

### ACCELERATING YOUR CASH FLOW

*By Silka Gonzalez and Matthew Oakes*

Historically speaking, financial information has been the most important information asset. Ancient Mesopotamia used to protect financial and barter records of the royalty's treasuries. Empires from Rome to India and Egypt to China used encryption to protect financial information from subterfuge. Times have changed today, and how, but the principle of protecting financial information still remains as critical as ever.

The security of financial information ranging from payroll records to company financials can essentially make or break an organization's reputation today. With modern-day information systems now doing the jobs of humans in storing, processing, and sharing financial information, accountability has become more difficult and yet as unforgiving as in the past. This accountability lies in the hands of today's chief financial officers (CFOs) and there are some serious questions that CFOs should be asking about the security of their financial systems.

#### **Question 1: Where is my organization's financial information?**

Does your organization have current and complete documentation on the organization's financial information flow? If you need to protect your organization's financial information, you need to know exactly where it is, how it flows, and where it flows to. Ensure that such documentation is available and is updated on an ongoing basis to ensure that all changes are incorporated and that no information is overlooked.

#### **Question 2: Is our information security budget enough?**

The key, really, is to identify if the budget allocated to information security is commensurate with the nature of risks faced by the organization. Key executives of an organization must sit down together to identify how they plan to secure the organization's critical information, the regulations they need to comply with, and their own standards of what they define as "acceptable" information security. Once this is done, the information security budget only needs to be commensurate to achieve this baseline. A security budget doesn't have to go beyond what is required. That would be a waste!

#### **Question 3: Are we optimizing our budget usage?**

Various regulatory compliance requirements across several regulations often have many similarities. To be fair, all they're trying to tell you to do is to secure critical and sensitive information. The fact is, you would be trying to that anyway as a part of your ongoing security program. There is, then, no need to view these through separate windows. Combining requirements from different regulations that you need to comply with and addressing them collectively, even inclusively as part of your own security program, will not only save you a significant amount of time and money, but will also enable you with more efficient and effective information security.

#### **Question 4: What regulations do we need to comply with?**

Being aware of what regulations an organization needs to comply with may sound simple but, surprisingly, many organizations overlook certain regulations due to misinformation or plain oversight. It is a good idea to be aware of regulatory requirements in a little more detail. For instance, the Payment Card Industry Data Security Standard (PCI DSS) requires compliance from all organizations that handle, process, store, or transmit credit/debit card data. Another example is when educational institutions engage in student loan making or provide other such financial services; they fall under the purview of the Gramm-Leach-Bliley Act (GLBA). One of the often overlooked examples is that of state-specific regulations that mandate organizations to notify and disclose information security breaches. Often, the best approach is to either study information security relevant regulations to see what applies to your organization, or to get an expert to help you do it. Instead of being at the mercy of the regulatory officer's mood, it would be wise to take stock of the precise regulations that demand compliance.

#### **Question 5: Do we have a plan to respond to a security breach?**

In the process of designing and implementing information security in an organization, a critical aspect that can sometimes get lesser attention is that of incident response. While the security program will define how you will achieve information security, it isn't written

---

---

in stone that your organization will never be breached. Your organization must have an incident response plan in place which defines exactly what will be done in the face of a security incident, who will do it, and how the organization's normal functioning will be restored. Once documented, the precise roles and responsibilities need to be communicated to the incident response team identified. Ensure that regulatory compliance procedures are taken into account as well so that reporting requirements are met and evidences are retained using formal chain of custody procedures that allow the evidences to be permissible in a court of law at a later time, if the need arises.

### **Question 6: Should we outsource?**

A long-debated question of whether and how much information security should be handled in-house still has no right answers. The best way is to look at this question based on your own specific organizational size and needs. Overall, the economics of hiring expert help for information security needs undoubtedly offers serious cost advantages, particularly considering that the organization can still maintain control by retaining a small, yet

significant, information security function in-house. However, it is important to choose the expert carefully and ensure that the outsourced organization is not only technically gifted but can also view information security in the light of overall business impact and regulatory compliance.

Security must begin at the top of an organization. It is a leadership issue, and the chief executives, including CFOs, must set the example.

*Silka Gonzalez is president of Enterprise Risk Management, a leading provider of IT security and risk management services. Silka can be reached at [info@emrisk.com](mailto:info@emrisk.com). Matthew Oakes is president and chief executive officer of Direct Insite, a leading global provider of on-demand accounts payable, accounts receivable and payments solutions. Matthew can be reached at [matthew.oakes@directinsite.com](mailto:matthew.oakes@directinsite.com).*

---

*For more information, visit [www.directinsite.com](http://www.directinsite.com) or call 631-873-2900.*