



▶ Showing the Way

Emtec marshals unique resources to help client revive a stalled risk management project.

Risk

Risk is a word that typically carries negative connotations. However, progress always involves risk. As the old saying goes, sometimes you have to go out on a limb because that's where the fruit is.

Information Risk Management (IRM) frameworks are employed to help organizations recognize and remediate information or technology-based risks based on the potential for business impact. The idea is to protect the organization from excessive risk without creating barriers to innovation.

A major e-commerce payment processor with global operations recently saw the potential for using IRM to maintain innovation and collaboration while also ensuring compliance with a growing number of legal and regulatory mandates. However, laying the groundwork for an IRM framework proved to be a daunting task that lay outside its core competencies. The organization called on its longtime technology allies at Emtec to show them the way.

"We've had a long relationship with the CISO (chief information security officer), and they are a believer in our approach to security and to IRM in particular," said Michael Shortino, who served as Emtec's project manager for the engagement. "He brought us in to help them structure the program, with an initial focus on the policy and compliance aspects of their overall IRM strategy."

At a Standstill

Policy development is the cornerstone of an IRM program. Policies dictate how information flows across the various systems, devices, applications, users and locations in any complex business environment, as well as how that information is used and controlled. Policies must be detailed and coherent, yet flexible enough to apply over time to emerging technologies and changing legal and regulatory mandates.

Policies commonly address network access, log management, data encryption, identity protection, discovery and classification, access and authorization, data retention, compliance reporting and many other key issues. Because policy development is such an important first step with such broad ramifications, there is a certain amount of pressure to get things right the first time. As a result, many organizations experience "paralysis by analysis" and waste significant time and effort trying to get off the starting blocks.

That was one of the problems facing this particular client.

"They had a team in place and had published some policies, but they were having a hard time getting policies to the point where they could be actively utilized by the business and allow them to report on compliance from a legal and regulatory perspective," said Shortino. "They needed a strategy for how to create, implement and improve their policies over time."

Common Problem; Uncommon Solution

It was not a unique situation. Many other organizations seeking to implement a risk management program have similar issues. In fact, there is general agreement that the growing complexity of the regulatory landscape is causing organizations across all sectors to spend increasing amounts of time and resources on their compliance efforts. Although organizations are devoting more of their IT budgets to compliance, demands continue to outstrip resources. More than 90 percent of respondents in a recent Ovum survey said that compliance was taking more time and resources, while 96 percent said that the complexity of the regulatory landscape was increasing. There was less agreement about the way forward.

Emtec provided the guidance in formulating a clear path. With Emtec, they found a partner that could deliver an exceptional mix of resources and expertise. Emtec marshaled a team comprised of technical writers, policy documentation experts, application security experts, and a variety of IRM and compliance experts — all with a minimum of 15 years of industry experience. To provide executive-level guidance, Emtec also brought in the former CISO of a global financial services firm with direct experience implementing IRM policy and compliance controls that meet PCI Data Security Standards (PCI DSS) and Federal Financial Institutions Examination Council (FFIEC) guidelines.

One distinct aspect of the engagement is that Emtec took care to build a team of local resources, subject-matter experts from across its practice areas and industry renowned security experts. This enabled Emtec to provide the customer with constant face-to-face representation while also holding down costs.

“This isn’t the typical model where your consultants travel in each week and then go home on the weekends,” said Shortino. “We mix local and remote resources so that we can develop a framework as quickly as possible and deliver it at a relatively low cost.”

About Emtec

Established in 1964, Emtec, Inc. is a systems integrator that provides IT services and products to the federal, state, local, education and commercial markets. Our market leading value-based management methods, coupled with best-in-class IT technology, consulting and development services, address a wide range of specific client needs, as well as support broader IT transformation initiatives. Emtec’s service capabilities span the United States, Canada and countries around the globe.

Emtec helped the client create a library of policies and standards, based on templates and knowledge developed over numerous engagements. This library was aligned to an industry standard eGRC tool, that the client purchased, which can be used for ongoing policy life-cycle management and for compliance reporting.

Mind the Gaps

With resources in place, Emtec provided a detailed gap analysis between the client’s current information policies and controls and IRM industry best practices. The gap analysis provided a road map for continued policy development, resource deployment and technology utilization necessary for a successful IRM implementation. The client was so impressed that they actually retained key members of the Emtec team to consult on two other troublesome projects.

The first involves developing the metrics and measures required to report on key performance indicators related to their organization-wide security. This will allow for visibility into the security health of the organization.

The other is the development of an application inventory (what apps have been developed, who are the business owners, what other apps do they interact with) - to gain a real understanding of what their critical applications are for security. Both of these projects are ongoing with metrics and measures recently extended.

“I think this client and the 3 engagements in particular show the real breadth of Emtec’s capabilities and the depth of our resources both in-house and through industry-wide connections,” said Shortino. “There’s a tendency in this industry to be very insular in your thinking about who you can or can’t use on an engagement. We don’t have those kinds of boundaries at Emtec. We always look to use local resources when possible, but we have a large number of internal subject matter experts across the company and long-standing relationships that enable us to call on industry recognized specialists when necessary.”