BRIDGING THE CHASM BETWEEN BUSINESS AND IT - THE GRC WAY

Posted July 1, 2015 By CloudTweaks

Business And IT

In today's world, company operations function at two distinct levels: the business operation level and the IT infrastructure operation level. While the two functions operate independently, IT exists to support the business. Many of the IT operations, like the deployment and management of IT infrastructure, applications and services are driven by the business layer requirements in a top-down fashion to enable the company to carry out its business. IT infrastructure management, including addressing **cyber security risks** is exclusively done in the IT layer. There are several tools, such as FireEye, McAfee, Qualys, ArchSight and BMC Software which IT deploys and uses in order to identify and manage IT security risk, but something is missing.

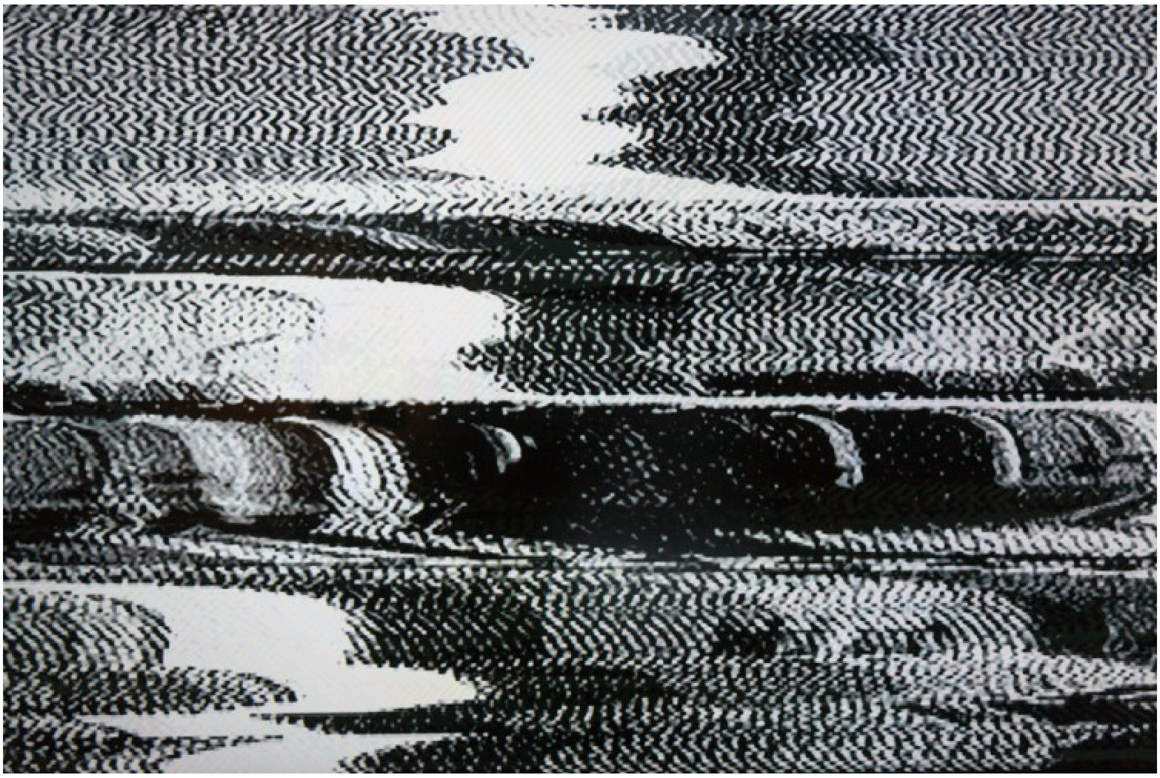
A chasm exists between the IT layer and business layer, when looked at from a bottom-up perspective.

Let's say someone hacked into your organization's network, and some data was compromised. What does that IT event really mean for the business? It's vital to understand that in business terms because that event could potentially put the company at serious risk.

Perhaps the data breach jeopardized the company's financial data; then it will need to do some proactive reporting. Perhaps the data breach made the company non-compliant with a regulatory requirement; then it will need to re-certify. Perhaps the data breach compromised personnel records, like the **June 2015** federal government hack; then the company will need to alert its employees.

The point is you need a unified business and IT perspective towards comprehensive enterprise risk assessment and management.

Don't lose the signal in the noise



The massive 2013 Target data breach showed what can happen when you ignore the gap between IT and business risks.

Target was PCI-certified (Payment Card Industry), thanks in part to a $1.6 million malware detection system from FireEye. On November 30, 2013, **Target's security team in Bangalore, India**, received alerts from FireEye, and informed Target headquarters in Minneapolis. But no one foresaw the risk to the business. In the words of Molly Snyder, a Target spokeswoman: "*Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow up.*"

Obviously something critical got lost in the noise. The first IT event detected was not high priority —from the IT perspective. But from the business perspective, red flags waved: the event occurred during the busiest shopping period and involved customers' credit card information.

The data breach cut Target's profit for the holiday shopping period by 46 percent, compared to the previous year. Worse yet, Target still faces dozens of potential class-action lawsuits and legal actions from creditors.

Prioritization is Key

Today's IT departments cope with a tsunami of security events, but how do they know which one to prioritize? How do they know that an event that may, on the surface, seem trivial and unimportant can have significant impact and jeopardize the business?

There is an obvious need to fill this gap that exists where low-level IT events can be mapped into enterprise risk from a bottom-up perspective.

- A Governance, Risk and Compliance (GRC) system, promises to help fill this gap between the IT and business layers.
- Governance, Risk, and Compliance (GRC) systems help organizations connect the dots across key areas: the limits for regulatory compliance, the analytics for risk management, and the metrics for risk controls. Because a GRC system spans the enterprise, it can help guide and prioritize the appropriate response.
- When setting up a GRC system, a company must define its critical assets, metrics, and risk assessment controls. The system can help manage and prioritize anything that impacts regulatory compliance — such as Payment Card Industry (PCI) compliance or the Health Insurance Portability and

Accountability Act (**HIPAA**).
- A GRC solution provides a bottoms-up approach to managing and addressing IT events—by keeping the business needs in mind. An apparently low-level risk will be given higher priority if it threatens a critical asset—or if it jeopardizes a regulatory requirement. This integrated and pervasive 360-view is where the value of a GRC solution lies.

Visibility

It's all about understanding the business risk context when prioritizing IT assets and responses to IT events.

Chief Risk Officers (CROs) see and understand key business risks. They have the visibility and they can make the call. They report out on the organization's risk profile by leveraging a variety of tools and risk dashboards to the Board of Directors level. Equally important, they collaborate across the C-suite and provide management with the guidance on what needs to be addressed, how, and when.

Needles in Haystacks

Moving forward, I see challenges ahead on all three fronts: regulations, systems and threats.

Regulatory requirements are increasing and it's more challenging for companies to be 100 percent compliant with all the appropriate risk controls in place. In terms of systems, an organization's IT footprint and adoption of cloud-based applications is constantly evolving and expanding.

Meanwhile, the variety and number of cyber threats are increasing, and malware is becoming ever more sophisticated. I anticipate that the volume and severity of IT events will increase significantly. Figuring out which events will have the biggest impact on a company's business is like finding a needle in a haystack. But it need not be.

That's precisely where a GRC system can help. By leveraging the correct GRC analytics and intelligence, organizations are able to identify and understand their risks from both the business and IT perspective. Bridging this gap can lead to better data-driven decision making and superior business performance.

(Image Source: **Shutterstock***)*

##

By Rajesh Raman / *Vice President at* **MetricStream**

Rajesh is responsible for Zaplet, an Enterprise GRC Platform-as-a-Service (PaaS) business unit. Rajesh is a seasoned senior software executive with extensive experience in leading products and technology in Security, Networking and Cloud domains. Previously Rajesh worked at Cisco, where he led the development of a number of innovative and pioneering products, including Cisco's award winning Identity & Policy based Secure Access & Mobility product, Identity Services Engine (ISE), and the Application-Oriented Networking (AON) products. Prior to that Rajesh worked in leadership roles at companies such Oblix, BEA Systems (both acquired by Oracle) and Lotus/IBM.