



Abstract..... 3
GRC – the challenges are
significant 3
IT-GRC - an approach framework 5
New ways of managing new risks –
Call for innovative solutions 6
SecureGRC from eGestalt 8

June, 2010

Concerns towards effective information governance and risk management strengthen from the increasing trend in cyber-security and data breaches, the average cost per breach being US\$202. As per a recent survey in 2009, Corporations lost \$1 trillion worldwide as a result of data loss, both malicious and accidental. The impact of the breach leaves no segment untouched – retail, technology firms, medical industry and even the defense!

The next generation solution needs to integrate and automate GRC combining compliance workflow with control assessment automation and security monitoring.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, eGESTALT TECHNOLOGIES INC. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of eGestalt Technologies, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of eGestalt Technologies Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 eGestalt Technologies Inc., all rights reserved.

SecureGRC: Unification of Security Monitoring and IT-GRC: The Next Generation of IT Compliance and Business Risk Management

eGestalt Technologies Inc.

Integration and automation of IT-GRC with Security: Why is there a need and why is it the next big thing? Why should enterprises care?

Page | 3

Abstract

Concerns towards effective information governance and risk management strengthen from the increasing trend in cyber-security and data breaches, the average cost per breach being US\$202. As per a recent survey in 2009, Corporations lost \$1 trillion worldwide as a result of data loss, both malicious and accidental. The impact of the breach leaves no segment untouched – retail, technology firms, medical industry and even the defense!

An innovative tool, IT GRC management software, has emerged to address some of these problems. The “G” in GRC – governance – connects security management practices with enterprise wide governance and overall risk that goes beyond information technology. However the IT-GRC tools are not integrated with the security monitoring tools in the enterprise leading to disparate views assessment of the enterprise risk, leading to risk and liability exposure which can lead to catastrophic results.

*The next generation solution needs to integrate and automate GRC combining compliance workflow with control assessment automation and security monitoring. **SecureGRC** from eGestalt Technologies, is a comprehensive solution covering enterprise security, governance, risk management, audit, and compliance needs through a unified solution offering delivered via Software as a service.*

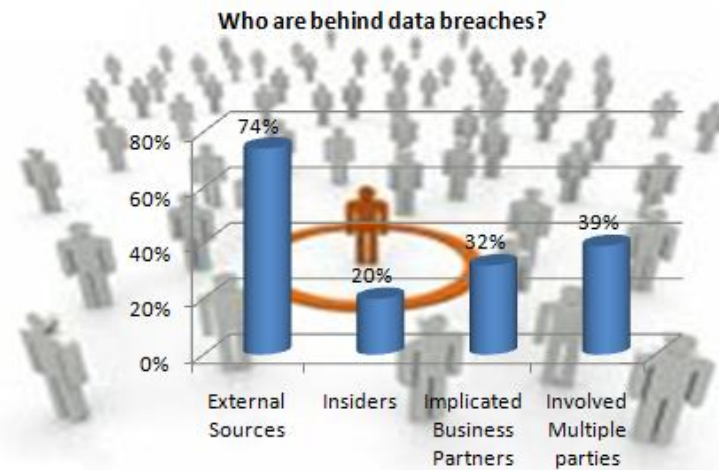
Read on...

GRC – the challenges are significant

You might not know it yet, but your organization and possibly even you are involved in IT GRC (aka IT Governance, Risk and Compliance) activities – every day! If you worry about compliance, deal with risks to information systems, think about controls and even simply report to IT senior management, you are doing IT-GRC. Moreover, it is likely that you’re not doing it well.

From a stage when organizations were blissfully ignorant of the impact of information security infringements, more focused on finding automated business solutions through information technology, today the awareness is growing and organizations are investing heavily on IT security solutions. With a number of solutions, products and platforms that are available in the market, the security products have evolved over a period of time – typically as any software solution that have emerged in the enterprise segment – pieces of solutions that address or focus on some specific elements of the problem. Organizations were left to themselves in managing all the technical and policy controls that they implemented for risk reduction and compliance.

Concerns towards effective information governance and risk management strengthen from the increasing trend in cyber-security and data breaches. The press today – online and traditional print media, has plenty of stories of such incidents. Surveys and research studies keep reinforcing the lack of security, or where measures exist, their lack of effectiveness to counter the security threats; Cyber threat and cyber security are hot topics today.



The 2009 Data Breach Investigations Report from Verizon Business for instanceⁱ, reports “90 confirmed breaches within our 2008 caseload encompass an astounding 285 million compromised records”. In further analyzing as to who were behind the data breaches, the report highlights the incidence of ‘external sources’ behind the data breaches as the highest.

The report also highlights that the highest cause of the breach is due to

‘significant errors’ - 67%! The report adds, “99.9% of the records were compromised from data resident on internal servers and applications”!

And the costs of all kinds of breaches are mind boggling. Costs from the largest computer data breach in corporate history at TJX, in which more than 45 million customer Credit and Debit card numbers were stolen was estimated at US\$ 256 million! Gartner analysts estimate that the cost of sensitive data break will increase 20 percent per year through 2009. “When you consider that the *average* cost per record breached is US\$ 202, it becomes clear just how much we all stand to lose”ⁱⁱ.

Who are the most affected? The retail industry (35%), followed by technology firms (20%), banking and financial industry (20%), medical industry (15%) and the defense industry (10%) What these figures signify is the truth – ‘better the security infrastructure lower is the percentage of breaches’. Overall, only 5% of the companies resort to security monitoring! The majority (55%) has absolutely no mechanisms for monitoring, and the rest 40% conveniently outsourced the IT security monitoring functions to managed services providers.

15 most common security attacks:

1. Key-logging and spyware
2. Backdoor or command/control
3. SQL injection
4. System access / privilege abuse
5. Unauthorized access via default credentials
6. Violation of acceptable use & other policies
7. Unauthorized access via weak or misconfigured access control lists (ACLs)
8. Packet sniffer
9. Unauthorized access via stolen credentials
10. Pre-texting or social engineering
11. Authentication bypass
12. Physical theft of asset
13. Brute-force attack
14. RAM scraper
15. Phishing

The 15 most common security attacks are in the side barⁱⁱⁱ. On top of the increase in threat levels and dramatic rise in regulatory activity, complexity of information technology also goes up. Companies now have to deal with complex, networked systems that perform critical business functions and might have components deployed inside the enterprise, on partner networks and also on private and public cloud infrastructure. More and more assets also use virtualization technology to achieve cost savings as well as other benefits such as energy savings and improved infrastructure resiliency.

IT-GRC does NOT stop threats; it helps people manage “the whole process” of IT security, compliance, and risk management through policy guidelines and implementation. Complying with a regulatory framework, as a first step, reduces the risk significantly, as these regulations or standards are the collective

wisdom of specialists in the society and thereby helps reduce the risk exposure through adoption of the best practices prevalent in the industry.

All such facts leave the CSOs and CISOs, the custodian for IT security, searching for solutions that would help him and the enterprise.

IT-GRC - an approach framework

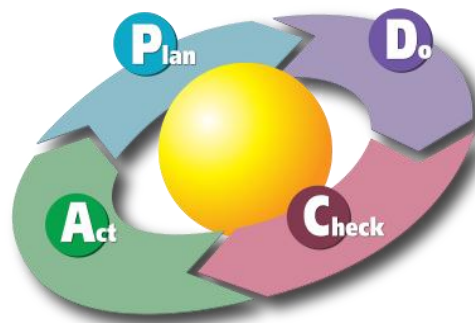
As organizations deploy more tools and more technologies to deal with threats, regulations and IT operational issues, the complexity of security management also goes up by a significant amount. However, few organizations consider how they would govern all these safeguards, both technical, process, and people based. A special category of tools, IT GRC management, has emerged to solve these problems.

GRC solutions deliver a higher level functionality than specific security tools (such as network IPS) and even high level than security management tools (such as SIEM). The “G” in GRC – governance – connects security management practices with enterprise wide business processes and governance and with overall business risk that goes beyond information technology.

In order to get a comprehensive picture, we need to go back into some fundamentals. What does IT Governance call for and fundamentally what is it?

Good Governance calls four simple steps:

1. Establish objectives and process for attaining those objectives, and reaching a new state, integrating the fact that this is an iterative process (**Plan**);
2. Implement the new process (**Do**); Do something as part of the action plan in moving towards the end results; processes and good practices or mandatory compliance requirements and risk mitigation
3. Measure new state against expected results (outcomes) to ascertain variance (**Check**); Learning occurs continuously which can result in redefining the desired state, state, identify the gaps, improve the planning and implementation steps
4. Audit to measure the resultant state (was it as expected? – Short of it? – Nowhere near it?) Determine cause of variance, determine changes for improvement, and repeat the sequence (**Act**).



Readers would be familiar with the above PDCA model [Dr. W. Edward Deming]

Let us look at the information security from a simple 6-A principle: The Six A's are Awareness – Availability – Assessment – Acceptance – Action - Audit. Awareness gets us to recognizing the truth that security threats are a reality and just therefore cannot ignore it. This awareness makes one to look at the 'availability' of data within the enterprise through logs, and network packets captured. The next step is to examine the available data which is the assessment phase which includes analysis of the data to pinpoint specific security breaches or understand a broad pattern. The analysis followed by recognition of the threats and accepting the vulnerability, results in action. The appropriateness of the action has to be audited which highlights any existing gap that is still vulnerable and needs to be plugged. This is a continuous process.

Early IT GRC tools were engineered to require massive volumes of Consulting Services (exceeding the cost of the tool itself in most cases). They also had issues handling larger volumes of control and compliance data.

Such tools failed to deliver on the promise of peer comparisons across organizations in regards to their approach to security management, compliance management and overall risk management, thus leaving enterprises in the dark about how well they're doing with security, risk and compliance. Finally, the old GRC tools relied on other – often expensive and themselves hard to deploy - Security Products to deliver security monitoring and control assessments.

Traditionally, the information security tools and the compliance management applications are separate application silos, with their own deployments in the enterprise with no interaction and communications amongst them leading to disparate and perhaps incomplete assessment of the business risk. This means that the policies defined by the IT-GRC framework is not calibrated with the reality on the ground as measured through the security assessment and management tools. This can lead to a huge gap in reality about the desired business risk and the reality on the ground, leading to potentially huge risks and liabilities due to threats and vulnerabilities.

A new innovative approach is required to integrate and automate GRC tools by combining compliance workflow with control assessment automation and security monitoring. Such a solution when deployed in the cloud enables simplified deployments, unlimited scalability and extensibility. It enables easier “pay-as-you-grow” subscription based consumption model enabling wide spread adoption through a SaaS model.

New ways of managing new risks – Call for innovative solutions

The next generation Enterprise solution should holistically cover all aspects of threats – internal or external, accidental or deliberate, intentional or unintentional through an effective system of IT governance, well evolved IT Risk mitigation system, and the flexibility and extensibility to plug in the requirements of any new regulation, present or in the future to seamlessly address many compliance requirements. This calls for not only new approach to addressing compliance solutions, but also for information security monitoring, 24 X 7, for all activities of the Enterprise assets and users in real-time, insiders and outsiders, by fully capturing all the data transferred, by analyzing them for events, patterns, incidents, to make a quick and meaningful analysis of any impending threats. Even where security violations have happened, the solution should bring it to the attention of decision makers in real-time, with all the information required for making a decision before it turns out into a debilitating impact with wide-reaching regulatory impact. For example, relevant regulations, affected critical assets and other information about the affected business function needs to be available immediately after a violation or missing critical control is detected.

Deployed in the cloud, such tools should integrate, security monitoring, automate end-point assessment with compliance and management workflows. They should resolve the security and compliance manageability challenges and break the spell of “management via Excel spreadsheet.” These new tools should deliver value for both strategic and day-to-day compliance management as well as security monitoring and data protection and thus help both executive management and “in the trenches” IT professionals and security analysts.

The combined solution should therefore provide:

1. Integrated compliance management and security monitoring - solution should be configurable as per the security policies requirements for each enterprise; Compliance and risk management workflows for management and IT professionals; automatic compliance scanning.
2. Multiple global regulations support “out of the box”; Compliance framework should address the compliance requirements of ISO, COBIT, BASEL II, FISMA, PCI, SOX, HIPAA, GLBA, RBI, IRDA, NSE, BSE, MCX, NCDEX, and any global, industry- or country- specific frameworks that require to be complied

- with. It should come with a readily available and useful content to address the regulations and not require the user to actually pay to build such content
3. Automated control assessment - It should automate online questionnaires to quickly assess the gaps in compliance, asset management, audit and compliance management, vulnerability checks, extensive report generation facilities, email integration, alert management, workflow schema, user access control, etc Such questionnaire should significantly reduce the burden of assessing the non-technical, policy controls and safeguard.
 4. Secure end-point devices – where a lot of sensitive and regulated data is stored - that should be easily accessible for remote monitoring and centrally managing, provide endpoint visibility such as the devices accessing a secure network via Wi-Fi, Bluetooth, USB, FireWire, PCMCIA, serial and other ports
 5. The security solutions for monitoring the network traffic should cater to the following features
 - a. Real-time network intelligence and advanced integrated tools for network forensics, fully integrated into risk and compliance views, not only for threat monitoring
 - b. Full packet capture, use of live network sessions and a rules based analytical process
 - c. Not limited by constraints inherent in only using signatures, log files and statistics
 - d. Must be ‘obsolete-proof’ through auto-learning capability by offering extensible infrastructure for rules-based and interactive session analysis across the entire protocol stack – from the network to the application layer
 - e. Provide an effective and highly automated process for problem detection, investigation and resolution, mitigating the IT risks lowering the overall business impact
 6. It should address business problems through detection of advanced threats, acceleration of incident response, policy and compliance verification, insider threat identification through 360 view of insider threats, incident impact assessment, and application and content monitoring
 7. Must scale up to global enterprises and down to small and medium businesses, struggling under the same regulatory burden as large organizations
 8. Capability to integrate multiple solutions to provide a complete picture to truly secure the enterprise and prove that you have indeed done so to the auditors and business partners
 9. The solution must deliver compelling value to the organization and be affordable Cloud based suite of services brings down the cost to enterprises including SMB Cloud delivery and “pay as you go” that would reduce the total cost of ownership compared to legacy tools and on-premise solutions

An effective and a complete combined solution must provide for a comprehensive security coverage that would simplify the management of multiple compliance mandate and conflicting security goals, deliver objective security metrics and be more affordable than legacy tools through innovative business models built around the cloud infrastructure and SaaS delivery model.

Today’s increased mobility, connectivity, complexity combined with demands for increased productivity offers equally increased vulnerability of endpoints wide open to data leakage and theft, introduction of malware and other cybercrime. GRC provides the framework while integrated security monitoring allows assessing technical controls, validating the policy implementation and assessing risk management dynamically to ensure efficacy of the IT-GRC management system.

Thus, a new generation of solutions is a compelling requirement that should integrate IT GRC and security monitoring tools to finally deliver on the vision of “a single pane of glass” for CSOs, allowing them to effortlessly view all security and compliance issues across the organization, its partners and service providers.

SecureGRC from eGestalt

SecureGRC from eGestalt Technologies, is a comprehensive solution of all enterprise security, governance, risk management, audit and compliance needs through a unified solution offering, SecureGRC™. SecureGRC is the first break through solution as it provides a comprehensive solution to address all aspects of information security and IT compliance. SecureGRC™ delivers what customers have been looking for - an integrated solution for security and IT-GRC through an integrated dashboard facilitating comprehensive log management, network monitoring and end-point assessment.

SecureGRC addresses all the requirements for the next generation unified solution mentioned in the previous section and a lot more.

SecureGRC includes all security and IT-GRC functions required to be compliant with ready to use compliance frameworks from across the world, leading edge context-based inference engines, most advanced alert processing and an easy-to-use logging and monitoring solution. It has built-in framework support for Compliance requirements of many countries which are ready to use and deliver value during the audits.

SecureGRC helps to assess and proactively deal with business risks, security threats, compliance policy and other IT-Security and GRC policy controls. It provides integrated coverage of security and compliance management, from endpoints and networks to management workflows and reporting, from end-point security through Network forensics and advanced threat detection to ensuring compliance with regulations as required in any country A solution is deployed in the cloud with on-premise and hybrid option an available on request.

SecureGRC is offered as a 'pay-as-your-grow', Software-as-a-service (SaaS) model targeted at Enterprises, including small and medium business segments. Through a patent pending innovate architecture and algorithms, the SecureGRC solution lowers the total cost of ownership dramatically, and thereby enabling enterprises, including SMB's to adopt IT-GRC and Information security services at a fraction of the cost of any other available solution.

Multiple deployment models are available including hybrid deployment models with on-premise software component if required (Customer Premises Equipment). It helps reducing the cost of IT Security significantly compared to other legacy tools, deployed as traditional enterprise software.

About eGestalt

eGestalt Technologies Inc. is a world-class, innovation driven, leading provider of cloud computing based Enterprise solutions for Information Security and IT-GRC Management. eGestalt is headquartered in Santa Clara, California, and has offices in US, Asia-Pacific and Middle East.

The Consulting and development team in eGestalt Technologies in India was founded in 2007 by former Intel and IBM executives.

For further information about the company, please visit <http://www.egestalt.com>

References:

ⁱ Verizon business, 2009 Data Breach Investigation Report

ⁱⁱ <http://www.pcicomplianceguide.org/merchants-20090416-cost-data-breach.php>

ⁱⁱⁱ <http://www.net-security.org/secworld.php?id=8597>