Global Limited has the reputation as one of the world’s leading providers of infrastructure information systems, software, and services around the world. Global’s clients range from world-wide enterprises to startup companies across all industry sectors, including financial services, manufacturing, transportation, and public services.

**Business Case**

Information is an organization’s most valuable asset, yet traditional security practices have either not provided adequate protection of information or have been so restrictive that they have prevented organizations from making the maximum use of information to innovate, collaborate, and achieve competitive advantage. This is primarily due to the reactive approach to security that many organizations have been forced to take in the past. Rather than viewing information security as a business enabler, they have tended to view it as a business inhibitor—a defensive strategy, designed to prevent bad things from happening. What’s more, security policy has tended to be fragmented, especially for large global corporate organizations whose information technology (IT) infrastructure spans across many countries and business units.

This approach has been likened to a game of Whack-a-mole—the problem is that good efforts in one area can be quickly nullified by failures in another. For example, a bank may protect its online banking portal from fraud only to have a privileged user copy confidential customer data to an unsecured laptop, which they then leave in a restaurant. These days, however, forward-thinking organizations like Global recognize the benefits of moving away from reactive “silo security” to take a more proactive and holistic approach to information security and compliance, based on the established discipline of risk management.

To help with its security transformation, Global called upon the expertise of CIS–its own Security Division. CIS’s information risk management (IRM) strategy brings together, within a global framework, all the components that an organization needs to plan and implement an end-to-end approach for protecting a business’s most critical information assets.

**Tracking Data Across the Enterprise**

The first step in this approach is to understand which information is critical to the key business initiatives. Global, for example, relies on a number of enterprise portals to share information and business processes across its global organizational boundaries. By enabling collaboration between employees, partners, customers, and suppliers through the sharing of critical business information, online resources such as Global Connect-Link, gives Global a competitive advantage in the market. However, they also create additional risks.

Global Cadence is the front-end for over 40 applications and has over 200,000 registered users. Some people are allowed access to more information than others, and this must be provided through a secure online transaction. It is also important to note that these online transactions hit all parts of the IT infrastructure: from the end point, through to the network, and the data center. However, rather than letting this risk hinder its business initiatives, Global works with it to minimize its impact.

Following CIS’s information risk management approach, Global follows the data involved to gain a complete and transparent view of all the places, the approach exists across the organization. Global identifies the points of vulnerability and what events could put the business at risk. This exercise is very complex, since data resides in many places.

**Prioritizing Investments**

The second core concept behind CIS’s IRM strategy is the idea that security investments should be prioritized, based on the risk that a given activity entails, relative to the potential business reward, and in keeping with the organization’s appetite for risk. Risk is defined as the likelihood that an event will occur and the consequences if it does.

Global, through CIS, prioritizes its business initiatives and protects the most valuable information at the point where it is most vulnerable. Once the information has been located and the risk assessment performed, Global implements controls, including policies, technologies, and tools to mitigate that risk. Repeatability and reuse of security controls is central to CIS’s strategy.

Ideally, this control framework should be established on best practices or standards like International Organization for Standardization (ISO) 27001 ensuring that it is broadly applicable and effective in addressing most of the security challenges an organization may face. The range of controls will be very wide, but CIS places significant importance on two groups of information-centric controls—data controls and access controls.

**Implementing Security Controls**

Using CIS Continuity Manager to secure information at the end point, Global is able to manage large number of external users while enforcing a centralized security policy that protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs.

Global has also issued secure-access tokens to all employees to add an additional layer of security for access to enterprise portals like Global Cadence. This offers authentication based on two factors, something the user knows, such as a personally selected personal identification number (PIN), and something the user has, such as a secure access token. CIS Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

Global must also ensure end-to-end data security, not just at the end-point. To do this, Global uses the data loss prevention (DLP) product across its entire enterprise to discover, classify, and take policy-based actions on all of its structured and unstructured data, whether it is in use, in motion, or at rest on endpoints, networks, and servers.

Beyond this, the DLP suite enables Global to monitor activity in different business units and develop campaigns targeted at specific user groups. For example, DLP suite can help Global understand which particular departments display high bandwidth usage, meaning they are using the Internet quite often. It can then monitor these business units more closely, since the chances of a security breach, such as a Trojan embedded in a Web page will be higher for them than in other departments that use the Internet much less.

**Reporting, Auditing, and Compliance**

Finally, Global uses the CompScan platform that provides a mean to audit its controls and document the effectiveness of the controls with regard to compliance and security regulations. This security information and event management (SIEM) solution collects and analyzes huge amounts of data regarding access in real time.

CIS CompScan provides Global with a centralized view of the log information from thousands of security devices, including data generated by CIS DLP Suite, security tokens, and intrusion detection systems (IDSs). Identifying correlations between logs from all these sources can help in the early identification of potential security threats via Global Cadence. CompScan also helps the company to identify important cost efficiencies ensuring that Global will lead the market in infrastructure information systems provision. For instance, Global’s IT Security Division can see what percentage of a business unit, region, or site is causing the most impact to network performance or causing risks to Global, its partners and its customers. This information is then used by Global to drive remediation and save hundreds of thousands of dollars.