Breach Response Planning in the Privacy Age
An Overview

Chris Courchesne & Matt Ford
Mandiant Consulting
Agenda

- Privacy Laws’ Impact to Incident Response
- Incident Response Planning
  - Preparation
  - Identification
  - Investigation
  - Remediation
  - Post Incident
- Key Takeaways
Privacy Law Impact to Incident Response
The Clock is Ticking…

- In a data breach situation, privacy laws may require different time frames for notifying the respective authority
- With the General Data Protection Regulation (GDPR) at 72 hours, many companies use that window as a baseline to:
  - Confirm that there has been an incident with privacy implications
  - Scope the incident
  - Draft containment and remediation plans
  - Inform regulators and individuals of the breach
What Effective IR Planning Can Provide

- The organization can reduce the risk associated with a data breach and meet the 72-hour reporting requirements with the fundamentals:
  - Actively Monitor Data Access – Answer the question of whether the data has actually been accessed, and if the access is truly suspicious in nature
  - Perform a Complete Incident Response – Document the facts relating to the breach:
    - The nature of the breach
    - Data and number of subjects affected
    - The likely impact and consequences of the breach
    - The measures taken or proposed by the organization to remediate the breach
Incident Response Lifecycle

- **Preparation**: Establishing and training of key resources, acquiring necessary tools, and assessing risks
- **Identification**: Identifying potentially adverse events and assigning an initial severity rating and category
- **Investigation**: Analyzing systems and information to determine the facts of a security incident
- **Remediation**: Planning and executing activities to contain and eradicate the threat and recover from the incident
- **Post-incident**: Assessing and documenting lessons learned to enhance capabilities to prevent, detect, and respond to incidents
Preparation
Governance Preparation

- Define a Crisis Management Team with oversight of cybersecurity incidents
- Identify relevant third parties to include in the response process:
  - External Counsel
  - Cyber Insurance
  - Forensic Investigators
  - Public Relations
  - Regulators
  - Law Enforcement
- Develop a Communication Plan with notification requirements and templates for both internal and external parties
Incident Response Plan

- Defines events and incidents
- Details relevant types of incident by category
- Defines incident severity levels
- Assigns roles and responsibilities
- Communications planning for both internal and external audiences
IRP Questions to Answer

- Who will take ownership of the breach?
- Who is the key decision-maker at each stage?
- How do you coordinate between stakeholders?
- Are there different legal / regulatory obligations?
- Are there different priorities for resolution? Who sets those?
Asset Inventories

- Critical assets are inventoried and system details exist in a centrally accessible location
- A robust asset inventory is maintained with detailed information to quickly determine if security incidents have privacy implications
- Each asset should have the following documented:
  - Business and IT Owners
  - Business function the asset supports
  - Physical and logical location
  - Operating systems, configuration information, and installed applications
  - Supported data types
Data Protection Controls

- Implement data protection controls to minimize the risk of data exposure:
  - Encryption defined by state (i.e., Data-at-rest, data-in-transit, data-in-use)

- Establish Data Retention and Destruction standards:
  - Data should not be kept longer than is necessary for that purpose
  - Archive or delete data that is no longer required
Identity and Access Management

- Multi-factor authentication (MFA) for remote access and critical systems
- Use role-based access control and “least privilege” for access provisioning
- Users are not local administrators on their system
- Remove shared accounts from the environment
- Utilize a Privileged Access Management (PAM) solution for privileged accounts and password resets after use
TTX Scenarios to Test Processes

- Customer Data Breach
  - Compromised Web Server
  - Insider Access
  - Extortion
  - Ransomware

- Consider privacy implications during the exercise
- Create a mock timer for reporting requirements
- Ensure that TTXs are performed on at least an annual basis
Visibility into the Threats

- Preventative technologies are valuable log sources for event-based monitoring:
  - Endpoint Detection and Response (EDR)
  - Web proxy
  - Data Loss Prevention (DLP)
- Wherever possible, expand these technologies to cloud and virtual environments
- Perform SSL decryption and inspection at egress
- Correlate relevant sources within a Security Information and Event Monitoring (SIEM) solution with Threat Detection Use Cases
Define a log source retention standard

Reduce time required to extract log sources

Define process to share log files with investigators

An insufficient retention period may lead to an incomplete investigation
Threat Detection Use Case Application

- **Initial Recon**
  - Open source intelligence gathering
  - Network and application reconnaissance
  - Remote access identification

- **Initial Compromise**
  - Social engineering
  - Internet-based attacks
  - Leverage service provider

- **Establish Foothold**
  - Backdoors
  - Remote access subversion

- **Escalate Privileges**
  - Credential harvesting
  - Password cracking
  - “Pass-the-hash”

- **Maintain Presence**
  - Command and control
  - Remote access subversion
  - Account abuse

- **Move Laterally**
  - Remote command execution
  - Remote administration

- **Internal Recon**
  - Critical system identification
  - System enumeration
  - Account and password enumeration

- **Complete Mission**
  - Staging servers
  - Data consolidation
  - Data theft
Cyber Threat Intelligence

- Evidence-based insights into adversary motives and capabilities
- Focus on events or trends to facilitate decision-making

- Utilize knowledge about threats and attacker Tactics, Techniques and Procedures (TTPs) to inform monitoring and risk management strategies
Operationalizing Threat Intelligence

- Intelligence drives operational processes:
  - Monitoring strategies (e.g., Threat Detection Use Cases)
  - Prioritizing threats (e.g., Threat Modeling)
- Intelligence is regularly communicated across the organization during and after response efforts
- Intelligence is used to analyze enterprise architecture’s exposure to threats (i.e., Threat Modeling)
- Integrate intelligence feeds with existing security monitoring solutions
Proactive Threat Hunting

- Patrolling the network for relevant Indicators of Compromise (IOCs)
- Mining historical data for threats and trends
- Successful hunting provides new IOCs which can be integrated into a SIEM
- Post-incident, hunting assists in ensuring remediation and eradication activities were successful
Investigation
Incident Response Playbooks

- Standardize response processes and communications for SOC personnel and MSSP
- Procedures to identify, investigate, and remediate to specific incident categories
- Detail when handoffs between teams should occur
- Include notification procedures to stakeholders
- Include follow-up procedures and activities
Communications Tools

- Up-to-date contact lists for all personnel and backups
- War room for in-person discussions
- Incident bridges for executive and technical teams
- Chat groups for technical teams
- Case Management System to orchestrate and document response efforts
- Additional Out-of-band communications
- Considerations for handoffs between geographic locations
An Escalation Matrix should define the following by incident category and severity:

- Internal and external stakeholders with documented SLAs
- Defines liaisons and points of contact for third parties
- Notification protocols with communication mechanisms
- Update frequencies
Forensic Capabilities

- Forensic capabilities either in-house or from a third-party such as Mandiant
- In-house considerations:
  - Available toolsets (disk & network forensics, live response, malware analysis)
  - How many resources are in place? What level of training do they have?
  - What scale and complexity of incidents can in-house resources manage?
- Third-party considerations:
  - Defined SLAs for engagement
  - Established liaisons and points of contact
  - Engagement through external counsel
Many investigations require deployment of an Endpoint Detection & Response (EDR) tool for visibility to:

- Sweep multiple endpoints for Indicators of Compromise
- Perform remote forensic analysis
- Contain compromised devices

Is an EDR currently deployed in the environment? If not:

- Has the agent been tested on all operating systems & images?
- Can we quickly deploy EDR through a systems management tool?
- Will the deployment coverage of all network segments? Remote offices?
Remediation
Timing Containment & Remediation

Contain & Remediate in the Strike Zone
- Thorough understanding of the extent of the compromise
- Can reliably detect the attackers’ malware and tools

TOO EARLY
- Extent of compromise is unknown
- Attacker active during remediation event

TOO LATE
- Attackers may change their TTPs or become inactive
- Lack of activity increases difficulty to investigate

STRIKE ZONE
- Need to start cycle again
- Too Early
- Too Late

Knowledge of Attack vs. Time
Establish containment process with pre-approved responses for:

- Individual systems
- Business-critical systems
- Multiple systems

Establish containment process for all accounts types:

- Individual users (including VIPs)
- Administrators
- Service accounts
Remediation

- Specific remediation strategies should be developed for:
  - Restoring from backups
  - Reimaging systems
  - Password resets
  - Performing and verifying relevant patching
  - Performing IOC sweeps to verify no additional evidence of malicious activity exists
Post Incident
Enhanced Monitoring

- Perform additional monitor impacted systems and accounts
  - Increase operating system and application logging
  - Monitor compromised accounts for abnormal activity
- Systems which were hardened but not rebuilt may pose additional risk
After Action Reporting

- Identify areas requiring procedural or technical improvement
- Identify training opportunities
- Facilitate better coordination and communication between stakeholders
- Processes should be routinely reviewed and updated
- Develop an employee feedback loop to update processes
Drain CVR: Dwell Time and Containment Time

\[ f ((D + R + A + I + N) + (C + V + R)) \]
## Metrics and Reporting

<table>
<thead>
<tr>
<th>Category</th>
<th>Measurement</th>
<th>What can we learn by measuring it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>Time from initial entry into the system/network to detection</td>
<td>Measures the effectiveness of detection systems and capabilities</td>
</tr>
<tr>
<td>Review</td>
<td>Time from detection to analyst to review the incident</td>
<td>Determines if staffing level is properly sized</td>
</tr>
<tr>
<td>Analyze</td>
<td>Time to analyze the incident</td>
<td>Determines if the organization has the right expertise and tools and if the right escalation occurs</td>
</tr>
<tr>
<td>Identify</td>
<td>Time to identify the affected assets, locations, and owner</td>
<td>Measures the effectiveness of asset inventory</td>
</tr>
<tr>
<td>Notify</td>
<td>Time to successfully notify appropriate contacts</td>
<td>Measures the effectiveness of contact database and Communication Plan</td>
</tr>
<tr>
<td>Collect</td>
<td>Time to collect live response data</td>
<td>Determines whether or not the right tools are deployed to assist in collection</td>
</tr>
<tr>
<td>Validate</td>
<td>Time to validate intrusion based on collected data</td>
<td>Determines whether or not the right skill sets are in place at each level</td>
</tr>
<tr>
<td>React</td>
<td>Time to react (contain, remove, etc.)</td>
<td>Determines whether or not there is the right definition of remediation, and if it is applied consistently</td>
</tr>
</tbody>
</table>
Key Takeaways
Key Takeaways

- In the new age of privacy laws, incident response can be a race against the clock requiring new capabilities to be developed and maintained.

- **Preparation**: Defining processes, roles & responsibilities, and implementing technical controls support prevention, detection, and response efficiency.

- **Identification**: Rapid detection of potential incidents and will limit the scope of security and privacy impact.

- **Investigation**: Processes and capabilities will allow teams to quickly gather and share information to fully scope the incident.

- **Remediation**: Defined processes will limit downtime and reputational impact.

- **Post-Incident**: Process improvement will enhance all relevant capabilities in the future state.