



## **Where's the "S"?**

**Don Gray and Jon Heimerl**

The latest buzz in Information Technology is IT-GRC, hyped by the vendors and abetted by the analysts as the next great wave of IT management solutions.

GRC stands for Governance, Risk, and Compliance and IT-GRC packages claim to be able to integrate these three domains under one roof. The underlying promise is that finally the board and management can get control of IT and appropriately govern and manage the IT operations to ensure that enterprise risk management goals are met. Regulators and business partners will be kept satisfied by the organization and its partners in regards to compliance.

But just as the best financial management systems and a bevy of auditors have not substantially stopped the flow of financial malfeasance and misconduct by motivated perpetrators, this promise will also fundamentally miss the mark without directly addressing the issue of security.

As evidenced most recently in the Hannaford data breach incident, where an estimated 4.2 million payment card holders had their trust violated through a security flaw, an organization can have a risk management program and a compliance program and still not be secure.

Hannaford, according to public statements, used an IT-GRC package to manage their risk and compliance program, had undertaken and passed outside assessments and audits, and from all outside appearances had been doing "the right things". But if having a risk management and compliance program nets the organization a very public and costly data breach, exactly what is the point? How many dollars spent on those programs would have been better spent on addressing the fundamentals of security?

After the breach was publicized Hannaford president and CEO Ronald C. Hodge said in a statement: "We have taken aggressive steps to augment our network security capabilities."

Section 4.1 of the PCI Standard requires "Encrypt transmission of cardholder data across open, public networks" stating further "Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit." Is it arguably "reasonable" to believe that internal networks are significantly less vulnerable to attack than public networks? Yes. Is it actually true in the real world of the large distributed network? Probably not.

Compliance is not security and risk management does not automatically provide risk reduction.

Many security firms have been telling enterprises for years that the best way to address IT Compliance and Risk is to assess where the organization's security program is from a maturity standpoint and then use compliance requirements and risk objectives to inform and advise the actions they need to take to move their security program where it needs to be. The best IT shops know that the way to optimize the scarce resources at their disposal is to include security in the architecture and design process, make the most of the security features and functions available in the products and tools they are already using, and judiciously apply additional capital and outside assistance for new functionality and the tasks they cannot or would rather not do themselves.

However, without a firm understanding of where their security program stands in terms of IT frameworks such as ISO or CobIT/COSO and in terms of their industry peers, security efforts tend to be misdirected, piecemeal, wrong-sized, or inefficient. Without the full inclusion of the organizations' security staff, compliance and risk management efforts will continue to fall short, discovering only after the fact that carts should not drive horses.

Consider the approach to "security" of two separate companies. The two companies are in similar industries and had comparable security budgets for their compliance and security program projects. Company "A" spent their time and resources to explicitly prepare for a Sarbanes-Oxley audit. All attention on their security controls was designed to make them more compliant with SOX requirements.

Company "B" spent their time and resources in more general management of their overall security program. Attention on their security controls was designed to improve their overall security program. They both achieved their specific goals, but received different results. Consider assessment results performed on the two organizations after similar amounts of resources were expended. The table here shows compliance results against a reasonable set of standards after each company completed its project work.

They both achieved their specific goals, but received different results. Consider assessment results performed on the two organizations after similar amounts of resources were expended. The table here shows compliance results against a reasonable set of standards after each company completed its project work.

Standard	Company A	Company B
SOX	80%	65%
ISO2005	41%	75%
PCI 1.1	27%	70%
HIPAA	46%	83%

Company "A" achieved good results becoming about 80% compliant with the appropriate SOX requirements. For the resources and time spent, this was a reasonable result for the company, and they considered the project a success. However, for about the same amount of time and resources, Company "B" came within 20% of the same level of compliance with SOX requirements, but made significant compliance in-roads with the other standards. Which of the two companies has the better enterprise-wide security program?

IT-GRC packages present a tantalizing image of a smoothly integrated IT function acting in perfect harmony with the wants and needs of the enterprise. And once the segment exits the "Peak of Inflated Expectations" phase of Gartner's hype-cycle these types of solutions will present a fine tool that can aid enterprises in managing IT. But a house is still only as good as its foundation. Many organizations would be better served ensuring that their security program is of a sufficient maturity before trying to add yet another layer of management and technology.

*Don Gray is vice president of technical strategy; Jon Heimerl is director of SecurCompass® development for Solutionary, Inc*

**Solutionary** is a pure play information security company that provides cost effective services for customers who outsource or co-source their managed, monitored, or on-demand security and compliance needs. Enterprise, mid-market, and SMB companies nationally and abroad count on Solutionary's security and compliance expertise, service delivery options, consulting services, and strong commitment to customer satisfaction.