Assignment 4: Cybersecurity Breach Event Response Plan

Team 6

Aydan Paul, Emma Lewis, TJ Fields, Toshan Misir

Table of Contents

Overview

Background

Loan Depot was founded in 2010 by Anthony Hsieh, who worked in the mortgage industry. The company was headquartered in Irvine, California, and licensed in every state, with branches across the US. From the beginning, Loan Depot has focused on retail mortgage lending and serving as a "non-bank" lender. They promote an effortless and straightforward mortgage experience, where customers are their sole priority.

Loan Depot has consistently maintained a digital-first approach when it comes to financing and lending to its customers. They integrate their use of the Mello software platform to enable direct-to-customer channel sales. This strategy allows the company to generate revenue through its home loans, servicing charges, and home equity products. At the end of 2023, Loan Depot reported revenue of $974 million, which was down from 2022. By quarter 2 of 2024, Loan Depot had seen significant improvements in its productivity cost, as evidenced by its reported revenue of $265 million.

Although Loan Depot saw significant improvements in its productivity costs between January 3rd and January 5th, the company faced a significant security breach in which an unauthorized third party accessed some of its systems, affecting approximately 17 million individuals. The company reported that data, including names, addresses, emails, phone numbers, social security numbers, financial account information, and dates of birth, were all compromised.

Breach

In early January 2024, Loan Depot experienced a ransomware and data theft attack. The company discovered unauthorized access to its network and responded by shutting down several internal systems to contain the intrusion. The APLHV/BlackCat ransomware group later claimed responsibility for the attack.

During the breach, attackers accessed and exfiltrated sensitive personal information (SPII) belonging to about 16.6 to 16.9 million customers. The compromise data included addresses, names, D.O.B, SSN, and in some cases financial account numbers. The attackers also encrypted data and systems, disrupting operations and temporarily preventing some customers from accessing online accounts and loan services.

Loan Depot notified federal and state regulators, filed SEC disclosure, and began notifying impacted individuals. The company offered affected customers' identity theft monitoring and credit protection services. In addition to customer impact, the incident resulted in operational disruptions, reputational damage, and millions of dollars in incident response and recovery costs.

The exact initial cause of the breach has not been publicly conformed, but the attack followed patterns commonly associated with the BlackCat ransomware group, which often uses credential compromise, phishing, or exploitation or remote access systems to gain entry.

Post-Breach Transformation Goals

Following the breach, Loan Depot strategized and implemented a comprehensive NIST Cyber security Framework following the 2.0 standard. The new framework will emphasize rapid response, regulatory compliance, and transparency between roles in the business and technology sectors.

Main goals include:

- Setting a standard breach severity zone model to assimilate reporting and recovery procedures for breach incidents.
- Mapping all cybersecurity controls to financial and cybersecurity regulations and acts.
- Enhancing governance oversight to establish clear lines of accountability and roles for all acting players.
- Building and incorporating regular testing and audits to help mitigate future risk and financial loss.

Breach Severity Zone Model

Zone	Severity Level
5 - Critical	Enterprise-wide Ransomware or Major Breach
4 – High	Significant System or Data Breach
3 – Moderate	Isolated Data or Access Breach
2 – Low	Low Impact Incident
1 – Minor	Minor Security Event
0 – Negligible	Routine Technical Issues or False Alarms.

Governance

Organizational Context (GV.OC): Loan Depot operates as a lender but is classified as a non-bank lender. They are licensed to practice across all 50 states. Due to the vast majority of clientele, Loan Depot manages a large volume of customer financial data through software platforms. It relies heavily on its cloud software and third-party vendors for day-to-day operations. Due to this integration, cybersecurity for consumer data, cloud platforms, and vendor connections is highly vital. Due to a 2024 ransomware attack that affected almost 17 million customers, Loan Depot realized its incident response framework needed vital improvements, shifting from a less technical security response to a more strategic business mitigation response. The shift will include integrating cybersecurity measures with mitigation for everyday operations, risk and financial management, and strategic operations. With an emphasis on accountability, visibility, and communication across all levels, the board of directors will handle data protection and ensure it aligns with all relevant business regulations.

Risk Management Strategy (GV.RM): Loan Depot will focus on prioritizing the alignment of its strategy with business regulatory compliance, prevention, and mitigation tactics. It will map all frameworks within the NIST 2.0 to align with all financial responsibilities under the Gramm-Leach-Bliley Act and FTC safeguards, along with all cybersecurity compliance requirements under the SEC, SOX, and USA Patriot Act. To ensure all complaints are addressed, quarterly risk assessments will be conducted to evaluate any vulnerabilities and threats that are flagged. Setting up an insurance plan to offset potential breaches and financial losses. This new strategy displays Loan Depots' risk transparency and their ability to meet all compliance needs from regulators, customers, and shareholders.

Roles, Responsibilities, and Authorities (GV.RR): Restructuring Loan Depot's leadership ladder to strengthen authority for cybersecurity oversight across all organizational levels, rather than solely relying on the IT department for responsibility and ownership.

- **Chief Information Security Officer (CISO):** To build a more strategic cybersecurity measure, the CISO will directly report to various teams to have a clear line of communication. The CISO, depending on the breach of impact, will communicate orders with the Board of Directors, the CIO, and the incident Response Team. This collaboration creates greater transparency and tactical alignment between business and cybersecurity operations. Overall, it enhances risk visibility and facilitates faster decision-making, establishing a clear line of accountability for all parties involved.
- **Chief Risk Officer (CRO):** Works with the CISO to integrate the cybersecurity risk measures with financial risks within the corporation's risk management framework. This integration helps measure all

risks beyond technological involvement that are covered, mitigated, and prioritized within the set frameworks. Strengthening this relationship allows the company to have a clear line of regulatory compliance under the Gramm-Leach-Bliley Act.

- **Incident Response Teams (IRT):** This team is a group of leaders from the HR, Legal, and IT teams who communicate and create clear actions in response to incidents. Their primary goal is to contain incidents rapidly while communicating with one another to ensure compliance with all regulatory requirements. Complying with all regulations enables them to restore normal operating functions with ease.
- **Employees:** Including the executive team and board, all employees a part of the organization will complete annual cybersecurity training that will include practicing breach simulations and any possible cyberattacks that could occur during operations. These periodic refreshers will be tailored to each employee's specific role and risk exposure. Higher risk department members suck as executives and IT, will participate is quarterly simulation exercises to reinstate response readiness and decision making.

Policy, Processes, and Procedures (GV.PO): Loan Depot will adhere to and align all its regulatory compliance requirements under the Securities and Exchange Commission (SEC) and the Sarbanes-Oxley Act (SOX). Loan Depot will ensure there is clear accountability across all organizational levels and will have strong internal controls that will provide accurate and communicated incident information. Along with protecting customers' financial data and security, Loan Depot will align its privacy and cybersecurity policies to meet the requirements of the FTC safeguard rules and the GLBA. They will focus on not collecting **non-public** customer data or sharing it in any manner. Loan Depot will adhere strictly to compliance requirements under the USA Patriot Act. All policies will ensure that Loan Depot operates legally and follow all regulatory compliance frameworks to protect and maintain the trust of customers and shareholders. To maintain these compliances, there will be semi-annual audit reviews of all policies led by the CISO and CRO, to ensure all data meets the cybersecurity requirements.

Oversight (GV.OV): Oversight will extend beyond the executive level and focus on all employees, adhering to continuous monitoring, compliance, and transparent oversight of the NIST 2.0 framework. To measure the effectiveness of the framework, Loan Depot will conduct audits semiannually. Following these audits, the incident response teams will perform penetration testing with practice breach simulations of all potential cyberattacks that the company could face, to help measure the meantime to detect, respond to, and recover. Results from these activities will be reviewed by executive members to correct any actions and controls. These enhanced oversights will demonstrate Loan Depot's visible accountability following the 2024 breach.

Cybersecurity Supply Chain Risk Management (GV.SC): Loan Depot relies heavily on third-party vendors to assist with its day-to-day operations. Due to the close relationship and trust between parties, Loan Depot has established a clear and separate third-party risk management framework that outlines all potential supply chain vulnerabilities and mitigation processes. Vendors are expected to participate in regular security assessments that include independent audits, penetration testing (if their contractually feasible), and certifications that will be reviewed by Loan Depots incident response team. Loan Depot will continuously monitor the vendors' systems through AI tools to track any potential red flags and performance issues. Loan Depot will ensure that each vendor it works with maintains cybersecurity certifications and includes a 24-hour breach notification clause, or the closest legally equivalent permissible agreement in their contracts.

Identify

When an incident becomes known, it will have an impact on the response process and the urgency correlated with it. Examples of how Loan Depot becomes aware of an attack or flag in the AI monitoring systems include:

1. **Internal Detection:** The Security Operations Center (SOC) or AI monitoring systems detects unauthorized access, abnormal activity, or data exfiltration within the network, application, or cloud infrastructure

2. **Vendor Notification:** A third-party vendor or partner notified Loan Depot of a cybersecurity threat or alert affecting shared data.
3. **Customer or Constituent Report:** A partner, customer, or employee reports suspicious behavior, such as unauthorized account access, irregular loan application activity, or phishing attempts.
4. **External Disclosure:** Loan Depot becomes aware of an incident through law enforcement, industry threat intelligence feeds, or public reports in the media.

Common Categories of Cyber Incidents

Incident Type	Description	Scope of Impact
Ransomware or Data Encryption Attack	Attackers encrypt or disable key systems, blocking access to loan data, emails, or servicing platforms until ransom is paid.	High
Business Email Compromise	Criminals impersonate executives or vendors to redirect wire transfers, invoices, or payroll payments.	High
Account Takeover	Attackers gain control of borrower or employee accounts to steal funds, alter loan records, or access PII.	High
Third-Party or Vendor Breach	A partner system is compromised, exposing Loan Depot data.	High
Payment System Compromise	Unauthorized access or manipulation of payment, ACH, or escrow systems used to reroute or steal funds.	High
API Exploitation	Attackers exploit weak or exposed APIs to pull data, alter loan records, or bypass authentication.	Medium
Cloud Configuration Exposure	Misconfigured cloud storage makes internal data publicly accessible or vulnerable.	Medium
Insider Data Misuse	Employees or contractors intentionally or accidentally access, copy, or share sensitive data.	Medium
Synthetic Identity or Fraudulent Loan Application	Use of fake or stolen personal data to apply for loans or create false borrower profiles.	Medium
Distributed Denial of Service (DDoS) Attack	High volumes of web traffic, temporarily disrupt public portals, calculators, or customer tools.	Low
Minor Policy Violations	Employees install unauthorized software, use work systems for personal purposes, or ignore cybersecurity policy.	Low

Incident Impact Definitions

Security Objective	Description	Low Impact	Medium Impact	High Impact
Confidentiality	Protect borrower, employee, or corporate information from unauthorized access, use, or disclosure. Includes safeguards for PII, and financial records.	Limited internal exposure. Quickly contained with no external impact.	Breach affects a business unit, vendor, or small customer subset. Possible limited external exposure.	Large scale data breach involving PII or financial data with external visibility or regulatory implications.
Integrity	Ensuring accuracy, consistency, and trust of data across all systems. Prevent unauthorized changes or destruction of records.	Minor non malicious errors affecting isolated records; easily corrected.	Improper modification of multiple records or systems causing business disruption.	Widespread manipulation or destruction of borrower or loan data requiring full system disclosure.
Availability	Maintaining reliable, timely access to the system, applications, and data required for daily operations or customer transactions.	Short outage (under 2 hours) affecting limited users or one application.	Prolonged disruption (2-12 hours) of key systems such as servicing platforms.	Major outages or denials or service lasting over a day, halting business activities.

Incident Severity & Response Classification

Severity Level	Typical Incident Characteristics	Incident Response	Activate Incident Response Team?
5 - Critical	Major, ongoing attack that shuts down or severely disrupts systems across the whole company. Involves data theft and exposure.	Immediate activation of the Incident Response Team and IT Security. The CISO leads response coordination and briefs the Cybersecurity and Oversight Committee. Legal counsel, corporate communications, forensics, and law enforcement are engaged.	Full team is active.
4 – High	Significant incident affecting a department or multiple users, involving unauthorized access or potential exposure of sensitive data.	Response directed by IT Security under CISO oversight. IRT informed and engaged as needed. Legal counsel notified if PII data is involved. Updated provided to the Cybersecurity and Oversight Committee.	Full team is informed and advised.
3 – Moderate	Isolated event affecting one user or system,	Response coordinated by IT Security with notification to the CISO and IRT members.	Primary team informed.

	involving access to sensitive data.	Legal counsel involved is PII confirmed. Root cause review documented and shared with the oversight team.	
2 – Low	Limited impact event affecting small groups, with no sensitive data exposed.	Managed by IT Security. CISO is notified, and the incident is documented, and corrective action is taken.	Primary team informed.
1 – Minor	Minor events affecting a single user or device. No sensitive data is exposed.	Handled by IT Support. The CISO may be notified if the issue continuously repeats.	No.
0 – Negligible	Routine technical issues or false alarms.	Managed through standard IT support channels.	No.

Protect

Identity Management, Authentication, and Access Control (PR.AA):

LoanDepot will centralize identity and access management on a single authoritative identity platform so that all employee, contractor, and approved third-party accounts that can reach loan-origination, servicing, Mello, or Windows/Active Directory resources are created, changed, and removed in one place. This reduces "shadow" or duplicate accounts and makes it easier to see exactly who has access to what. Multifactor authentication (MFA) will be enforced for all accounts, with stronger or step-up MFA (such as phishing-resistant methods or additional verification when risk is high) applied to administrative roles and systems that contain sensitive customer information like Social Security numbers and bank details. Access will be based on role-based access control (RBAC) and least-privilege principles so that users can only view or modify the information they need for their job. Privileged accounts (for admins and system owners) will be managed through a privileged access management (PAM) solution that issues time-limited, just-in-time access and records administrative sessions for later forensic review if anything suspicious happens. HR "joiner/mover/leaver" events will trigger automatic access provisioning and deprovisioning on the same day, preventing old accounts from remaining active after a person changes roles or leaves the company. Network access to internal applications will align with zero-trust principles—continuous authentication, continuous authorization, device health checks, and detailed logging of each access decision. Identity logs, VPN logs, and application-access logs will all be forwarded into the central security monitoring and SIEM capabilities, so security analysts can correlate identity activity with other events during threat hunting and incident response.

Awareness and Training (PR.AT):

All personnel, including executives, managers, loan officers, and support staff, will receive recurring cybersecurity awareness training that reflects the current ransomware and data-theft tactics being used against financial institutions. This will include examples of real-world attacks on the industry, how attackers typically move from an initial phishing email to data exfiltration, and what "red flags" employees should look for in emails, links, and authentication prompts. Employees in higher-risk roles—such as IT administration, help desk, loan operations, finance, and anyone with elevated system access will receive additional, shorter micro-

trainings and more frequent simulated phishing exercises. These will focus specifically on credential-stealing emails, social engineering tactics, reporting suspicious messages, and proper handling and storage of Gramm-Leach-Bliley Act (GLBA)–protected customer data. New personnel must complete baseline cybersecurity and data-protection training before their production access is activated, so there is no period where untrained users are operating in sensitive systems. Training completion, phishing-test performance, and required retraining will be tracked and reported as part of security-governance metrics to senior leadership and the board. This demonstrates that LoanDepot is taking concrete corrective steps after the 2024 breach and is building a culture where cybersecurity is treated as part of everyone's job, not just an IT problem.

Data Security (PR.DS):

Customer information identified in the 2024 incident, including names, addresses, emails, phone numbers, Social Security numbers, dates of birth, and financial account information will be formally classified as "sensitive" or "GLBA-protected" data in LoanDepot's data inventory and data-classification policy. Systems that store, process, or transmit this information will use strong encryption for data at rest (such as full-disk or database encryption) and TLS for data in transit so that intercepted traffic cannot be read. Data loss prevention (DLP) controls will be deployed on endpoints, email, and sanctioned cloud-storage platforms to detect or block unusual or large transfers of sensitive data to external destinations (for example, large customer-data exports being emailed to personal accounts). Alerts from DLP will flow into the security operations function for triage and investigation. Non-production environments (such as test and development) will use masked, tokenized, or synthetic data to significantly reduce the impact if an attacker gains unauthorized access to those systems. Backup copies of critical data will be stored in immutable, access-controlled locations that require MFA and are logically separated from daily user accounts and administrative credentials, making it much harder for ransomware operators to tamper with or delete backups. Data-retention schedules and secure-disposal rules will be enforced technically and operationally so that LoanDepot does not keep sensitive to customer data longer than regulatory or business requirements. Reducing the "data footprint" directly lowers the amount of information that could be exposed if an attacker gets in again.

Platform Security (PR.PS):

Internet-facing and customer-facing platforms that support loan origination, servicing, Mello, and other digital channels will be hardened according to recognized baselines (for example, NIST, CIS Benchmarks, or vendor hardening guides). Systems will be patched on a defined schedule, with emergency or out-of-band patching for vulnerabilities that are being actively exploited in financial services or that enable remote code execution. Endpoint detection and response (EDR) tools will be deployed on servers, desktops, and cloud workloads to provide real-time visibility into suspicious behaviors such as lateral movement, credential dumping, abnormal process execution, and encryption patterns seen in ransomware attacks. Public web applications and APIs will sit behind a web application firewall (WAF) or API gateway configured to detect and block common attack patterns like SQL injection, cross-site scripting, and authentication abuse, reducing the risk that these systems serve as an initial entry point. Periodic penetration tests and controlled breach simulations (red-team or purple-team exercises) will validate that network segmentation and security controls are working—for example, that a compromised user workstation cannot directly access domain controllers, databases containing sensitive customer information, or backup management consoles. Administrative and management interfaces (for hypervisors, databases, security tools, and cloud consoles) will be placed on isolated management networks, restricted to specific administrator devices, and protected with MFA and strong logging. These controls collectively make it harder for attackers to gain a foothold and to move laterally to "crown jewel" systems.

Technology Infrastructure Resilience (PR.IR):

Core identity, logging, loan servicing, and customer account systems will maintain tiered and geographically separated backups so that LoanDepot can meet business-defined recovery time objectives (RTOs) and recovery point objectives (RPOs) even if primary infrastructure is encrypted, destroyed, or taken offline during incident containment. Network segmentation will be strengthened not just at a high level (separating environments) but also within data centers and cloud networks to limit east-west movement and reduce the blast radius of any future intrusion. Critical services such as directory services, VPN, SIEM, identity providers, and backup/recovery platforms will be deployed in highly available configurations across at least two data centers or cloud regions. Documented and regularly tested failover procedures will make sure that staff know how to operate in a degraded or disaster mode. Regular recovery and restoration exercises where teams rebuild systems from clean images and restore data from backups will be scheduled after audits and major changes to confirm that systems can be recovered reliably and that security controls like logging, MFA, and monitoring are re-established as part of the rebuild. Third-party service providers that support customer-facing platforms, payment processing, or monitoring functions will be required through contracts and due-diligence processes to meet comparable resilience and recovery standards. Together, these measures ensure that even if another serious incident occurs, LoanDepot can contain damage, restore operations, and protect customer data more quickly and confidently than it did in 2024.

Detect

Continuous Monitoring (DE.CM): Loan Depot will retain and store public personal information and should have a system designed to assess, identify, and manage possible risks that become evident. They will also use a third-party monitoring system for further monitoring of adverse events. AI monitoring platforms use real-time data collection to automatically detect adverse events. Through using root cause analysis, they identify the main incident that triggered the chain of events. They will also establish a cybersecurity and oversight committee that works closely with the Chief Information Security Officer to manage and monitor software, hold annual cybersecurity training for all employees, and hold quarterly penetration testing.

Information security teams, alongside the CISO, physically monitor machines, systems, accounts, and applications to prevent or mitigate data loss, theft, misuse, access, or other security incidents and vulnerabilities that could attack the system. Access to their systems, electronic and physical, should only be accessed and handled by high-ranking managers and professionals. Loan Depot will also monitor all employees, regardless of their security clearance or position. They will build teams dedicated to tracking personnel activity, like the cybersecurity and oversight committee, to track logins at strange hours, large data downloads, or access files that are unauthorized.

Loan Depot must ensure they maintain data user agreements to regulate how third-party partners use data. They will make sure vendors aren't misusing data and must make sure their security teams are overseeing said vendors. Loan Depot audits their third-party vendors, suppliers, and contractors. Third party vendors also sign confidentiality agreements and yearly contracts to protect sensitive data shared with them. They need to make sure there are policies backing up the vendors; including lawyers, security teams, IT teams, and other teams that will make sure the company is protected. Loan Depot has tools to watch its servers, applications, clouds, and data all the time to ensure attacks are confirmed quickly and efficiently. The cyber security teams receive all information that looks suspicious or is flagged by the system and investigate further.

Adverse Event Analysis (DE.AE): When suspicious activity is flagged, Loan Depot conducts an initial detailed analysis before escalation occurs. Analysts examine logs and network traffic to determine whether the flag is a false alarm or a serious threat. Teams document their findings, classify the event type, and determine whether further investigation is necessary. If suspicious activity is flagged within the system, the Security Operations System begins to collect logs from affected servers, systems, and cloud environments to identify the root

cause and develop a timeline. Analysts use tools such as SIEM to determine whether this activity was the result of a technical malfunction, user error, or malicious intrusion. This process happens immediately, within minutes of the alert. SOC analysts will gather data from multiple sources including endpoint logs, network traffic, and third-party reports to determine whether the alert is adverse. CISO's cyber security and oversight committee launches a formal impact assessment determining which systems were accessed, what data types were exposed (financial data, sensitive customer data, etc.), and how far the breach may have spread. This process must be handled within the three-to-six-hour range.

Once the activity is confirmed harmful, the SOC reports the findings to authorized leadership, including the CISO and other high-level managers, and other branches of the business. For the next two hours, data and findings are uploaded to incident management and response tools to coordinate containment actions. Access to these reports is restricted to only authorized personnel. The cyber security team then cross references the findings with other current cyber threat intelligence feeds to determine any relationships with other breaches. This includes researching ransomware groups' known tactics, techniques, and procedures. Within hours 18-24, and analysis confirms unauthorized access and potential data exfiltration; the CISO formally declares a cybersecurity incident to senior executives, legal teams (internal and external), and law enforcement. Since the breach involves customer sensitive data, the public must be notified about the attack in a press release, Form 8-K (since it is a publicly traded company), 10Q, or SEC filing.

Respond

Incident Management (RS.MA): Once an incident has occurred, the Loan Depot should activate a Cyber Incident Response Team (CIRT) and place the organization under an incident command structure to centralize decision making. They should isolate all affected systems and networks segments to prevent any lateral movement and further data extraction. Once all affected systems are isolated, they should engage a third-party digital forensics and incident response team to preserve any evidence and ensure an unbiased analysis. Lastly, all executives, legal, HR, risk management, and public relations should be notified to ensure coordinated actions. The primary goal is to contain the threat, protect all evidence, and ensure all decisions are unified.

Incident Analysis (RS.AN): For the incident analysis, a deep forensic review needs to be conducted. Find out what is the initial vector of compromise (Stolen credentials, exploited vulnerabilities). Find out what privilege escalation pathways the attackers used also the systems and data that have been accessed, exfiltrated, and encrypted. Once that is known, validate all SPII and PII that were exposed, such as SSN, account details, D.O.B, and address. Lastly, find out the scope and timeline of the attacker and whether that maintained persistence via hidden accounts, scripts or scheduled tasks.

Incident Response Reporting and Communication (RS.CO): Loan Depot will need to draft regulator ready documents including SEC 8-k, Form 10-Q/10-K, CFPB and FTC, FFIEC. Before any public disclosure is made, the cybersecurity team must provide structured internal situation report to executives and legal counsel on a periodic basis. Once the scope of the incident and the affected materials are confirmed, the company had 4 business days to formally submit a report to the SEC 8-k describing the incident's nature, scope and impact, and the ongoing remediation efforts. Disclosure requirements may vary from state to state, depending on where the company operates and where the affected customers are located. LoanDepot therefore must ensure compliance with each applicable state breach-notification statute, some of which have deadlines shorter than federal requirements.

Incident Mitigation (RS.MI): For incident mitigation, Loan Depot should rebuild affected systems from a known clean baseline when forensic analysis indicates that backups may contain contaminated artifacts. A structured credential-rotation process should follow, covering user accounts, privileged accounts, and service accounts, based on the level of exposure identified. After credentials are rotated, identity and access management controls can be strengthened by enforcing MFA for administrative access, reviewing conditional access rules, and tightening authentication requirements where gaps were observed. Systems identified as vulnerable or misconfigured during the investigation should be patched, updated, or reconfigured to reduce the likelihood of

reinfection. Containment validation testing should be performed to help confirm attacker expulsion and ensure no persistence mechanisms remain. To further reduce residual risk, the organization may conduct targeted threat-hunting across the environment, expand EDR (Endpoint Detection and Response)/XDR (Extended Detection and Response) visibility, and review network segmentation to limit lateral movement. Monitoring authentication logs for anomalous activity after credential changes, validating the integrity and isolation of backup processes, reassessing, vendor and third-party access pathways, and conducting a structured lessons-learned review can help identify systemic weaknesses and lower the chances of similar incident occurring in the future.

Recover

Incident Recovery Plan Execution (RC.RE): For recovery execution, LoanDepot should follow an organized, phased sequence of actions that align technical restoration with business continuity priorities. Compromised systems may be built first from verified clean images, beginning with core infrastructure components such as identity services, directory systems, and network controls. Once foundational services are stable, application layers and business platforms can be restored in structured groupings. After system rebuilds, the organization should validate application and data integrity using hashing verification, log correlation, and anomaly scanning techniques to detect any residual compromise. Rather than bringing all systems online simultaneously, LoanDepot should reactivate services in controlled phases. Initial phases may focus on mission critical functions including loan servicing platforms, payment processing systems, and customer facing account portals to maintain operational continuity and minimize revenue loss. Subsequent phases may include supporting applications, internal administrative systems, and lower priority workloads once critical services have been confirmed to be stable. Throughout this process, the business continuity plan should directly align with the technical restoration order, ensuring that the timing of hardware and software reactivation supports essential business functions and avoids operational disruption.

Incident Recovery Communication (RC.CO): For recovery communication forensics teams need to present final executive forensics report which summarizes the root cause, attack vector, how the incident was mitigated and remediation steps, and the scope of data exposure. Strategic risk and compliance recommendations need to be provided to the Board of Directors. Also support long-term customer assurance messaging to help with brand reputation and strengthen controls.

Sources

Center for Security and Privacy Controls. (n.d.). *ID.RA-10 – Critical suppliers are assessed prior to acquisition (NIST Cybersecurity Framework v2.0).* CSF.Tools. https://csf.tools/reference/nist-cybersecurity-framework/v2-0/id/id-ra/id-ra-10/

Dynatrace. (n.d.). *loanDepot customer story.* Dynatrace. https://www.dynatrace.com/customers/loandepot/

International Journal of Innovative Science and Research Technology. (2025, April). *Cybersecurity GRC framework analysis report [PDF].* IJISRT. https://ijisrt.com/assets/upload/files/IJISRT25APR1107.pdf

Jewish Federations of North America. (n.d.). *Cyber-security incident response template.* https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf

loanDepot, Inc. (n.d.). *Privacy policy.* loanDepot, Inc. https://www.loandepot.com/privacypolicy

loanDepot, Inc. (2025, March 13). *Form 10-K: Cybersecurity GRC – Board Cybersecurity.* loanDepot, Inc. https://www.loandepot.com/

Red Canary. (n.d.). *Incident response and readiness guide.* https://resource.redcanary.com/rs/003-YRU-314/images/IncidentResponse-and-Readiness-Guide__RedCanary.pdf