Cybersecurity Management

Securing client data is paramount to business operations

Cyberattacks are becoming more prevalent in today's connected business environment. GES has implemented proactive and aggressive security measures and continually assess and modify our cybersecurity plan to ensure that your data remains secure with GES. Our approach mitigates the risks associated with a gamut of threats and attacks including, but not limited to, malware, phishing schemes, click baits, URL-hijacking, spoofing, SQL injections, Man-in-the-Middle (MitM), cross-site scripting, product exploits, zero-day exploits, and password attacks.

- GES utilizes a robust set of cybersecurity applications and systems to protect our networks, including:
- Internet content inspection and policy filtering to eliminate travel to unsafe sites
- Three layers of Anti-X Filtering Solutions to block malware, spam, viruses, phishing schemes, etc., from entering GES' network
- Internal office networks restricted to GES computers only
- True two-factor login authentication (DUO)
- Intrusion prevention systems at all internet perimeters
- Advance Malware Protection (AMP) scanning data flows
- Firewall controls on all internet perimeters
- Controlled behavioral and educational awareness tools
- Outlook "report suspicious email" tool
- Highly-secure file transfer protocol to send/receive data externally
- EndPoint protection agents running on all GES-managed computer end servers
- Patch management strategy
- Strong password requirements and 30-minute inactivity lock-out
- Access control lists (ACL)

Cybercrime Statistics[1]

Hackers attack every 39 seconds, on average 2,244 times a day

Cybercrime rose 600% since the COVID-19 pandemic began

The average cost of a data breach is $3.92 million

The average cost of a ransomware attack on businesses is $133,000

The average cost of a malware attack on a company is $2.6 million

GES Cybersecurity Practices and Procedures

Personnel identification and background screening

New employee security training

Monthly cybersecurity training

Subcontractor screening for cybersecurity measures

Controlled behavioral and educational awareness tools

Cyber asset management

Data-loss prevention

Controlled access management

Facility physical hardening

Threat and vulnerability management

Traffic monitoring for malicious content

[1] Statistics came from this web site: https://www.solutionzsecurity.com/cybersecurity-statistics-2021