#### **Step 2: Involve the Right People**

SOLUTION

The following employees or department need to be involved in order to reach 0% goal in the employee behavior:

**Incident Response (IR) Manager** - designate action plans during the detection, analysis, and containment of security incidents. Also conveys the severity of incidents to the rest of the company and reports regulatory implications to the legal department.

**SOC Analysts** - responsible for identifying, reporting, containing, and escalating incidents. Also responsible for threat and vulnerabilities analysis.

**Security Architect** - responsible for maintaining the security of the company’s computer systems. They think like hackers and preempt all possible moves and tactics an attacker could use to compromise the company’s network, to help them position security control and breach countermeasures.

**Software Engineers** - responsible for the design, development, maintenance, testing, and evaluation of applications.

**Director of Network Security** - responsible for VPN service configuration and maintenance. He/She is also responsible for network security and patch management.

**Director of Human Resources (HR)** - responsible for the up to date database of employees. Also coordinates the employees' training.

**Director of Communications** - responsible for managing the company’s internal and external communications. They work with the security team to create strategies to communicate to the public in the event of breach

**Director of Finance** - responsible for the financing of the projects that involves training and other technical solutions that requires funds. Also responsible for providing financial advice to all managers and staff regarding their budgets.

**Chief Legal Officer (CLO) / General Counsel** - reports directly to the CEO and responsible for overseeing, and identifying legal issues in all departments. CLO manages administrative tasks in the event of breaches that have legal/ regulatory implications.