Genome "GApp" – The people Centric Cyber Application Datasheet

About Genome GApp:

'GApp' is a People Centric Security mobile application to mobilize the organization against the rapidly growing cyber threats. With GApp, employees can demonstrate accountability by taking active role in defending the company against cyber-crime. GApp increases the organizational cyber awareness, alert employees and owners of organizational risks, and produce insightful analytics as an input to reducing Cyber Risks.

Genome's 'GApp' customers are typically corporate organizations which strive to reduce risk associated with Cyber Attacks and choose to improve their proactive approach. The constantly changing nature of attacks combined with our individual customized Awareness Training ensures continuous learning and demonstrated reduction in risk.

Key Benefits:

- ✓ Governance – Extending the boundaries of traditional security governance to include the current mindset of 'people centric security' (Considering that nowadays employees are considered as the #1 cause for data breaches);
- ✓ Providing employees with customized awareness training based on Micro learning approach;
- ✓ Ongoing security bulletins and updates on topics of interest;
- ✓ Providing reports regarding risks which are currently not managed effectively (Employee related);
- ✓ Increasing overalll organizational security awareness of employees;
- ✓ Measurement & Reward system for employees which demonstrate high awareness;
- ✓ Used as a 'Guardian' to alert employees of identified risk conditions;
- ✓ Provides first response services for cyber insurance policy holders (*Available for clients holding cyber liability policies with Genome Technologies' affiliated insurance Partners).

Approach:

- ✓ Improving the organizational incident response - Embedding an organizational culture of high security Awareness
- ✓ Providing insights regarding risks which are currently not managed (Employee related) - Increasing overall organizational security awareness of employees - Mitigating internal Risks - Lowering costs and increasing

effectiveness of security trainings by delivering customized awareness training content directly to employees' devices.

Learning Objectives - Deliverables:

Delegates will be converted from passive observers to cyber defence warriors through practical and memorable training on phishing attacks and how these should managed to reduce the risk of exposure.

Additional Information:

- ✓ Engagement is conducted over a twelve month period;
- ✓ Engagement includes a set-up phase, and an active operational phase;
- ✓ Includes a near real time dashboard and metrics report;
- ✓ Ongoing engagement;
- ✓ The campaign Is provided remotely.

Contact information:

For further information about this course please contact Dr Graham Wright at-

Mobile: +27 83 252 5727

Email: Grahamw@gnlcyber.com