HOW TO DEVELOP A

SECURITY INCIDENT RESPONSE PLAN

1. The Plan Starts With A Team

The smallest possible team capable of providing the right skills to the challenge quickly should be identified in advance. One human resources executive and one business affairs executive should be on the team. **The team must be able to:**

- **Define** the type of incident quickly and clearly.
- **Protect** the company's information assets.
- **Centralize** all activities required to respond to an incident quickly.
- **Prevent** contagion into other company and 3rd party partner systems.
- **Comply** with all federal, state and industry requirements.
- **Minimize** the potential for fines, litigation, loss of revenue, negative exposure, loss of customer confidence, and all other adverse consequences.
- **Communicate** with all persons outside of the team who need to be engaged.

2. Responding to an Incident

1. **Identification –** realizing that something has gone wrong is many steps short of defining the incident. The tech team members need to be well-rehearsed in order to get this done quickly.
2. **Containment –** Most security breaches involve malicious code that wants to spread. The tech team must be well drilled and the immediate steps that isolate the breach.
3. **Eradication -** Removing the cause of the incident can be a difficult process. It is both a technical challenge and an HR challenge. Unfortunately, employee behavior is probably connected to the source of the problem.
4. **Recovery -** Restoring all critical IT operations comes first. Back-up servers and data storage resources should have been isolated from an attack as a best practice long before the incident occurred. Restoring the originally infected hardware and software platforms may take more time in order to be certain that the malicious code is definitely gone.
5. **Communication –** while the technical members of the team are hunkered down working on steps 1-4 above, the human resources and business team members must be communicating with every critical stakeholder. This could include lawyers, clients, and police as well as employees.
6. **Postmortem -** Some incidents require considerable time and effort. Performing a postmortem is critical. The team needs to distance itself from the emotions of the moment and look back clinically. An incident in not fully resolved until the whole enterprise is smarter and better prepared for the next one.

3. Red Team Exercises

The strength of the team and value of the policy is 100% dependent on preparedness. "War game" scenarios where good people join a "Red Team" to describe different types of system attacks is an established best-practice for training a team to respond effectively in a crisis.

4. Contact a Professional

Anybody seeking advice about Incident Response Planning is encouraged to contact Electronic Office, at 828-274-1196.