Is your business prepared for Cyber Risks in 2018

The 2018 GSS Security Assessment

Excellus BCBS customers hurt by security breach
Hackers Access 80 Mn Medical Records At Anthem
Security breach in the California State Univ
Hackers stole 21.5 mn Social Security Numbers
Harvard Investigates IT Security Breach
CVS confirms data breach

GSS SECURITY TRANSFORMATION SERVICES

Helping Business Adopt Security Practices

gss Infotech

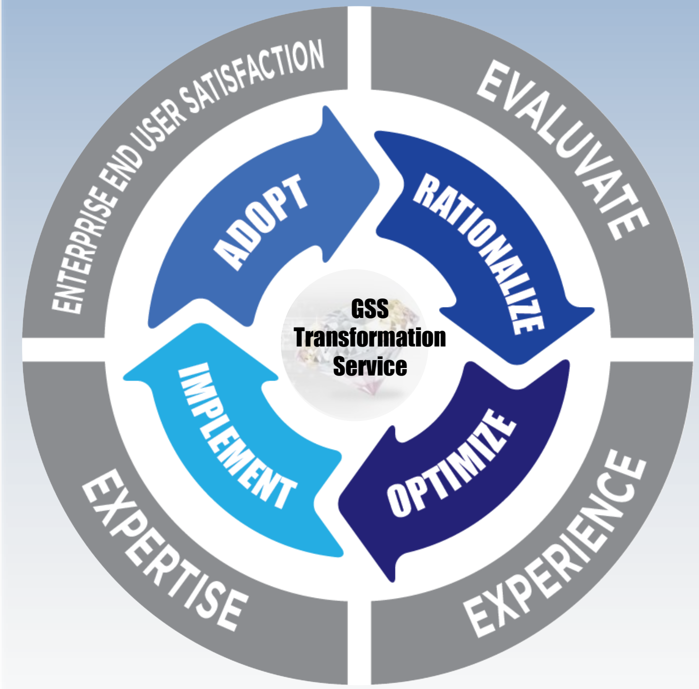
Why Do a Security Assessment ?

Over the last year the number of security breaches has increased two fold and the business is getting vulnerable to external hackers. While we continue to tighten our internal security, it becomes important to realize that keeping a continued vigil on customer's data is leading to more sleepless nights for C-level Executives .

The security breaches have also increased with the penetration of social media and mobility solutions driving both ecommerce and buying decisions on a scale that has overshadowed technology advances in security. Research has shown last year that an average of over USD 500k was spent by small and medium businesses to recover from cyber attacks. Knowledge and solutions are needed to create a secure environment for your business, both of which add to IT CAPEX and slow adoption of IT to business scalability.

GSS Infotech has over 20 years of experience in building Global IT infrastructure and with over 250+ IT engineers in the US, launched its IT security Assessment Service to "cyber proof " Business. With our combination of global experts and unique tools , we cover a wide area of your overall IT infrastructure and its exposure to vulnerabilities and threats .

GSS SECURITY TRANSFORMATION SERVICES



Our approach to IT Transformation Services is driven by our four key stages of Rationalization | Optimization | Implementation | Adoption.

Each of these by stages use proven methodologies and tools that are designed to identify your security strengths and weaknesses.

Over the next few pages you will cover all the different aspects of security assessment that we use to expose vulnerabilities and threats to your Business.

We have also defined our methodology for each type of Assessment to help understand what you will receive from our final report.

The time for each assessment is based on the Infrastructure and the number of locations the data is accessed from and our Consultants are available to estimate the time and effort to complete.

Partner with GSS Infotech to help cyber proof your business for 2018 .

> *In 2014 External hacking accounts for 98.73 percent of total records that were compromised - Privacy Rights Clearinghouse*

VULNERABILITY ASSESSMENT

Customized exploitation and assessment work to your environment and goals.
Areas explored: Infrastructure Security & Application Security

Infrastructure Security:

- External network vulnerability assessments
- Internal network vulnerability assessments
- Wireless security assessments
- RDP assessments
- Network architecture and firewall review
- Host and network device review

Application Security:

Application vulnerability assessment is to identify and remediate vulnerabilities and maintain a resilient web presence. This process involves:

- Web and client-server application security assessments.
- Mobile application assessments across most platforms.
- Software development lifecycle (SDLC) reviews
- Application architecture assessments
- Custom services as requested

Methodology:

- *Data Gathering & Project Set up*
  - Review of the project assumptions;
  - Detail list of IP addresses for scan;
  - Arrange to configure (IDS/IPS) to accept the originating IP address;
  - Optional scan using User credentials;
  - Contact information for both parties; and
  - Plan the scans including time-of-day.
- *Conduct Vulnerability Scans*
  - Perform an in-depth scan of the IP addresses provided and any optional User credential scans to identify security weaknesses and vulnerabilities.
- *Vulnerability Research & Verification*
  - Verify all vulnerabilities discovered;
  - Determine the potential impact of exploited vulnerabilities;
  - Prioritize remediation efforts; and
  - Generate specific recommendations for remediation.
- *Report Creation & Close-out*
  - Deliver a final report
  - Facilitate an effective knowledge transfer

> ***If Passwords Received as Much Attention as PSI We'd All Be More Secure - Mark Hatton, Data Protection***

gss Infotech

PENETRATION TESTING

A proactive & authorized attempt to evaluate security of an IT infrastructure by safely attempting to exploit system vulnerabilities including OS, service and application flaws, improper configurations, and even risky end-user behavior.

External Penetration Testing

Review of vulnerabilities that could be exploited by external users without credentials or the appropriate rights to access a system

Internal Penetration Testing

Protection from internal threats and ensures that internal user privileges cannot be misused.

Application Penetration Testing

Testing is performed in a black-box, ***(white-box will be a custom module)***

- Black box testing involves providing GSS only very essential information pertaining to the application, such as the URL or address

Wireless Penetration Testing

GSS's wireless security testing focuses on enumerating and verifying potential attack vectors and threats to your organization's wireless infrastructure. Evaluate and provide recommendations for improvement.

Methodology:

External and Internal Penetration Testing:

- Obtaining information about your Internet facing assets
- Security testing identify vulnerabilities in externally/internally facing systems and applications
- Optional phase includes exploitation of the underlying vulnerabilities

Application Penetration Testing

- To identify both common and application specific vulnerabilities
- Network and operating system security tests to verify that the underlying platforms are configured securely
- For role-based systems, testing is conducted across all user roles

Wireless Penetration Testing

- Access point discovery
- Wireless Penetration Testing
- Post wireless exploitation

Report Creation & Close-out

- Deliver a final report
- Facilitate an effective knowledge transfer

> **Phishing attacks -- like the one that may have been behind the recent Twitter AP hoax -- will persist because they work.** ***- Kevin Casey, InformationWeek Network Computing***

CLOUD SECURITY

Covers physical security of the infrastructure and the access control mechanism of cloud assets

Cloud Application Assessments
Uncover software vulnerabilities, demonstrate the impact of weaknesses, and provide recommendations for mitigation.

Cloud Infrastructure Assessments
Remotely identify the networks, hosts, and services that comprise your cloud's external and internal environments. Vulnerabilities are identified and if desired, exploited during a penetration test.

Host/OS Configuration Reviews
Remotely review the configuration of key applications, servers, databases, and network components to identify vulnerabilities that may go unnoticed during network testing.

Cloud Architecture Reviews
A network architecture review will evaluate the function, placement, and gaps of existing security controls and compare their alignment with the organization's security goals and objectives.

VPN Security Reviews
Compare your current configuration against recommended best practices and identifies any areas of concern. The assessment includes a remote configuration review as well as an architecture review.

Host-based Firewall Reviews
Analyze both the configuration of the host-based firewalls (accounts, logging, patch management, etc.) as well as the implementation of network security controls (ACLs) via the firewall.

Methodology

Evaluation
Understand exactly what types of data or processing the customer is considering moving to a cloud service and classify that data according to risk.

Discovery
Determine where the organization’s data resides so that appropriate controls can be put in place.

Analysis
Work with targeted cloud providers to analyze the extent to which the business goals can be achieved whilst ensuring the sensitive data remains protected.

Mitigation
Consult on the planning, supply and installation of those elements required to fulfil the security requirement that enable the cloud service migration.

> ***For years, popular opinion held that the threat of identity theft was overblown …. All that has changed." -*** *StaySafeOnline.org*

gss infotech

IT RISK & COMPLIANCE ASSESSMENT

Identifies risks, internal controls, and gaps in controls. The IT Risk Assessment breaks down the probability and impact of individual risks.

Our meticulous process quantifies threats business-wide:

- Infrastructure, applications, operating systems, facilities, and key personnel
- Business processes, implemented controls, and existing risks
- Ranked risks for key business units, departments, products, and services
- Review of audit plans, schedules, cycles, and scope

These controls are critical, and have two facets: design of controls and operating effectiveness of controls. In addition, organizations are required to comply with a variety of regulations, whether it is SSAE16, PCI-DSS, HIPAA or ISO 27001.

GSS has written guidelines on the use of risk assessment tools, risk factors and review these guidelines with your various stakeholders.
Our Consultants use these guidelines to grade or assess major risk areas and to define the range of scores and assessments.

Methodology

- GSS uses automated tools to identify gaps in existing security policies and SOPs to ensure compliance to major security frameworks including ISO 270001, PCI- DSS and SSAE 16.

- Our consultants will work with your internal quality teams to identify the existing policies and SOPS and then provide a risk assessment on the areas and gaps based on existing frameworks and standards.

- In case your business uses its own framework our auditors will familiarize themselves on the custom framework and provide custom assessment.

- GSS uses a unique and proprietary tool to facilitate cost optimization and cost of highly expensive consultation for multiple Frameworks and Certifications

> ***Businesses lose up to US$551,000 due to security breach** -B2B International in 2015*

OTHER ASSESSMENT

Other areas within the IT Infrastructure environment that may cause vulnerabilities and risks to the Business

Wireless Security Reviews

GSS's wireless penetration testing and assessment services evaluate the security of your organization's wireless implementations and provide recommendations for improvement. An optional wireless penetration testing phase includes exploitation of the underlying vulnerabilities.

VPN Security Reviews

The VPN review compares your current configuration against recommended best practices and identifies any areas of concern. The assessment includes remote and onsite configuration review as well as an architecture review.

Firewall Security Reviews

Firewall security reviews are important because they identify vulnerabilities that cannot normally be detected through network penetration tests and black box network assessments.

Methodology

Wireless Security Reviews

Focuses on enumerating and verifying potential attack vectors and threats to your organization's wireless infrastructure. The wireless security review is compromised of the following three phases:

- Wireless architecture review
- Wireless configuration review
- Access point discovery.

VPN Security Reviews

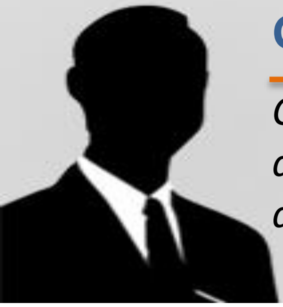
- Account management and passwords
- VPN security settings
- Patch management
- Network security
- Logging and auditing
- Client security

Firewall Security Reviews

An understanding of the overall security architecture and of the assets the firewall has been dedicated to protect.

- Examine the firewall configuration.
- Review of firewall rules and groups, system & account management, access controls, and logging and auditing.

> ***The single biggest existential threat that's out there, I think, is cyber -Michael Mullen***



GSS Security Assessment Cost Estimation

Costs can be minimized by setting out all the factors at the start and defining exactly what the assessment will include before diving in.

Security assessment projects have a beginning and an end, and produce a unique value to the organization. However, security assessments constitute a special type of project, where it is often a challenge to identify the project objectives, as well as to scope the time and effort needed to complete the security assessment.

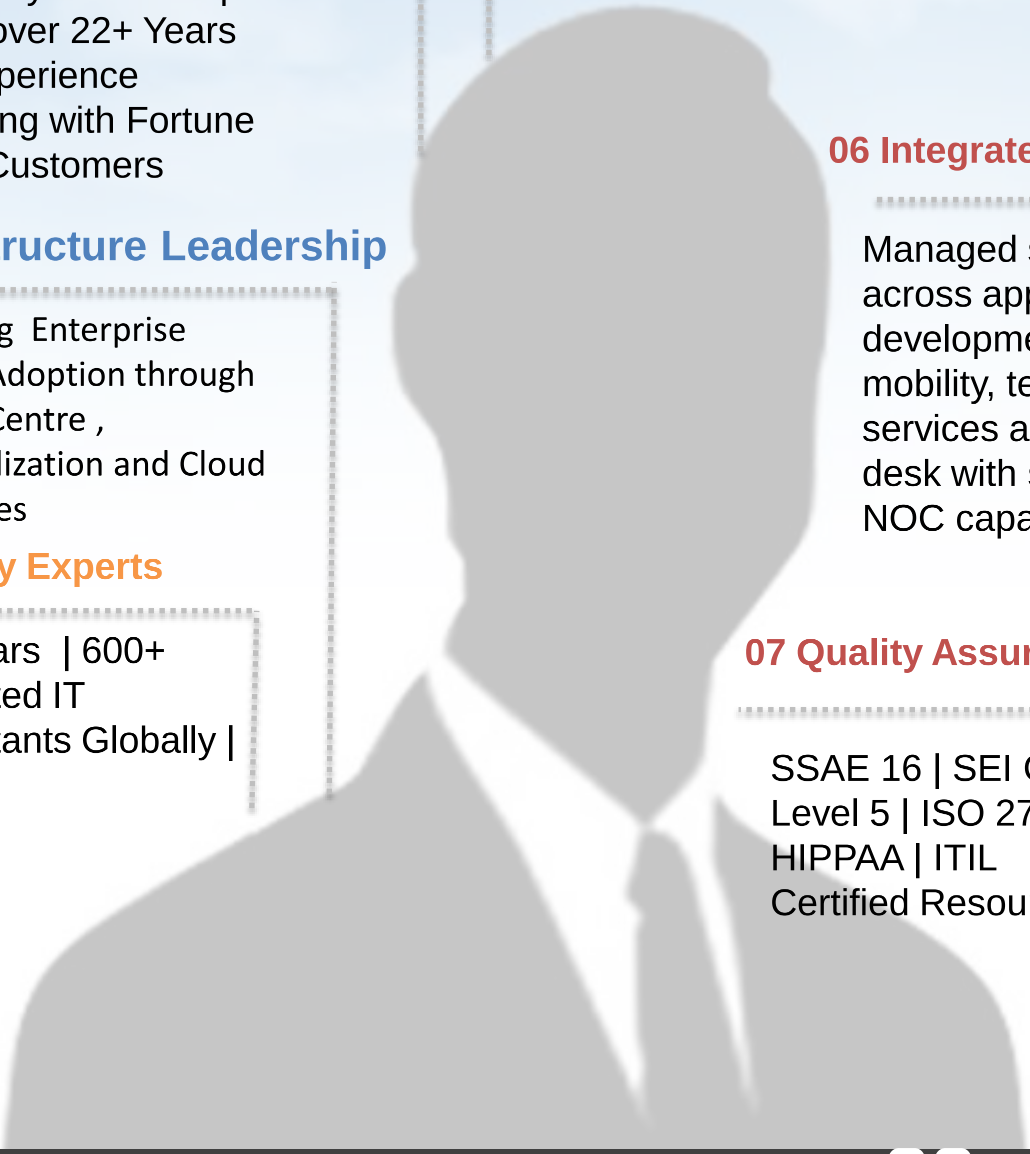
GSS Infotech takes a project management approach to scoping security assessments to make it easier. The result will be a more effective and efficient assessment .
The below information about your Organization and IT infrastructures will enable us provide a cost estimation, to help you move forward with this assessment.

2018 GSS Security Assessment

S#	Description of the item	Response
1	Number of IPs to perform Security Testing for Black box, White box and Grey box.	
2	Are all the specified IPs located at one location or different locations? If different location, please provide details.	
3	Are the server's physical servers or virtual servers?	
4	How many servers does your organization use for windows, Open systems and Unix?	
5	What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL)	
6	What Enterprise Resource Planning (ERP) application(s) does your organization use? (Examples - SAP/People Soft or In-house developed)	
7	Is there any Web application need to be tested? If Yes, Please specify details	
8	High level Network diagram	
9	Is your organization subject to any specific regulatory requirements? (PCI, Sarbanes-Oxley, GLBA, HIPAA)	
10	What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)	

To Thwart Attackers, Measure What Matters - Marc Solomon

The GSS Advantage



04 Service Delivery Framework

Innovative Delivery Framework based on leveraging Integrated CoE

03 Global Delivery Leadership

Delivery Leadership with over 22+ Years of Experience working with Fortune 500 Customers

02 Infrastructure Leadership

Driving Enterprise User Adoption through Data Centre , virtualization and Cloud services

01 Industry Experts

20+ Years | 600+ Dedicated IT Consultants Globally |

05 Alliances and Partnerships

Premium VAR for RH, NetApp, CITRIX , VMware, EMC , Dell, HP and a Gold partner for Microsoft

06 Integrated DevOps

Managed services across app development, mobility, testing services and service desk with security and NOC capability

07 Quality Assurance

SSAE 16 | SEI CMM Level 5 | ISO 27001 | HIPPAA | ITIL Certified Resources

> *GSS Infotech has consistently met and exceeded our expectations throughout the project – **IT Director , Large Association***

Ask for your 2018 GSS Security Assessment.

Rhonda K.Brown
Director of Business Development
GSS Infotech Limited
An SSAE 16 Company
Email: Rhonda.Brown@gssinfotech.com
Web: www.gssinfotech.com