Data governance: going beyond compliance


Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

Information security, in its broadest sense, is often an afterthought in an organisation's IT planning and spending and rarely gets the high-level attention it needs and deserves. The problem is worse when you look at the specific aspects of data security that fall under the umbrella of governance risk and compliance (GRC). In this interview, Danielle Jackson, chief information security officer at SecureAuth, thinks that's changing. But is the change heading in the right direction or is the responsibility simply being shifted?

Buried in IT

"GRC definitely does not get attention and funding within an organisation, especially within IT," says Jackson and one of the reasons is that it is increasingly being "buried" within the IT or security function. The various activities that comprise GRC have traditionally been spread around the organisation, with no overall organisation or co-ordination.

"There are a few areas in which GRC got buried," says Jackson, "and it started off with the development of GRC – the involvement with governance, risk and compliance in the various areas across an enterprise." Now, she explains, there's a "new initiative to collaborate and to grab all of those different areas together in one unit: that's traditionally the responsibility of a security organisation."

So while the various GRC activities might be finally emerging from their hiding places within miscellaneous parts of the organisation, the danger, says Jackson, is that this discipline is now being regarded as just another IT problem rather than something that affects the whole business. One way of understanding why this could raise issues is to see what's driving the adoption of GRC practices.

Driving force

"The driver right now is regulatory compliance," says Jackson. "As IT groups and security groups get a stronger presence in the executive suite and at the table with the other executives in the company – hiring CIOs [chief information officers], CISOs [chief information security officers] and CTOs [chief technology officers] – it definitely gives GRC more visibility."

Danielle Jackson is chief information security officer at SecureAuth Corporation. With more than 15 years of leadership experience implementing vendor security risk and assessment programmes for start-ups and Fortune 500 companies, Jackson defines the security road map for SecureAuth's suite of adaptive authentication and IS solutions. Prior to joining SecureAuth, Jackson served as director of information security for Bloomberg BNA and Mandiant, enabling integrity, accountability and assurance across various networks, systems, applications, data, cloud and security design. She is recognised as a subject matter expert in governance, risk and compliance (GRC) frameworks. Other key roles in Jackson's background include supporting various privacy and security efforts at Verisign, Accenture Federal Services and AOL. She has executed advisory and consultative engagements with public, private and global companies across multiple industries. Jackson holds a Bachelor of Science degree and a Project Management Certification from George Mason University in Fairfax, Virginia.

At last, information security issues are being brought to the boardroom and there is an opportunity to evangelise the benefits of security in general and GRC in particular. But there's a question over whether this is to do with a proper understanding at the C-suite level of the risks that make activities such as GRC necessary or whether organisations are being forced down this road by regulatory compliance requirements. Jackson points out that regulation is at least helping organisations' security functions to obtain funding and resources to enable GRC capabilities.

The number of firms feeling this pressure is increasing. At one time, compliance-driven information security was confined to a limited range of organisations – for example, if you handled payment card transactions you would need to be compliant with the Payment Card Industry Data Security Standard (PCI DSS): or if you were a US firm engaged in certain areas of the healthcare industry you might have to conform to the requirements of the Health Insurance Portability and Accountability Act (HIPAA).[1,2] But now, as technology creeps further into our lives, more and more firms are finding that they have to ensure that their data governance is up to scratch because there's hardly any organisation that isn't touched by some sort of regulation.

The forthcoming EU General Data Protection Regulation (GDPR) is a

case in point.[3] Unlike, say, PCI DSS, which spells out in exhaustive detail the steps that firms must take to protect information in order to meet the standard, the GDPR is deliberately vague, focusing more on what happens to you if you fail and your organisation is breached. Affecting any organisation that does business in the EU, it's likely to have a global impact, even on firms that previously were relatively untouched by regulation when it came to their IT systems.

Those firms that find themselves caught up in the regulatory net might do well to look at what has gone before – for example, how organisations have previously responded to requirements such as PCI DSS.

"Entities that are responsible for, or have access to, personal data for individuals are going to see some of these regulatory requirements and are going to be held to standards that they may not have taken into consideration before"

"PCI DSS was one of the pioneers in helping organisations pay attention to and really focus on compliance and GRC efforts – specifically with payment card data and cardholder data," says Jackson. At the same time, she adds, this also brought about a great awareness among organisations of the need to pay attention to the privacy needs and desires of individuals and a growing understanding that, when firms gather personal data, there is a great potential for harm if they don't take care of it. Where PCI DSS blazed a trail, other regulations followed, including HIPAA, GDPR and Australia's new rules on mandatory breach notification.[4]

"Entities that are responsible for, or have access to, personal data for individuals are going to see some of these regulatory requirements," says Jackson, "and are going to be held to standards that they may not have taken into consideration before."

Jumped or pushed?

This raises an important question: are organisations embracing GRC because they know it's the right thing to do and makes sense for the business, or are they simply giving in to external pressure? And does this mean they wouldn't do it unless forced?

"That's a tricky question," says Jackson. "I can't speak on behalf of every organisation, but in my experience and from the exposure that I've had with several companies, even in consulting engagements that I've been involved in, it is very difficult for organisations to get the resources, either monetary or personnel, to staff appropriate data security practices within their environment. It just becomes a secondary priority for a lot of these enterprises. The structure, the organisation, suffers as a result of that and unless there are monetary fines associated with non-compliance, strong data governance is just not going to be in place. I do see there is a lot of struggle, where organisations may focus on brand and consumers. They may focus their capital on their market strategy, whereas they're not paying enough attention to the security practices that they have in place until they're forced with fines, or until they face a breach themselves."

"I see the benefits and the advantages of entities and organisations paying attention to this, not only to help reduce and prevent some of the negative impacts on their environment, but to protect their consumers and their customers"

The good news, she adds, is that this is changing – the message is starting to filter through that good data governance is actually a business asset and worth undertaking.

"I definitely see a trend in the right direction," she says. "But we're not there 100% – it's definitely been a slow road."

A contributory factor in this, Jackson believes, is the difficulty of ensuring that any GRC solutions or strategies remain current when the environment they are meant to address is rapidly evolving all the time. "Technology moves so fast," she says. "And so do we as consumers. Products are launched quickly, especially in the security space where I've spent the majority of my career. Technology is just advancing every minute."

Given that, for so many organisations, GRC is a secondary consideration, there's rarely a time when the situation is sufficiently stable for a mature engagement with security.

"I am a security practitioner and I have a passion for GRC, so I would like to see it move at a rapid rate," she says. "I see the benefits and the advantages of entities and organisations paying attention to this, not only to help reduce and prevent some of the negative impacts on their environment, but to protect their customers. If you really are going to be obsessed with protecting your customers and you value them that much, your data governance and security practices should be at the forefront of your mind. And I don't think that it is a financially-driven motive unless there are outside pressures from regulatory requirements to help raise awareness as to what those impacts might be. Breaches have helped with that as well, but unless you're breached significantly, like healthcare or retail, or like Home Depot and Target, you may not feel the impact, or you may not see it as necessary for your company."

Business benefit

This situation might be alleviated somewhat if firms could see GRC as a business benefit with an identifiable (and preferably measurable) return on investment (ROI), but Jackson doesn't think it's that easy.