for non-technical audience
- Technical details sufficient for security professionals

Simulation Deliverables

You must submit the following deliverables documenting your incident response actions throughout the simulation:

Deliverable 1: Incident Response Decision Log (20 points)

Create a chronological decision log documenting every major decision you made during the simulation, including:

Timestamp	Decision Point	Decision Made	Rationale	Alternatives Considered	Outcome
Example: Monday 7:00 AM	Initial containment strategy	Isolated affected systems but kept network operational	Balanced containment with business continuity; core banking system needed to remain operational for	Full network shutdown (rejected due to business impact)	Successful containment; no additional systems encrypted

		branches			

Your decision log should include minimum 15 major decision points across all four phases of the simulation.

Deliverable 2: Stakeholder Communication Portfolio (15 points)

Compile all stakeholder communications you drafted during the simulation including:

- Internal notifications (CISO, CEO, CSIRT)
- Executive briefings and recommendations
- Regulatory notifications (NCUA, FinCEN SAR)
- Member notification letter
- Public statements and media responses
- Employee communications

Each communication should be professional, appropriate for the audience, and demonstrate understanding of legal, regulatory, and business considerations.

Deliverable 3: Incident Response Action Plan (20 points)

Document your comprehensive action plan for each phase of the incident response:

Phase 1: Detection and Analysis

- Initial assessment and triage
- Evidence preservation
- Scope determination
- Severity classification

Phase 2: Containment

- Short-term containment actions
- Long-term containment strategy
- Business continuity measures
- External resource engagement

Phase 3: Eradication and Recovery

- Eradication strategy
- Recovery approach and timeline
- Validation and testing procedures

- Return to normal operations

Phase 4: Post-Incident Activity

- Lessons learned session
- Root cause analysis
- Improvement recommendations
- Metrics and measurement

Deliverable 4: Final Incident Report (30 points)

Submit the comprehensive Final Incident Report as specified in Inject 4.2, following the required structure and including all specified sections.

Deliverable 5: Lessons Learned and Improvement Plan (15 points)

Create a detailed improvement plan based on lessons learned including:

Immediate Actions (0-30 days):

- Critical security gaps requiring immediate remediation
- IR plan updates based on actual incident experience
- Quick wins to improve security posture

Short-Term Actions (1-6 months):

- Security architecture improvements
- Process and procedure enhancements
- Training and awareness initiatives

Long-Term Actions (6-12 months):

- Strategic security investments
- Organizational structure changes
- Maturity model advancement

For each recommendation, specify:

- Description and justification
- Responsible party
- Timeline and milestones
- Resource requirements (budget, personnel)

- Success metrics

Submission Requirements

Format and Organization

Submit all deliverables in a single compressed file (ZIP) with the following structure:

```
GRC105_Week20_Practical_[LastName]_[FirstName]/
├── 1_Decision_Log.xlsx or .pdf
├── 2_Communications_Portfolio.pdf
├── 3_Action_Plan.pdf
├── 4_Final_Incident_Report.pdf
├── 5_Improvement_Plan.pdf
└── README.txt (brief description of contents)
```

Formatting Standards

- **Font:** Arial or Calibri, 11-12pt
- **Margins:** 1 inch on all sides
- **Spacing:** Single or 1.15 line spacing
- **Headers/Footers:** Include document title, page numbers, your name, and date
- **Professional Quality:** Business-appropriate formatting, no spelling or grammar errors

File Naming Convention

```
GRC105_Week20_Practical_[LastName]_[FirstName].zip

Example: GRC105_Week20_Practical_Smith_John.zip
```

Grading Rubric

Deliverable 1: Incident Response Decision Log (20 points)

Criteria	Excellent (18-20)	Good (16-17)	Satisfactory (14-15)	Needs Improvement (0-13)
Decision Quality	Decisions are sound, well-reasoned, and aligned with IR best practices	Most decisions are appropriate with minor issues	Some questionable decisions but generally acceptable	Poor decision-making or failure to consider key factors
Rationale and Justification	Clear, comprehensive justification for each decision considering multiple factors	Good justification with minor gaps	Basic justification provided	Weak or missing justification
Completeness	All major decision points documented with thorough detail	Most decision points covered adequately	Some decision points missing or superficial	Significant gaps in decision documentation

Deliverable 2: Stakeholder Communication Portfolio (15 points)

Criteria	Excellent (14-15)	Good (12-13)	Satisfactory (10-11)	Needs Improvement (0-9)
Appropriateness	All communications perfectly tailored to audience and context	Most communications appropriate with minor issues	Communications generally appropriate but some mismatches	Inappropriate tone, content, or approach for audience
Completeness	All required communications included and comprehensive	Most communications included with minor gaps	Some communications missing or incomplete	Significant missing communications
Professional Quality	Exceptionally well-written, clear, and professional	Well-written with minor issues	Acceptable quality with some issues	Poor writing quality or unprofessional

Deliverable 3: Incident Response Action Plan (20 points)

Criteria	Excellent (18-20)	Good (16-17)	Satisfactory (14-15)	Needs Improvement (0-13)
NIST Lifecycle Alignment	Perfect alignment with all four NIST IR phases	Good alignment with minor deviations	Basic alignment with some gaps	Poor alignment or missing phases
Practical Applicability	Action plan is detailed, actionable, and immediately usable	Generally practical with minor ambiguities	Somewhat practical but lacks detail	Vague or impractical action plan
Comprehensiveness	Addresses all aspects of incident response thoroughly	Covers most aspects adequately	Some aspects covered superficially	Significant gaps in coverage

Deliverable 4: Final Incident Report (30 points)

Criteria	Excellent (27-30)	Good (24-26)	Satisfactory (20-23)	Needs Improvement (0-19)
Completeness and Structure	All required sections included with comprehensive detail and logical organization	Most sections complete with minor gaps	Some sections incomplete or poorly organized	Significant missing sections or poor organization
Technical Accuracy	Technically accurate throughout with proper terminology and concepts	Generally accurate with minor errors	Some technical inaccuracies	Significant technical errors
Professional Quality	Exceptionally well-written, formatted, and suitable for executive/regulatory review	Well-written with minor quality issues	Acceptable quality with some issues	Poor quality or unprofessional
Analysis and Insight	Demonstrates deep understanding with insightful analysis	Good understanding with solid analysis	Basic understanding with superficial analysis	Limited understanding or weak analysis

Deliverable 5: Lessons Learned and Improvement Plan (15 points)

Criteria	Excellent (14-15)	Good (12-13)	Satisfactory (10-11)	Needs Improvement (0-9)
Root Cause Analysis	Thorough root cause analysis identifying systemic issues	Good analysis with minor gaps	Basic analysis identifying some causes	Superficial or missing root cause analysis
Recommendations Quality	Recommendations are specific, actionable, prioritized, and well-justified	Good recommendations with minor issues	Basic recommendations lacking detail	Vague or impractical recommendations
Implementation Planning	Detailed implementation plan with timelines, resources, and metrics	Good plan with minor gaps	Basic plan lacking some details	Inadequate or missing implementation plan

Overall Assessment Criteria (Applies across all deliverables)

Bonus Points (up to +5):

- Exceptional creativity or innovation in problem-solving
- Demonstration of advanced knowledge beyond course material
- Outstanding professional quality exceeding expectations

Deductions:

- Late submission: -10% per day (up to 3 days)

- Missing deliverables: -20 points per missing item
- Plagiarism or academic dishonesty: 0 points for assignment + disciplinary action
- Poor grammar/spelling (excessive errors): -5 points
- Failure to follow formatting requirements: -3 points

Learning Resources and References

Students should reference the following materials when completing this simulation:

Primary References

59 **NIST Special Publication 800-61 Revision 3** - Computer Security Incident Handling Guide
   - Provides the foundational framework for incident response
   - Available at: https://csrc.nist.gov/publications/detail/sp/800-61/rev-3/final

60 **CISA Incident Response Plan Basics**
   - Practical guidance for incident response planning
   - Available at: https://www.cisa.gov/incident-response

61 **SANS Incident Handler's Handbook**
   - Step-by-step procedures for incident response
   - Available through SANS Institute

Regulatory Guidance

62 **FFIEC Cybersecurity Assessment Tool**
   - Federal financial institution cybersecurity requirements
   - Available at: https://www.ffiec.gov/cyberassessmenttool.htm

63 **GLBA Safeguards Rule and Privacy Rule**
   - Financial institution data protection requirements
   - Available at: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

64 **State Breach Notification Laws**
   - Varying requirements across jurisdictions
   - Reference: National Conference of State Legislatures database

Ransomware-Specific Guidance

65 **FBI Ransomware Guidance**
   - Law enforcement perspective on ransomware response
   - Available at: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

66 **CISA Ransomware Guide**
   - Technical guidance for ransomware prevention and response
   - Available at: https://www.cisa.gov/stopransomware

Additional Resources

- Course lecture materials from Week 20
- NIST Cybersecurity Framework
- ISO/IEC 27035 Information Security Incident Management
- Your organization's incident response plan (if available for reference)

Simulation Tips and Best Practices

Approach the Simulation Realistically

67 **Think Like an Incident Response Manager** - You are not just answering questions; you are making real decisions with real consequences. Consider business impact, legal implications, and stakeholder concerns.

68 **Work with Incomplete Information** - Real incidents involve ambiguity and uncertainty. Make the best decisions you can with available information, document your assumptions, and be prepared to adjust as new information emerges.

69 **Balance Competing Priorities** - You will face pressure from multiple stakeholders with different priorities (security, business continuity, legal, reputation). Your job is to balance these concerns and make defensible decisions.

70 **Document Everything** - In real incidents, documentation is critical for legal, regulatory, and operational purposes. Maintain detailed logs of your decisions and actions.

71 **Communicate Clearly** - Different audiences require different communication approaches. Executives need concise summaries; technical teams need detailed instructions; regulators need compliance evidence.

Common Pitfalls to Avoid

72 **Rushing to Pay Ransom** - Consider all alternatives before recommending ransom payment. Payment provides no guarantees and funds criminal enterprises.

73 **Delaying Regulatory Notification** - Understand notification requirements and timelines. Delayed notification can result in regulatory penalties.

74 **Inadequate Evidence Preservation** - Maintain chain of custody and preserve evidence from the beginning. You may need it for legal proceedings.

75 **Poor Stakeholder Communication** - Keep stakeholders informed with regular updates. Silence creates anxiety and speculation.

76 **Skipping Post-Incident Review** - The lessons learned phase is critical for continuous improvement. Don't treat it as an afterthought.

Time Management

This simulation requires 6-8 hours of focused work. Recommended approach:

- **Hours 1-2:** Read through all injects and understand the full scenario
- **Hours 3-4:** Work through Phase 1 and Phase 2 injects, creating decision log and communications
- **Hours 5-6:** Work through Phase 3 and Phase 4 injects, developing action plans
- **Hours 7-8:** Compile final incident report and improvement plan, review all deliverables

---

Academic Integrity

This is an **individual assignment**. While you may reference course materials and external resources, all work submitted must be your own original analysis and decision-making. You may not:

- Collaborate with other students on decisions or deliverables
- Share your work with other students or use work created by others
- Use AI tools to generate your responses without proper attribution

You **may** use AI tools for:

- Research and information gathering

- Grammar and writing assistance
- Brainstorming ideas (but decisions must be your own)

Any AI assistance must be disclosed in your submission with a brief statement describing how AI tools were used.

Violations of academic integrity will result in a zero for the assignment and referral for disciplinary action.

Questions and Support

Getting Help

If you have questions about the simulation:

77 **Review the scenario carefully** - Many questions are answered in the detailed injects

78 **Reference course materials** - Week 20 lectures and NIST SP 800-61 provide guidance

79 **Post in discussion forum** - General clarification questions can be posted for all students

80 **Attend office hours** - Individual guidance available during instructor office hours

81 **Email instructor** - For time-sensitive questions, email at least 48 hours before deadline

What You Can Ask About

- Clarification of scenario details or inject information
- Guidance on deliverable formatting or structure
- Technical questions about incident response concepts
- Regulatory requirement interpretation

What You Cannot Ask About

- "What decision should I make?" - This is your professional judgment to demonstrate
- "Is this the right answer?" - There may be multiple defensible approaches
- Requests to review your work before submission - This is an assessment, not a draft

review

Conclusion

This practical simulation provides invaluable experience responding to a realistic ransomware incident. The decisions you make, the actions you take, and the documentation you create mirror real-world incident response operations. Approach this simulation with the seriousness and professionalism you would bring to an actual incident.

Remember: there is rarely one "right" answer in incident response. What matters is that your decisions are:

- **Well-reasoned** - Based on sound analysis and consideration of relevant factors
- **Defensible** - Supported by clear rationale and aligned with best practices
- **Documented** - Properly recorded with justification for future review
- **Appropriate** - Suitable for the organizational context and stakeholder needs

This simulation will challenge you, but it will also prepare you for real-world incident response responsibilities. Good luck!

Instructor: [Insert instructor name]
Contact: [Insert contact information]
Office Hours: [Insert office hours]
Course Website: [Insert LMS link]

This simulation is based on real-world ransomware incidents affecting financial institutions. While the scenario is fictional, the challenges, decisions, and consequences reflect actual incident response operations. Treat this assignment as preparation for your future career in cybersecurity and GRC.