RYAN SWANSON
Lawyers since 1897

Ryan, Swanson & Cleveland, PLLC
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3034
www.ryanswansonlaw.com

# Get a Plan in Place: Sample Incident Response Plan

The following is intended to be the formal incident response plan for YOUR COMPANY to aid in the firm's navigation of varying degrees of ongoing information security threats.

## INCIDENT RESPONSE TEAM

| Role | Person | Title |
|---|---|---|
| Privacy Principal | | |
| Technical Lead | | *example*: Director Technology Engineering |
| Internal Security Specialist | | *example*: IT Engineer |
| External Security Specialist | | |
| External Legal Counsel | | |
| Compliance | | *example*: Chief Compliance Officer |
| Public Relations | | |

## SAMPLE COMPANY – INCIDENT RESPONSE PLAN

| Step | Detail |
|---|---|
| **1.** | **Defense and System Awareness**<br>Internal systems monitoring:<br>▪ Software and Applications, what are they, what systems to those programs monitor, how to they alert Internal Security Specialist to potential threats.<br><br>Technology Asset Inventory:<br>▪ Where is the location and identity of company assets for full impact analysis?<br>▪ Update the inventory. Track and document hardware, software and leased assets. Employee-owned devices, hosting or cloud services, and retired equipment are all relevant.<br><br>External systems monitoring:<br>▪ Location of your confidential information and personal information. Who is accountable for security and breach monitoring? |



206.464.4224 | Fax 206.583.0359 | Toll-free 800.458.5973

RYAN SWANSON
Lawyers since 1897

Ryan, Swanson & Cleveland, PLLC
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3034
www.ryanswansonlaw.com

| Step | Detail |
|---|---|
| **2.** | **Identify Threats**<br><br>Once notice of a threat is detected, identify tasks:<br>▪ Hierarchy of Incident Response Team involvement and task assignment.<br>▪ Quarantine systems and hardware.<br>▪ Notice to stop normal data overrides to preserve data.<br>▪ Incident Response Team required status checks and communications.<br><br>Threat Determination.<br>▪ Identify who is in charge of clearing whether a threat is a breach or not.<br>▪ Next steps and assignments if threat poses breach potential. |
| **3.** | **Impact Assessment**<br><br>Forensic Analysis.<br>▪ Determine scope of threat<br>▪ Review hardware data and log files<br>▪ Determine impacted stakeholders (e.g. staff, vendors, remote workforce and offices, etc.)<br><br>Determination of a breach.<br>▪ Outside counsel involvement<br><br>Prioritize and establish material facts:<br>▪ What is the impact level?<br>▪ What data was compromised?<br>▪ Can the source of the breach be determined and contained?<br>▪ Has the existence of vulnerability been identified?<br>▪ What is initial timing of the compromise and company's first identification and response? |
| **4.** | **Suppress Threat**<br><br>Engage forensic and incident response professionals to maintain data integrity. Eradicate the threat and close the vulnerability. Ensure preservation of work, log files and event traces during suppression. |



206.464.4224 | Fax 206.583.0359 | Toll-free 800.458.5973

RYAN SWANSON
Lawyers since 1897

Ryan, Swanson & Cleveland, PLLC
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3034
www.ryanswansonlaw.com

| Step | Detail |
|---|---|
| 5. | **Compliance**<br><br>Outline steps for potential scenarios:<br>▪ Breach but no data compromise<br>▪ Breach with data compromise<br>▪ Compliance with notification laws in applicable jurisdictions<br><br>Notification Procedures and Risk Management considerations:<br>▪ Notify insurer<br>▪ Notice to consumers<br>▪ Notice to vendors and stakeholders<br>▪ Notice to press |
| 6. | **Incident Review**<br><br>Fully collect and archive documentation relevant to incident. Engage in discussion regarding policy changes and implement policy, training and procedural changes as necessary.<br><br>Prepare and deliver formal executive report for stakeholders. |

*Questions? Contact Teruyuki Olsen at 206.326.5736 or olsen@ryanlaw.com.*



206.464.4224 | Fax 206.583.0359 | Toll-free 800.458.5973