Incident Response Plan & Technical Controls for Deerfield Beach Police Department

By

Cyber Security Intern

Aadith Preetham (C0902681)

Submission: 7 Mar 2025

Table of Contents

Introduction

The Deerfield Beach Police Department (DBPD) operates in an increasingly digital environment where cyber threats pose significant risks to law enforcement operations, officer safety, and community trust. As custodians of sensitive law enforcement data, DBPD must be prepared to detect, respond to, and recover from cyber incidents effectively.

The Incident Response Plan (IRP) provides a structured framework to manage cybersecurity incidents and ensure the continuity of police operations. It is designed to minimize damage, prevent escalation, and ensure a swift recovery in the event of a cyber attack. The IRP follows the NIST SP 800-61 Rev. 2 guidelines and is tailored to DBPD's structure, which includes police officers, cybersecurity officers, and interns.

To strengthen Deerfield Beach Police Department's cybersecurity posture, we have integrated a real-world case study: APT29 (Cozy Bear) – U.S. Defense and Law Enforcement Attacks (2021). This historical attack provides valuable lessons on supply chain threats, phishing campaigns, and advanced persistent threats (APT), enabling DBPD to adopt proactive security measures against similar attacks.

Scope

This Incident Response Plan (IRP) applies to all Deerfield Beach Police Department (DBPD) personnel, as well as third-party vendors accessing Deerfield Beach Police Department systems.

Systems Covered

- Internal Networks & Servers – Case management, evidence storage.
- Endpoint Devices – Patrol laptops, mobile devices, workstations.
- Cloud & Remote Systems – Secure police databases, SaaS applications.
- Forensic & Surveillance Systems – CCTV, digital forensics tools.
- Public-Facing Portals – Citizen complaint systems, emergency alerts.

Legal & Compliance

This plan aligns with CJIS Security Policy, NIST Cybersecurity Framework, and Florida law enforcement regulations to protect sensitive police data and operations.

This IRP ensures a rapid response to cyber incidents, minimizes risks, and maintains DBPD's operational integrity.

Integrating APT29 (Cozy Bear) – U.S. Defense and Law Enforcement Attacks (2021)

APT29 (Cozy Bear) is a Russian-state-sponsored cyber espionage group known for targeting government agencies, law enforcement, and defense organizations. In 2021, APT29 conducted a coordinated attack against U.S. law enforcement agencies, using:

- Spear-phishing emails to steal credentials.
- Zero-day exploits to gain access to government systems.
- Supply chain compromises to infiltrate networks.
- Persistence techniques to maintain access and exfiltrate classified data.

Relevance:

Given that Deerfield Beach Police Department officers, cybersecurity staff, and interns regularly communicate with state and federal agencies, an attack like APT29's campaign could:

- Compromise police evidence databases and case files.
- Allow attackers to monitor police communications.
- Result in identity theft or misuse of officer credentials.

To counter such threats, Deerfield Beach Police Department's IRP incorporates advanced security controls and a structured response framework to detect, contain, and mitigate similar nation-state-level cyber threats.

What qualifies as an Incident?

A cybersecurity incident is any event that compromises DBPD's digital security, disrupts operations, or leads to unauthorized data access. Examples of Cyber Security Incidents are:

- Unauthorized Access: A hacker gains access to DBPD's databases and views sensitive case files.
- Phishing Attacks: An officer receives an email appearing to be from the Chief of Police, asking them to reset their password. The attacker then uses the stolen credentials to log in.
- Malware/Ransomware: A DBPD officer opens an email attachment that installs ransomware, encrypting all patrol reports and evidence storage files.
- Data Breach: Confidential law enforcement records, including witness statements, are leaked online.
- Denial-of-Service (DoS) Attacks: The DBPD website and emergency dispatch system become slow or completely inaccessible due to excessive malicious traffic.

Severity Matrix for different kinds of Incidents:

Severity Level	Example Incidents	Urgency & Response
Critical	Ransomware attack affecting police case files; Data breach exposing officer payroll and personnel records.	Immediate full-system lockdown, notify FBI/CISA, activate full Incident Response Team.
High	Unauthorized remote access to surveillance systems; Successful phishing attack compromising admin accounts.	Immediate containment, password resets, forensic analysis.
Medium	Repeated failed login attempts on an officer's laptop; Suspicious network activity detected.	Monitor activity, enforce MFA, reset affected accounts.

Low	Single unsuccessful login attempt; Officer receives a phishing email but does not click.	Security awareness training, email filtering.

Incident Response Plan

The plan is divided into 6 phases to handle cybersecurity incidents effectively:

Phase 1: Preparation

- Train staff to recognize and report incidents.
- Conduct regular security awareness programs and phishing simulations.
- Maintain and test incident response tools like firewalls, endpoint protection, and backup systems.
- Define roles and responsibilities of the Cyber Security Incident Response Team (IRT).
- Perform regular vulnerability assessments and patch management.

Suggested Tools**:**

- Google Authenticator or Microsoft Authenticator (for Multi-Factor Authentication - MFA)
- pfSense or Cisco Firewalls (for perimeter security)
- Acronis Cyber Backup (for secure system backups)

Phase 2: Identification

- Monitor systems using Security Information and Event Management (SIEM) tools.
- Investigate alerts for signs of suspicious activity (e.g., unusual login attempts, unauthorized access).
- Validate reported incidents from staff or external notifications.
- Classify incidents based on severity (e.g., Critical, High, Medium, Low).

Suggested Tools:

- Splunk Free or Wazuh SIEM (for log monitoring & event detection)
- Windows Defender Security Center (basic malware detection)
- Wireshark (for analyzing suspicious network traffic)

Phase 3: Containment

- Disconnect compromised systems from the network.

- Apply network segmentation to isolate affected areas.
- Disable compromised accounts and block malicious IP addresses.
- Deploy temporary security measures, such as restricting external access.

Suggested Tools:

- Active Directory Group Policies (to disable compromised accounts)
- Endpoint Isolation via CrowdStrike Falcon Free or Windows Defender ATP
- VLAN Segmentation using pfSense or Ubiquiti Networks

Phase 4: Eradication

- Perform malware removal using Endpoint Detection and Response (EDR) tools.
- Patch vulnerabilities identified during the investigation.
- Reconfigure security controls to close exploited gaps.
- Conduct forensic analysis to ensure all threats have been removed.

Suggested Tools:

- Malwarebytes or ClamAV (for malware scanning and removal)
- Microsoft Baseline Security Analyzer (MBSA) (to find system vulnerabilities)
- Sysinternals Suite (Process Explorer, Autoruns) (to detect hidden malware)

Phase 5: Recovery

- Restore systems from secure, verified backups.
- Test systems to confirm they are clean and functioning correctly.
- Monitor network traffic and logs for signs of reinfection or new threats.
- Notify stakeholders when systems are operational.

Suggested Tools:

- Acronis Cyber Backup or Veeam Backup & Replication (to restore affected systems)
- JumpCloud or Microsoft Intune (to reconfigure and secure endpoint devices)
- BitLocker (Windows) or VeraCrypt (to encrypt recovered data and prevent future exposure)

Phase 6: Post-Incident Activity

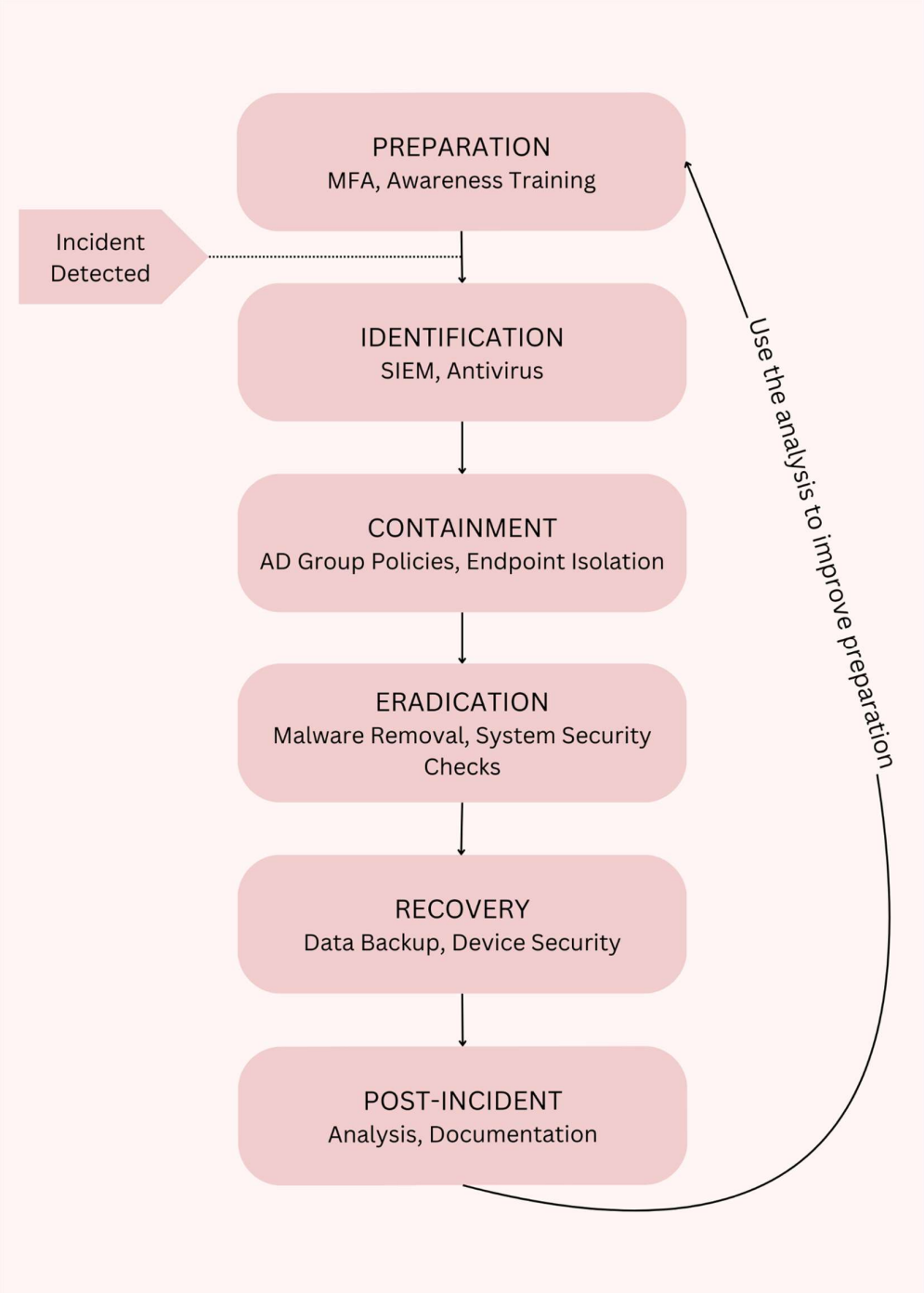
- Conduct a post-mortem review to identify root causes and lessons learned.
- Document the incident, response actions, and outcomes.
- Update security policies and refine the incident response plan.

- Provide refresher training to staff and IRT members.

Suggested Tools:

- Acronis Cyber Backup or Veeam Backup & Replication (to restore affected systems)
- JumpCloud or Microsoft Intune (to reconfigure and secure endpoint devices)
- BitLocker (Windows) or VeraCrypt (to encrypt recovered data and prevent future exposure)

Following flowchart contains phases and tools that can be used for each phase of the plan:



Contact Information

The department personnels can use these contacts in case of an incident:

Department Contacts

Role	Name	Title	Phone	Email

Incident Handler (Lead)	Jay Chhanang	Cybersecurity Officer	555-0101	j.chhanang@dbpd.gov
Incident Handler (Backup)	Mishika C.	IT Manager	555-0102	m.chhanang@dbpd.gov
Note-taker	Mark Taylor	Admin Assistant	555-0103	m.taylor@dbpd.gov
Communications	Sarah Lee	Communications Officer	555-0104	s.lee@dbpd.gov
Network	Linda B	Network Engineer	555-0105	l.bray@dbpd.gov
Server	Xytus Joseph	Server Specialist	555-0106	x.joseph@dbpd.gov
Legal	Ohm Trivedi	Legal Advisor	555-0107	o.trivedi@dbpd.gov
Executive	Jishant Acahrya	Chief of Police	555-0108	j.acharya@dbpd.gov

External Contacts

Role	Organization	Name	Title	Phone	Email
Network Security Vendor	TechSecure Solutions	Peter Clark	Support Lead	555-0201	p.clark@techsecure.com
Cyber Insurance Provider	SafeNet Insurance	Amanda White	Account Manager	555-0202	a.white@safenet.com
Legal Counsel	LegalEase Law Firm	Laura Green	Lawyer	555-0203	l.green@legalease.com
Ransomware Response Team	Encryptor Recovery Inc.	Rachel Adams	Recovery Manager	555-0204	r.adams@encryptor.com
Data Backup Vendor	CloudSafe Solutions	David Parker	Account Manager	555-0205	d.parker@cloudsafe.com
Card Payment System Vendor	SecurePay Ltd.	Karen Taylor	Support Lead	555-0206	k.taylor@securepay.com

So, to summarise, following technical controls should be used by the department to make sure it stays safe and unaffected by any incidents:

1. Controlling Access

- Two-Step Verification (MFA) – Extra login step for added security.
- Role-Based Access (RBAC) – Access only what is necessary.
- Admin Access Restrictions (PAM) – Limit critical system changes.
- Single Sign-On (SSO) – One login for multiple systems.
- Account Lockouts – Lock accounts after too many failed attempts.

2. Securing the Network

- Firewalls – Block harmful internet traffic.
- Intrusion Detection – Alerts for break-in attempts.
- Secure Remote Access (VPN) – Encrypt connections outside the station.
- Zero Trust Security – Verify every user and device.
- DDoS Protection – Prevent system slowdowns from fake traffic.
- Separate Networks – Keep police systems isolated from public access.
- Secure Wi-Fi – Strong passwords and encryption.

3. Protecting Devices

- Threat Detection Software (EDR) – Scan for and remove cyber threats.
- Approved Apps Only – Block unauthorized software.
- USB Restrictions – Prevent malware from external devices.
- Secure Mobile Devices – Manage and protect police phones.
- Encrypt Laptops & Hard Drives – Prevent unauthorized access.

4. Data Protection

- File Encryption – Protect sensitive case files.
- Automated Backups – Prevent data loss.
- Secure File Transfers – Use encrypted channels.
- Data Leak Monitoring – Detects unauthorized sharing.
- Secure Emails – Encrypted police communications.

5. Cloud Security

- Monitor Cloud Use – Track suspicious activity.
- Fix Security Gaps – Regularly review cloud settings.
- Secure Online Services – Require authentication.
- Detect Unusual Access – Alerts for unauthorized use.

6. Website & App Security

- Website Firewall (WAF) – Block hacking attempts.

- Vulnerability Scans – Detects weak points.
- Frequent Updates – Fix security flaws quickly.
- Developer Training – Ensure secure programming.

7. Threat Detection & Response

- Security Monitoring (SIEM) – Track system activity.
- Threat Intelligence Feeds – Stay updated on risks.
- Dark Web Monitoring – Detects leaked police data.
- User Activity Tracking – Find suspicious behavior.
- Forensic Tools – Investigate cyber breaches.

8. Physical Security

- Cameras & Access Control – Secure sensitive areas.
- Restricted Data Centers – Limit physical access.
- Security Training – Teach officers to spot threats.
- Emergency Response Plans – Prepare for cyber incidents.

9. Response & Recovery

- Incident Response Plan (IRP) – Clear steps for cyberattacks.
- Security Team (SOC) – Monitor and handle threats.
- Cyber Drills – Train staff on emergency procedures.
- Data Backup Plan – Restore lost files quickly.
- Cyber Insurance – Cover financial losses.

10. Audits & Compliance

- Regular Security Reviews – Ensure law enforcement standards.
- Penetration Testing – Ethical hacking to find weaknesses.
- Third-Party Security Checks – Vet external vendors.
- Log Monitoring – Track all system activity.

Glossary

- Incident Response Plan (IRP): A step-by-step guide that helps DBPD handle cyberattacks and security breaches quickly and effectively to prevent damage and recover safely.

- APT (Advanced Persistent Threat): A long-term, targeted cyberattack by a skilled hacker group (often backed by a government) that stealthily infiltrates networks to steal sensitive data.
  Example: APT29 (Cozy Bear), a Russian-backed hacking group that attacked U.S. law enforcement in 2021.
- Spear-Phishing: A trick email sent to specific people (like DBPD officers) that looks real but contains malware or fake login pages to steal passwords.
  Example: An email pretending to be from the Chief of Police asking you to "reset your password" but actually stealing your login details.
- Credential Theft: Hackers stealing usernames and passwords to access police databases, patrol systems, or digital evidence storage.
- Supply Chain Attack: Instead of hacking DBPD directly, attackers infect software vendors that DBPD trusts, allowing malware to enter police systems unnoticed.
  Example: A cybersecurity software update gets hacked, and DBPD installs the infected update unknowingly.
- Endpoint Detection & Response (EDR): A smart security system that monitors computers, patrol laptops, and devices for suspicious activities and stops threats before they spread.
- SIEM (Security Information and Event Management): A cybersecurity dashboard that collects, analyzes, and alerts DBPD cybersecurity officers about potential cyberattacks in real time.
- Network Isolation: Cutting off an infected computer or system from the rest of the police network to stop a virus or hacker from spreading further.
- Ransomware: A type of cyberattack where criminals lock DBPD's data with encryption and demand money ("ransom") to unlock it.
  Example: All police case files suddenly become unreadable, and a hacker demands $100,000 to restore them.
- Zero-Day Exploit: A security flaw in software that even the developer doesn't know about. Hackers find and use it before a fix is available.
- Forensics & Malware Analysis: A digital investigation to find out how hackers broke in, what damage they caused, and how to prevent future attacks.
- Dark Web Monitoring: Checking hidden parts of the internet to see if DBPD's stolen data or officer passwords are being sold by hackers.
- Multi-Factor Authentication (MFA): A security feature that requires two or more forms of verification to log in.
  Example: You enter your password AND a one-time code sent to your phone.
- Firewall & Intrusion Prevention System (IPS): A security filter that blocks dangerous websites, hackers, and malicious data from entering DBPD's network.

References

- Chapter 282 Section 318 - 2021 Florida Statutes - The Florida Senate. (n.d.). Retrieved from www.flsenate.gov website: https://www.flsenate.gov/Laws/Statutes/2021/282.318
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2022). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2
- CISA. (2022, May 9). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. Retrieved from Cybersecurity and Infrastructure Security Agency CISA website: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
- Fritsvold, E. (2019, May 10). The Cutting-Edge Technologies Transforming 21st Century Policing. Retrieved from University of San Diego website: https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/
- ISO), C. (2020, January). Criminal Justice Information Services (CJIS) Security Policy. Retrieved from Federal Bureau of Investigation website: https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view
- Swachchhanda Shrawan Poudel. (2023, October 26). Emerging Threat: APT-29 - The Not So Cozy Bear. Retrieved from Logpoint website: https://www.logpoint.com/en/blog/emerging-threats/apt29-cozy-bear/
- Team ZCySec. (n.d.). NIST Incident Response Plan | NIST SP 800-61 Security Incident Response Plan. Retrieved from Zcybersecurity website: https://zcybersecurity.com/nist-incident-response-plan-playbook/