Houston Hiring Trends
Cyber Security

By

Michael Del Monte, Infrastructure & Security Lead

With the 2014 Oil and Gas bust, Houston saw some huge changes in the hiring landscape. Not only has our energy sector experienced layoffs by the thousands, HPE just announced a major layoff and MD Anderson announced a 10 percent cut. So where's the light at the end of the tunnel?

Depending on your area within IT, available openings are either abundant or scarce/non-existent. Lucky for us, cyber security is a growing space and is only going up. In response to our recent survey of Houston CIOs, we have a few interesting findings in the security space.

The need for cyber security derives from the executive level, rather than from the bottom up. This translates to a demonstrable need for security folk and a high probability of investment in hardened security programs. That said, growth may not be as robust as one would hope.

Through our survey, we found that every participating company has, in some form, critical infrastructure with sensitive data. This could be anything from company secrets, client data, patient data, or HR's internal personnel data. However, only 53 percent of these perceive said sensitive data as highly valued or target for malicious intent. 42 percent of these companies plan to invest in expanding their security programs with the latest and greatest tools and technologies and 20 percent intend to add additional headcount. Interestingly, only 30 percent of those surveyed have an internal CISO. So where's the disconnect?

The majority of new hires will be in compliance and audit. Growth is expected in the defensive technical arena; however, most offensive security positions will still be given to third party consultants. Even companies that have defensive and offensive teams in their soc still utilize third party consultants for a second opinion.

These findings are in keeping with threat projections from a prior CIO level survey. Protection from internal threat actors holds a higher priority than defending from external actors. We expect a surge in contingent labor as the Oil and Gas market picks up again. Contingent workers, disgruntled employees, and those swayed by money can access and distribute sensitive data. That is, unless the company maintains a high standard of compliance, tying in the need for compliance/audit experts. Penetration testing, forensics, and incident responses are roles typically managed by third party consultants. In my view, consulting specialists are more efficient and effective in managing this portion of work due to the nature of the changing threat landscape.

Cyber security is the top area of spending within IT. As Houston’s economy turns around, contingent labor is expected to pick back up, only increasing the likelihood of internal threat actors, in turn leading to a higher demand for compliance and audit professionals. Not every company is investing in the latest and greatest technologies; however, keeping that data secure in a way that is cost effective and not a huge blow to OPEX is the number one priority.