Incident Response Plan, Playbook, and Policy

Course 7

By Evelyn Wolfe

Table of Contents

Executive Summary

This document outlines the foundation for policies and incident response processes at **Circamax | Guardian Telecom Ltd.**, combining the NIST Risk Management Framework (RMF) and the Incident Response Playbook based on the Cynet Template. Together, these approaches provide a clear, actionable and scalable plan to address cyber security threats while aligning with industry best practices.

The NIST Framework focuses on reducing risks by following seven steps: Prepare, Categorize, Select, Assess, Authorize, and Monitor. These steps guide the organization in creating effective security measures. The Cynet Playbook complements this by offering a step-by-step guide for responding to cyber security incidents, ensuring quick and coordinated action when threats arise.

By combining these strategies, **Circamax | Guardian Telecom Ltd.** benefits a proactive approach to preparation, efficient processes for incident handling, and a focus on continuous improvement. This plan not only ensures the organization is ready to respond to security incidents but also clearly defines responsibilities, procedures, and documentation by empowering all employees to play a role in protecting the company's critical assets.

Through this unified framework, **Circamax | Guardian Telecom Ltd.** demonstrates its commitment to security, compliance, and safeguarding sensitive information, providing peace of mind for both the organization and its clients.

Incident Response Plan

This Incident Response Plan integrates the NIST 7-Step Processes, and the Incident Response Playbook from a Cynet Template. While these are policies driven by structured processes and the playbook, the plan needs to be driven from the details. Referencing CISA Framework to assist in creating the plan itself. Together, these elements ensure **Circamax | Guardian Telecom Ltd.** maintains a proactive stance in preparing for, responding to, and recovering from potential threats while safeguarding critical assets and sensitive information.

To build organizational readiness before a cyber security incident, the plan emphasizes the importance of training all staff, conducting attack simulation exercises, and preparing legal, technical and communication strategies. This includes clearly defining roles such as the Incident Manager, Technology Manager, and Communication Manager to ensure effective coordination during an incident. A continuous monitoring strategy, detailed in the NIST framework, is paired with CISA's focus on stakeholder engagement, ensuring that internal and external parties.

During an incident, the plan outlines how these per-defined roles come into action. The Incident Manager leads the response, the Technology Manager addresses technical aspects, and the Communication Manager conducts public communication all while adhering to structured processes from the Cynet playbook. This ensures a methodical approach to incident containment, eradication, and recovery, leveraging real-time situational awareness through continuous monitoring practices.

After an incident, a retrospective meeting is conducted to evaluate the incident response process. Guided by a blameless analysis, the retrospective identifies lessons learned, updated policies, and communicates finding organization-wide to reinforce a culture of security. By combining these frameworks, this plan enhances **Circamax | Guardian Telecom Ltd.'s** ability to manage risk, remain compliant with regulations, and maintain operational resilience in an evolving threat landscape.

Policies developed under NIST 7-Step Process

The objective of the NIST 7-Step process at Circamax | Guardian Telecom Ltd. is to provide a structured framework for developing and managing comprehensive cyber security policies. By systematically preparing for risk, categorizing areas requiring governance, selecting and implementing appropriate controls, assessing their effectiveness, authorizing policies, and continuously monitoring their application, the process ensures that the organization maintains a robust policies framework. These policies define how sensitive information, such as PII and customer data, is protected, accessed, and managed while ensuring compliance with industry regulations. This approach not only reinforces operational security but also establishes clear guidelines and accountability for safeguarding Circama | Guardian Telecom Ltd's critical communication solution and forestering trust with its clients. All policies will be applied to the organization personnel, systems and processes, The systems include internal IT Systems, IoT-enabled devices, and communication platforms. Furthermore all departments and personnel must comply with all policies detailed in this section.

Further breaking down the NIST Seven-Step Processes into actionable policies involves translating each category into detailed, practical guidelines. The processes are structured as follow:

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

Each step provides a foundation for creating clear and comprehensive policies that align with the organization's cyber security objectives and regulatory requirements.

Prepare

The purpose of this policy is to ensure that all levels of the organization are adequately prepared to manage security and privacy risk in alignment with the Risk Management Framework (RMF.) This preparation involves identifying responsibilities, establishing strategies, and implementing processes to mitigate risk effectively.

- Key Risk Management Roles

○ Define and assign key risk management roles, including a Chief Information Security Officer (CISO,) Risk Management Officer, and other stakeholders responsible for risk oversight.

○ Each role will have documented responsibilities and escalation pathways to ensure accountability.

- Risk Management Strategy
    - A formal, organization-wide Risk Management Strategy shall be developed and approved by senior leadership, outlining the approach to risk identification, assessment, and mitigation.
    - The strategy must include the organization's defined risk tolerance and threshold for acceptable risk levels.
- Organization-Wide Risk Assessment

    - The organization shall conduct a comprehensive risk assessment at least annually to identify vulnerabilities, threat, and potential impacts on critical systems, including IoT and communication devices
    - The results of the assessment must be documented and used to prioritize risk mitigation activities.
- Conscious Monitoring Strategy
    - A strategy for continuous monitoring of organizational assets, including system logs, network activity, and IoT devices, shall be developed and implemented
    - The monitoring strategy will include:
        - Defining metrics and performance indicators
        - Use of automated tools for real-time threat detection
        - Regular reporting to leadership on monitoring results and trends

      NIST RMF - Prepare

Categorize

The purpose of this policy is to ensure that organizational risk management processes are informed by a thorough understanding of the adverse impact that could result from the loss of confidentiality, integrity, and/or availability of the system and the information that they process, store, or transmit. This step is critical to prioritizing security measures and aligning resources to protect the most critical assets.

- System Characteristic Documentation
    - All organizational Systems must have their characteristics documented
        - Purpose and Function
        - Interface and Dependencies
        - Data processed, stored, and transmitted
    - Documentation must be maintained in a central repository and updated during system changes, updates, or decommissions
- Security Categorization
    - All systems and their associated data shall be categorized based on their Confidentiality, Integrity, and Availability (CIA) requirements, in align with the NIST Risk Framework (RMF)
    - Categorization process shall consider the potential adverse impact of security breaches of railures, and using the following impact levels
        - Low: Limited Impact
        - Moderate: Serious Incident
        - High: Critical or Catastrophic impact to the company
- Categorization Review and Approval
    - The categorization decision for the systems and information must be reviewed and approved by the designated Authorized Official (AO) or Senior Leadership.
    - Any disagreements or challenges in categorization shall be resolved through documented risk assessment discussion

      NIST RMF - Categorize

Select

The objective is to select, tailor, and document the security and privacy controls necessary to protect organizational systems in alignment with identified risk, ensuring controls are appropriately allocated and monitored for effectiveness.

- Control Baseline Selection and Tailoring
    - Baseline security and privacy controls must be selected based on the system's categorization and associated risk
    - Tailoring of controls shall consider organizational needs, operational environments, and risk tolerance
- Control Designation
    - All controls must be classified as one of the following
        - System-Specific: Controls unique to an individual system
        - Hybrid: Controls shared between multiple systems or processes
        - Common: Controls that apply organization-wide
- Control Allocation
    - Controls must be allocated to specific system components, ensuring accountability and clarity
    - Allocation must be documented to establish traceability between controls and their respective components
- Continuous Monitoring Strategy
    - Continuous monitoring strategy must be developed at the system level, detailing methods for assessing control effectiveness, detecting vulnerabilities and responding to security incident
- Security and Privacy Plan Review and Approval
    - Security and Privacy plans reflect the design of the control selection, designation, and allocation, and these must be reviewed and approved by the designated Authorized Official(AO) or governance body.
    - Plans must include all controls, their rational, and the methods by which their effectiveness is measured
      NIST RMF - Select

Implement

To implement the security and privacy controls specified in the organization's security and privacy plans, ensuring alignment with risk management objectives and updating documentation to reflect the controls as implemented

- Control Implementation
    - All controls specified in security and privacy plans must be implemented as detailed
    - Implementation must adhere to the organizational standards and timelines to ensure consistency and effectiveness
- Documentation Updates
    - Security and Privacy Plans require updating to reflect the implemented controls including
        - Details of the implemented configuration
        - Any deviations from the original plan with reason

Assess

Determining whether a control(s) are implemented correctly, operation as intended, and producing the desired outcomes in meeting the security and privacy requirements for the system and the organization.

- Selection of Assessor/Assessment Team
    - An independent assessor or assessment team must be selected to ensure objectivity and thorough evaluation of controls
- Development of Assessment Plans
    - Security and privacy assessment plans must be developed to outline the scope, methodology, evaluation criteria for assessing the implemented controls
- Review and approval of Assessment Plans
    - All assessment plans must be reviewed and approved by the designated Authorizing Official (AO) or governance body prior to the commencement of assessments
- Conducting Control Assessments
    - Control assessments must be carried out in accordance with the approved assessment plans, ensuring all controls are evaluated for:
        - Correct Implementation
        - Operational Effectiveness
        - Achievement of desire outcomes
- Development of Assessment reports
    - Comprehensive security and privacy assessment reports must be developed to document findings, including identified deficiencies, risk, and recommendations
- Remediation Action
    - Remediation actions must be initiated to address any deficiencies identified during the assessments
    - Actions must be prioritized based on the severity of the identified risks and their potential impact on the organization
- Updates to Security and Privacy Plans
    - Security and privacy plans must be updated to reflect changes in control implementation resultign from assessments and remediations action
- Plan of Action and Milestones
    - A plant of action and milestones must be developed to track remediation efforts, document progress, and ensure accountability for resolving identified deficiencies
      NIST RMF - Assess

Authorize

To ensure accountability by requiring a senior official to evaluate whether the security and privacy risk associated with the operation of the system or the use of the common controls are acceptable, and to render an authorization decision based on the evaluation.

- Development of Authorization Package
    - An authorization package must be created
        - Executive Summary - High-Level overview of the system and associated risk
        - System Security and Privacy Plan - Detailed documentation of implemented controls and their effectiveness
        - Assessment Reports - Results from security and privacy assessment

        - Plan of Action and Milestones - A structured plan for addressing identified risk deficiencies
    - Risk Determination
        - Formal risk determination must be conducted to evaluate the severity and impact of identified risk on organizational object and operations
        - The determination must consider the effectiveness of implemented controls and residual risk
    - Risk Responses
        - Based on the risk determination, appropriate risk responses must be provided
            - Acceptance
            - Mitigation
            - Transfer
            - Avoidance
    - Authorization Decision
        - The senior Authorizing Official (AO) must review the authorization package and determine
            - Approval
                - Approving the system or common controls for operation
            - Denial
                - Deny authorization based on unacceptable risk or insufficient remediation efforts
        - The authorization decision must be documented and communicated to all relevant stakeholders
          NIST RMF - Authorize

Monitor

To maintain ongoing situational awareness of the security and privacy posture of organizational system and operations, enabling informed risk management decisions and ensuring the continued effectiveness of implemented controls.

- Monitoring of Systems and Operational Environments
    - All systems and their operational environments must be continuously monitored in accordance with the organization's approved monitoring strategy
    - Monitoring activities must include the collection and analysis of system logs, network activity, and other relevant metrics
- Ongoing Control Assessments
    - Regular assessments of control effectiveness must be conducted as part of the continuous monitoring strategy
    - Assessment must evaluate the functionality, accuracy and impact of implemented controls in addressing in addressing identified risks
- Analysis and Response to Monitoring Outputs
    - Outputs from continuous monitoring activities such as alerts, logs, and vulnerability report, must be analyzed promptly
    - Identified issues or anomalies must be priortizied and addressed in alignment with organizational risk management protocols
- Reporting Security and Privacy Posture
    - Structured process must be in place to report the organization's security and privacy

posture to management
    - Reports must include insights from monitoring activities, assessment results, and identified risk or deficiencies
- Ongoing Authorization
    - Results from continuous monitoring activities must be used to support ongoing authorization decision
    - Systems and common controls must be re-evaluated periodically to ensure risk remain within acceptable thresholds
      NIST RMF - Monitor

Playbook

Overview

The Incident Response Playbook for Circamax | Guardian Telecom Ltd. is a strategic guide designed to empower the organization's Security Incident Response Team (SIRT) in effectively addressing and mitigating cyber security incidents.

Developed using **Cynet Incident Response Template** as a foundation, the playbook provides a structured framework for handling incidents, assigning responsibilities, and navigating the critical phases of incident response, including preparation, identification, containment, eradication, recovery, and lessons learned.

Key features of this playbook include:

1. **Customizing the Cynet Template**: The template was tailored to align with Circmax | Guardian Telecom Ltd.'s specific operational needs, internal systems, and organizational structure.
2. **Defining Key Processes**: Each phase of incident response, as outlined by the SANS Institute, was meticulously adapted to reflect the organization's existing protocols and anticipated challenges. These phases include Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
3. **Actionable Details**: Clear actions were detailed for each phase, with specific instructions for identifying and addressing security incidents, analyzing audit logs, isolating threats, and documenting every step of the process.
4. **Incorporating Organizational Context**: The playbook includes references to internal tools, team members, and specific assets, ensuring its relevance and applicability to Circmax | Guardian Telecom Ltd.
5. **Testing and Continuous Improvement**: A section on Testing and Updates emphasizes the importance of annual and biannual testing of the Incident Response Plan, incorporating real-world incident reviews to identify gaps and improve processes.

This playbook reflects a blend of industry best practices and tailored Strategies, equipping Circamax | Guardian Telecom Ltd. to minimize risk, enhance resilience, and stay ahead of cyber security threats.

Roles, Responsibilities & Contact Information

This Security Incident Response Plan must be followed by all personnel, including employees,temporary staff, consultants, contractors, suppliers and third parties operating on behalf of **Circmax | Guardian Telecom Ltd.** Throughout this plan, all personnel are collectively referred to as staff. The plan outlines the roles, responsibilities, and contact information necessary to prevent and respond to workplace incidents. While not an exhaustive list of duties, it provides staff with a clear understanding of their responsibilities and the responsibilities of others during an incident. By fostering clarity and accountability, this plan will enable a coordinated and efficient response to security incidents, minimizing potential harm to the organization and its stakeholders.

Incident Response Team Responsibilities

- Incident Response Lead is responsible for the following:
    - Ensuring that the Security Incident Response Plan, and associated response and escalation procedures are clearly defined and documented and capable of handling security incidents in a timely and effective manner
    - Verifying that the Security Incident Response Plan is current, reviewed and tested at least twice a year
    - Ensuring that staff with responsibilities outlined in the Security Incident Response Plan receive proper training at least once a year
    - Leading the investigation of suspected breach or reported security incident and initiating the Security Incident Response Plan when necessary
    - Communicating with and providing necessary reports to external parties, such as business partners, legal representative, law enforcement, and other relevant entities, to ensure proper coordination and resolution of incidents
    - Authorizing on-site investigation conducted by appropriate law enforcement or third party security/forensic personnel during any security incident investigation, including granting access to or removal or evidence from the site
    - Ensuring that all staff understand how to identify and report a suspected or actual security incident
    - Advising the Incident Response Team of an incident upon receiving a security incident report from staff
    - Investigating and documenting each reported incident
    - Taking action to limit the exposure of sensitive data and to reduce the risk associated with any incident
    - Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls
    - Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to the reported incident
    - Assisting law enforcement during the investigation process. Includes any forensic investigation and prosecutions
    - Initiating follow-up actions to reduce likelihood of recurrence as appropriate
    - Determining if policies, processes, technologies, security measures of controls need to be updated to avoid a similar incident in the future and assessing whether additional safeguards are required in the environment where the incident occurred
      (CYNET SIRT, Page 2-3)
- All Staff Members are responsible for:

- Ensuring Staff Members understand how to identify and report a suspected or actual security incident
- Reporting suspected or actual security incident to the Incident Response Lead or to another member of the Security Incident Response Team
- Reporting any security-related issues or concerns to line of management, or to a member of the Security Incident Response Team
- Complying with the Security policies and procedures of Circamax | Guardian Telecom Ltd. (CYNET SIRT, Page 4)

Roles, Responsibilities and Contact Info

Information Security

Roles	Responsibility	Contact Details
CSO/CISO	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plans. Authorizes when and how incident details are reported. Main point of contact for the executive team and Board of Directors.	Name: Phone: Email:
Incident Response Team Lead and Team Members	Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident. Maintains incident response plan, documentation, and catalog of incidents. Responsible for identifying, confirming, and evaluating the extent of incidents. Conducts random security checks to ensure readiness to respond to a cyberattack.	Name: Phone: Email:
Identity and Access Team Lead and Team Members	Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior. Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks. Takes action to prevent the spread of a breach by updating privileges.	Name: Phone: Email:
IT Operations and Support (internal)	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.	Name: Phone: Email:
Technical Partners (ISP, MSP, Hosting, Testing Partners, etc.)	Manages security controls to limit the progression of a cyberattack across third-party systems and organizations	Name: Phone: Email:
Third Party External Incident Response Teams	Coordinates with the Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can	Name: Phone: Email:

	be available in an emergency IR situation and provide any requested information prior to an emergency to help them become familiar with your environment.	

Compliance

Roles	Responsibility	Contact Details
Legal Counsel	Confirms requirements for informing employees, customers, and the public about cyber breaches. Responsible for checking in with local law enforcement. Ensures IT team has legal authority for privilege account monitoring.	Name: Phone: Email:
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	Name: Phone: Email:
Human Resources	Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees	Name: Phone: Email:
Regulatory Contacts	Receives information about a breach according to timeline and format mandated by regulatory requirements.	Name: Phone: Email:

Communications

Roles	Responsibility	Contact Details
Marketing & Public Relations Lead	Communicates externally with customers, partners, and the media. Coordinates all communications and requests for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Name: Phone: Email:
Web & Social Media Lead	Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media.	Name: Phone: Email:
Technical Support Lead (Internal)	Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.	Name: Phone: Email:
Technical Support Lead (External)	Provides security bulletins and technical guidance to external users in case of a breach.	Name: Phone: Email:

Testing and Updates

Practice and Walkthroughs of potential incident scenarios should be conducted to test the Incident Response Plan should be an annual schedule. These tests are designed to assess the readiness of Circmax | Guardian Telecom Ltd in the event of an incident. If a real incident occurs, it can serve as a practical test of the full functionality of the process.

- The Incident Response Plan will be tested at least once annual, with a target of twice a year
- The testing process will evaluate Circamax | Guardian Telecom Ltd's response to potential incidents scenarios, aiming to identify process gaps and improvement
- During the test, The Security Incident Response Plan (SIRT) will document observations, including steps that were poorly executed or misunderstood by participants, as well as aspects that require improvement
- The Incident Response Lead will ensure the Security Response Plan is updated based on test findings and distributed to the all SIRT members

Incident Response Process Overview

As defined by SANS Institute in their *Incident Handler's Handbook*, the following six steps outline the process flow for documentation.
(SANS - Pg 2-9)

1. **Preparation:**
    - Review and formalize the organizational security policy
    - Perform a risk assessment, identify sensitive assets, and define critical security incidents for the team to prioritize
    - Establish a Computer Security Incident Response Team (CSIRT.)
2. **Identification:**
    - Monitor IT Systems to detect deviations from normal operations and assess whether they represent actual security incidents
    - Upon discovering an incident, collect additional evidence, determine its type and severity, and document all findings
3. **Containment:**
    - Perform short-term containment measures, such as isolating the network segment under attack
    - Implement long-term containment strategies, which may involve temporary fixes that allow systems to remain operational while rebuilding clean systems
4. **Eradication:**
    - Removal of malware from all affected systems
    - Identify the roots cause of the attack and take action to prevent similar incidents in the future
5. **Recovery:**
    - Bringing the affected production system back online cautiously to avoid further attacks
    - Testing, verify, and monitor the systems to ensure they are back to normal operations
6. **Lessons learned:**
    - Conduct a retrospective review of the incident no later than two weeks after resolution

- Prepare comprehensive documentation of the incident, investigate it further, and evaluate containment measures. Identify areas for improvement in the incident response process

Incident Response Checklist

Incident Discovery and Confirmation

Phase of Cyber Incident	Action	Team Member / System	Day/Time Action Take
Incident Discovery and Confirmation	Describe how the team first learned of the attack (e.g., security researcher, partner, employee, customer, auditor, internal security alert, etc.)		
	Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm that an attack has occurred		
	Describe the potential attacker, including known or expected capabilities, behaviors, and motivations		
	Identify the access point and source of the attack (e.g., endpoint, application, malware downloaded, etc.) and the responsible party		
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response		
	Check applications for signatures, IP address ranges, file hashes, processes, executable names, URLs, and domain names of known malicious websites		
	Evaluate the extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed (see Appendix A for more information on Threat Classification		
	Review your information assets list to identify which assets have been potentially compromised. Note the integrity of assets and evidence gathered (see Appendix A for more information on Threat Classification)		
	Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the		

	network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.		
	Inform employees regarding discovery.		
Incident Discovery and Confirmation	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools		
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements		

Containment and Continuity

Phase of Cyber Incident	Action	Team Member / System	Day/Time Action Take
Containment and Continuity	Enable temporary privileged accounts for the technical and security teams to quickly access and monitor systems.		
	Protect evidence by backing up any compromised systems as soon as possible, ensuring no actions are taken that could affect data integrity on the original media.		
	Implement multi-factor authentication or peer review processes to ensure privileged accounts are being used appropriately.		
	Change passwords for all user, service, application, and network accounts to reduce the risk of unauthorized access.		
	Increase the sensitivity of application security controls (e.g., allowing, denying, and restricting access) to prevent the attacker from distributing malicious malware.		
	Remove systems from production or take systems offline as necessary to contain the incident.		
	Inform employees about the steps being taken to contain the breach and any necessary actions they should follow.		
	Analyze, document, and confirm any instances of potential data exfiltration across the network.		
	Potentially share breach containment updates		

	externally via website, email, social media, or tech support, ensuring compliance with regulatory requirements.		

Eradication

Phase of Cyber Incident	Action	Team Member / System	Day/Time Action Take
Eradication	Close firewall ports and terminate unauthorized network connections.		
	Test devices and applications to confirm that all malicious code has been removed.		
	Compare system data before and after the incident to ensure systems are fully restored and reset properly.		
	Inform employees about the eradication process and any actions required on their part.		
	Share eradication updates externally, if necessary, through website updates, emails, social media posts, or tech support bulletins, ensuring compliance with regulatory requirements.		

Recovery

Phase of Cyber Incident	Action	Team Member / System	Day/Time Action Take
Recovery	Download and apply all relevant security patches.		
	Close network access points and reset passwords for all accounts.		
	Conduct a thorough vulnerability analysis to identify and address any remaining weaknesses.		
	Return systems taken offline back to production once they have been verified as secure.		
	Inform employees about the recovery process and any necessary follow-up actions.		
	Share recovery updates externally through website updates, emails, social media posts, or tech support bulletins, ensuring compliance with regulatory requirements.		
	Review and analyze all forensic evidence collected to confirm the incident is fully resolved		

	and to strengthen future response efforts.		

Lesson Learned

Phase of Cyber Incident	Action	Team Member / System	Day/Time Action Take
Lesson Learned	Assess the financial, operational, and reputational costs of the incident.		
	Prepare an executive summary detailing the incident, the response actions taken, and the outcomes.		
	Report findings to the executive team and auditors, if required.		
	Implement additional training for all employees involved in the incident response, as well as for the broader organization, to enhance awareness and preparedness.		
	Update the Incident Response Plan based on lessons learned to improve its effectiveness for future incidents.		
	Inform employees about the lessons learned, any changes to procedures, and upcoming training opportunities.		
	Share information externally, if appropriate, through channels such as website updates, emails, social media posts, or tech support bulletins, ensuring alignment with compliance and regulatory requirements.		

Responsibilities At-A-Glance

	CSIRT Incident Lead	IT Contact	Legal Representative	Communication Officer	Management
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact	Updates	Updates	Advises	Updates	Owner

Document Name:	Security Incident Response Plan
Current Version:	
Plan Owner:	
Plan Approver	
Date of Last Review	

Consequences of Non-Compliance for both Company and Individual

Non-Compliance with industry regulation, internal policies, or cyber security best practices can have significant consequences for **Circamax | Guardian Telecom Ltd.** At an organizational level, failure to adhere to the Telecommunication Act, Personal Information Protection and Electronic Documents Act (PIPEDA,) or ISO standards could result in hefty fines, legal actions and the suspension of licenses critical to operation in the telecom industry. Additionally, a lack of compliance could tarnish the company's reputation, leading to the loss of trust from clients and partners who rely on **Circamax** for secure and reliable telecommunications products. This could result in a decline in business opportunities and long-term financial losses.

For individual employees, non-compliance with security protocols-such as mishandling sensitive customer data, neglecting to follow access control policies, or failing to report potential incidents could lead to disciplinary action, up to and including termination of employment. Employees who fail to follow regulatory requirements may also face personal legal consequences, especially if their actions result in data breaches or violations of privacy laws. Ultimately, a culture of non-compliance compromises not only the organization's operational stability but also its employee' job security and professional credibility. Ensuring that every individual understands and follows established policies is critical to maintaining the organization's security posture and regulatory standing.

Citations and References

Playbook Citations:

Original Playbook for Course 7.2, written by Evelyn Wolfe
https://docs.google.com/document/d/1Nz75i33GZriyLBE84O7-ZHa5l7sj_irqPi13f_5xJ20/edit?usp=sharing

Tubin, G. (2025, January 2). *Top 8 Incident Response Plan Templates and why you should Automate your incident response*. All-in-One Cybersecurity Platform - Cynet. https://www.cynet.com/incident-response/incident-response-plan-template/

NIST 7-Step Process

NIST Computer Security Resource Center (CSRC) U.S. Department of Commerce. (Date Accessed: 2025, January 20). *About the RMF - NIST Risk Management Framework | CSRC | CSRC*. https://csrc.nist.gov/projects/risk-management/about-rmf

Incident Plan:

CISA. (2021). Incident Response Plan (IRP) basics. In *CISA | DEFEND TODAY, SECURE TOMORROW* [Report]. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf