**Cybersecurity Incident Response Plan Template**

**Step 1: Preparation**

Consider the following opportunities to prepare your company before an incident occurs:

1. Create a complete **IT Cyber System Overview** of your company’s IT blueprint/architecture showing connectivity to understand all of the assets which could be at risk (e.g., in-house hardware, software, and data; phone system; online and cloud-based software and data; mobile devices; remote workforce)
2. Create a complete **IT Personnel Overview** for your company to document who is responsible for each of the various components of the computer systems (e.g., title production systems, email/messaging systems, network security) whether they be employees, consultants, or a Managed Service Provider (MSP)
3. Conduct a **Business Impact Analysis** to determine how a loss of access to hardware, software, or data for each system would impact everyday business
4. Establish a **Business Continuity Plan** to recover your daily business operations effectively after a limited-impact event (e.g., virus contained to one computer; power outage at a branch office; compromised system, device, or account)
5. Contact your insurance carrier(s) to determine if **Cyber Insurance Coverage** is in place or available to cover one or more types of potential cyber incidents and any requirements for an incident to be covered by the policy
6. Contact your attorney to identify requirements, draft notifications, and be prepared to distribute those notifications as documented in your company’s **Breach Notification and Reporting Requirements** as applicable to the jurisdiction(s) where you do business or where your clients and customers reside[[1]](#footnote-1)
7. Establish a **Disaster Recovery Plan** to recover from a catastrophic event (e.g., ransomware attack, network breach, email compromise, natural disaster affecting entire operation)
8. Establish **Roles & Responsibilities** for key functions in response to a cybersecurity incident (e.g., person responsible for coordinating response, talking with legal counsel, cyber insurance carrier, talking with customers, talking with media, talking with regulatory agencies, talking with law enforcement)
9. Create a **Crisis Communication Plan**, including:

* Contact information for internal and external stakeholders
* Prewritten communications for internal and external stakeholders
* Strategy for maintaining confidentiality and privileged communications

**Step 2: Analysis and Detection**

1. Monitor critical systems and alerts as defined in the **IT Cyber System Overview** (e.g., logon failure/success, firewall logs, computer logs)
2. Ensure alerts are monitored in accordance with your **Business Impact Analysis**
   * Refer to **IT Personnel Overview** to help monitor systems for alerts.
   * Refer to **Roles & Responsibilities** and **Crisis Communication Plan** for reporting and escalation processes.
3. If an incident is detected, determine if the scenario is a limited-impact event or a catastrophic event

**Step 3: Containment, Eradication, and Recovery**

1. Containment strategies are designed to remove active attackers from your network and contain a cyber incident (e.g., isolating the affected devices, system, or network; resetting passwords; disabling accounts)
2. Eradication strategies are designed to remove the threat or vulnerability before restoring operations to full functionality (e.g., remove unauthorized access; consider disconnecting backup process to maintain quality backup; clean the affected machine(s) or device(s); rebuild machine(s) as needed; consider removing all access for specific users)
3. Recovery strategies are designed to restore systems back to normal operations as documented by a **Disaster Recovery Plan** and **Business Continuity Plan**

**Step 4: Lessons Learned & Post-Event Activity**

1. Documentation of Incident
   * Document incident and resolution including lessons learned and any changes made.
   * Report to proper stakeholders as reflected in **Breach Notification and Reporting Requirements**
2. What did we learn?
   * What went well?
   * What went poorly?
   * Did we maintain confidentiality and privilege during the incident and response?
3. What actions should we take?
   * Review policies
   * Review/update processes (e.g., password strength and updates; user and security access levels; periodic testing of backup restoration; data retention)
   * Review/update technology for additional features, potential upgrades, or replacement (e.g., software, hardware, services)
   * Review Roles & Responsibilities for adjustments (e.g., business, technology, third-party consulting assistance)
   * Review insurance coverage
   * Consider additional staff training

1. See also: CSR Data Breach Reporting: <https://urisq.com/privacy-regulations/>

   See also: <https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf> [↑](#footnote-ref-1)