Cybersecurity engagement

Cyberattacks worldwide cost businesses more than $400B annually. Studies predict that number could climb to $2.1T by 2019

Cyberattacks worldwide cost businesses more than $400B annually.1 Studies predict that number could climb to $2.1T by 2019.2 Between apps being downloaded without approval, unmanaged devices being used within the corporate network, poor password protection, and more, too many organizations are leaving themselves vulnerable to attack. Now, with the arrival of digital transformation, more and more of these organizations need enhanced visibility and control over their IT infrastructure to take full advantage of the opportunity.

Cybersecurity engagement

Cybersecurity engagement provides you with a comprehensive analysis of your cybersecurity infrastructure, including your current software deployment, usage, and licensing data. In addition to helping ensure that you have the right processes in place to minimize cyber-risk, we'll also offer prescriptive guidance and best practices about cybersecurity in a digital world, freeing you to focus on innovation instead of protection.

Cybersecurity engagement benefits

- Minimize data loss, fraud, and employee downtime

- Save money combatting cyberattacks and increasing efficiencies

- Securely manage software assets and promote reliable cybersecurity practices

- Build a resilient IT infrastructure that can quickly respond to threats

- Ensure that you have a secure and effective defense against attacks

What to expect from a Cybersecurity engagement

PLANNING:

- Gather information in licensing, IT landscape & business organization

- Discuss project and arrange access & resources

Identify your needs & goals

DATA ANALYSIS:

- Review & validate all collected data

- Compare deployed assets with current utilization

Map to an optimized environment based on your goals

FINAL RECOMMENDATIONS:

- Discuss final recommendation

- Engage in data-driven discussions

Ensure your business needs & goals are met

53% of businesses in 2016 suffered at least one data breach in the past two years.[3]

[1]Http://www.cyberinsurance.co.uk/cybernews/lloyds-ceo-cyber-crime-cost-businesses-up-to-400-billion-a-year/
[2]The 2016 Cybe2Juniper Research, Cybercrime and the Internet of Threats, May 2015
[3]The 2016 Cyber Resilient Organization Executive Summary, PonemonInstitute and IBM

HALIAN International | Emaar Business Park, Building 4 | Telephone +971 4365 2600 | www.halian.com