BARBADOS TODAY.bb

How to write effective and efficient cyber security Requests for Proposals (RFPs)

Guest Column

Edward Millington

Cybercrime, (a World Economic Forum (WEF) top 10 global risk to businesses), continues to generate considerable damages and disruptions to businesses of all sectors, creating substantial business risks (financial, legal, compliance, reputational, etc.,) affecting businesses for months and sometimes, even for years. We must understand in 2023, cyber-attacks by the cyber-criminal enterprise are carried out solely (usually) for substantial financial gains, where efforts are made to steal valuable data for sale on the black market. Cyber-criminals have no sympathy for businesses and the lives of the people they affect, and it is therefore very important that businesses secure themselves and the data within their boundaries effectively and efficiently.

Operating and maintaining a high level of security that is needed (programs) can be very difficult and resource intensive. With budget constraints, these programs can become limited in their effectiveness and efficiency in managing the cyber-risk of the business. In such challenges, businesses usually look externally for security solutions and services, but this in itself can be very perplexing, and many times incorrectly done through inadequate, ineffective, and imprecise RFPs (Request for Proposals).

The following are common pitfalls to Cyber Security RFPs creation:

· The creators of the RFP provide vague insights and requirements, and most times, little data when requesting designs, complex recommendations, and or quotations from "informative" proposals, thereby preventing the business from having its strategic goals truly met.

· The Creator (s) have very limited knowledge of Cybersecurity & Data Risk Management, thereby preventing the RFP from fully capturing the business's strategic security needs. A full understanding of business resilience: cybersecurity, cyber-resilience, data-resilience - overall cyber & data risk management is usually and crucially noted.

· Committees which are involved in the process may not have a clear insight and need for what is being sought from providers. They are usually given a task to accomplish, and many times, stakeholders' involvement and knowledge sharing can be limited. This leads to an RFP that is generic and vague and lacks context.

· Collection of requirements by multiple contributors can create a document with similar questions - asked in multiple ways. In addition, this can create many requirements that may not help the business strategically. Such effects create a much-worded document, misrepresenting the needs of the business. In other words, the value of an RFP is lost in context.

· Third parties involved who are not aware of the operating needs, design, and functions of many business units and processes may not be able to offer or create an RFP that truly captures the strategic requirements of the business.

It is therefore important that businesses act diligently in vetting and selecting the correct consulting service (s) to achieve their needs.

With such common pitfalls, it is very difficult for any provider to informatively reply, thereby defeating the RPF's success in acquiring a proposal (s) that matches the requirements and needs of business strategic goals in cyber risk management – effectively business resilience.

Once the common pitfalls can be resolved, the RFP procurement process can be further enhanced accurately and in fullness with the following recommendations presented below.

Please note the following recommendations are compliments of the working partnership between CariSec Global Inc. (Barbados) and Trustwave Holdings Inc. (a Frost & Sullivan, CRN, Gartner, ISG, MSSP Alert, Global InfoSec Awards business awardee) – a Singtel group of companies.

- Select five vendors/service providers your peers have recommended and/or have scored highly in a respected third-party evaluation (e.g., Gartner, Forrester, etc.)
- Be willing to initiate an NDA between all parties.
- Invite them to an introductory call.
- Be clear, direct, honest, and communicative with vendors.
- Present the challenge (s) you would like them to solve .
- Supply each vendor with the presentation and any other relevant details.
- Book workshops with each vendor.
- Allow them two hours to present their solution.
- Discern the reality of what they can deliver. This is not simply a sales pitch. You must know the ins and outs of the solution, how it will solve your business need, how it operates within your existing structure, and the responder company's SLAs around implementation, support, etc.
- Narrow down the field to two finalists.
- Schedule a final workshop with each to address any unanswered questions or concerns.
- Negotiate – don't skip this part! You will ultimately regret "settling" for a solution or price that wasn't your intended goal.
- Sign contracts, start implementation.
- Form a relationship that can encourage development and partnerships at all levels.

Undertaking a successful RFP from creation to procurement to implementation is every business's goal and achievement. Good luck!

Edward MILLINGTON, (CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of CariSec Global Inc., a Caribbean (Barbados) based company and a Lead Security Consultant, strategically focused on providing Security & ICT Governance and Services to organisations operating in the following sectors: financial, government, health, manufacturing, private, retail, and energy and utilities. He is an Information Systems Security/ ICT/Telecommunications veteran of two decades, where he directed organisations, leading them in the achievement of further financial goals through strategic planning, designing, and solutions direction.