Security Services Training Materials

Customer Types & Strategies

Cyber Security Clients

Client Types (Jax examples):

1. National Corporations (1,000-5,000 employees):
   - Blue Cross, CSX, Crowley

2. Regional Entities (250-1,000 employees):
   - Baptist Hospital, Suddath, Interline

3. Medium Size Companies (50-250+ employees):
   - Limitless

National & Most Regional Corporations - 1

- About Them:
  - These companies already have some internal security teams.
  - They will need “Excess Testing Capacity” to meet internal or regulatory requirements.
  - They know security terms and understand their testing needs.
  - Their needs typically include:
    - **Penetration Testing** (network & applications):
      - They have too many applications to test internally, so they will outsource to Zones.
      - They have various locations and want to outsource to Zones since we can do remote testing.
    - **Vulnerability Testing**
      - They need a 3rd party company to provide testing for items like HIPAA compliance audit or FFIEC cyber security preparedness examination
      - They have various locations and want to outsource to Zones since we can do remote testing.

National & Most Regional Corporations - 2

- Our Strategic Advantage:
  - **Fast and Flexible Deployment** – Our remote testing teams can be testing within days of an engagement. We can extend their testing capacity so they can focus on managing the larger picture of test results and remediation requirements.
  - **Efficient and High Quality Testing** – Our testing teams are have 7 years minimum applicable experience with a strong history of premium testing results. Because of our remote capabilities, we can provide this premium service, all at very competitive pricing.
  - **Robust Results Reporting** – Our proprietary client facing dashboard provides all current and historical test results in an understandable and actionable format for remediation teams as well as a graphical and digestible format for management and executives.

- What To Do Next:
  - Talk to Chief Information Security Officer about how we can either offset or supplement their security testing needs.
  - Get their current & incoming testing needs/requirements.
  - We will provide immediate turn-around with quote and statement of work.

Regional & All Medium Size Companies -1

- About them:
  - Larger ones, refer to previous National slide.
  - Smaller ones either don't know they need it or don't want to pay for it. Need to be taught why.
  - Hospitals & Financial entities need testing for HIPAA compliance audit or FFIEC cyber security preparedness examination

- What To Do:
  - Feed them this data:
    - 1.5 million annual cyber attacks. 4,000 cyber attacks every day. 170 attacks every hour. Nearly 3 attacks every minute.
      - Data breaches average $154 - $300 per record. These costs do not include:
        - Federal & state penalties, Corporate and individual Lawsuits, Business downtime & Brand damage
    - This year's IBM study found the average consolidated total cost of a corporate data breach grew from $3.8 million to $4 million.
    - Cyber-attacks are costing businesses $400 to $500 billion a year and is quickly becoming the reason executive jobs are lost and small to medium sized businesses are destroyed.
    - Current cyber security insurance policies have many gaps that do not cover the overall cost of an attack.