TROFI SECURITY®
INTELLIGENT INFORMATION SECURITY

InfoSec and IT | Strategic Partners, not Tactical Clones

X-factors in Information Security | Executive Series

Michael Trofi, CISSP, CISM, CGEIT | Partner/Co-Founder for Trofi Security
Rod Saunders, CISM | vCISO/Partner for Trofi Security

Consider the following: Since the advent of software development, more than a half-century ago, it has been a standard and accepted practice to separate the roles of “development” and “quality assurance”. While based, in part, on principles put forth a quarter-century before that, by such people as W. Edwards Deming and Joseph Juran, the reasoning was not rooted in the idea of “make” vs “break”. Rather, it was rooted in the inherent differences in strategy and execution of the two roles, which necessarily had to come together to ensure the outcome matched, as closely as possible, the original design.

Fast forward 75 years (give or take 1 or 2) to today, and it’s surprising to find that many, if not most, executive managers still do not properly understand how those concepts can help their broader business strategy. This is especially true in the areas of information technology (“IT”) and information security (“InfoSec”), where that separation of roles has never been more important to successfully managing an organization’s information risk. Yet, the traditional view remains one of “leveraging the overlap in resources” given the number of common physical components between the functions, such as routers, firewalls, antivirus, etc.

With an ever increasing number of headlines announcing yet another breach, and the expanding admission by organizations across virtually every industry that they have been the target of successful cyber-attacks, when will executive managers finally realize the “traditional view” is no longer effective at protecting information assets?

Let’s be honest, today’s reality is one in which cyber criminals are staying a step ahead of most organizations’ ability to properly protect their information assets. Forget the headlines. One simply has to look at the rapidly growing number of marketplaces where data-stealing exploit kits are not only being bought, but stolen information is being sold in ever larger quantities, and at an ever growing profit. This, in and of itself, gives the cyber criminals the upper hand. They have a very direct and powerful incentive: making money. This incentive is made even more powerful by the fact that most organizations still consider InfoSec to be an expense (i.e. spending money), for which it is difficult, if not impossible, to calculate a return on the investment. Is it any wonder the cyber criminals are winning?

For organizations to start turning this tide of cybercrime in their favor, they need to begin understanding that protecting information assets requires a comprehensive, multi-disciplined approach, across all aspects of their business. There is no “magic bullet” in the world of information security. It takes a well-formulated combination of organizational, architectural, and operational strategies coming together to create multiple layers of defense against would-be attackers. And, as more and more companies are realizing, achieving this level of maturity simply cannot be done without separating the roles of IT and InfoSec.

For the very same reasons software development and quality assurance have been separated for so long, IT and InfoSec roles have very different, yet ideally aligned, priorities. IT professionals are focused on the functional execution of an organization’s business; on enabling the organization to achieve its goals from an operational standpoint. That means finding and deploying technology tools and platforms that enhance communication, facilitate information sharing, and support more efficient business processes. Functionality, availability, performance, and accessibility, at a cost that achieves a desired return on investment, are the paramount priorities.

InfoSec priorities, on the other hand, must be orthogonal to those of IT. The priorities for InfoSec professionals are to evaluate all information security risks to the business, whether directly related to the technologies being adopted by an organization, the business processes they support, or the people responsible for those processes, and then formulate ideal defense strategies against those risks. With the advances in sophistication in attacks and an ever widening footprint of attack vectors, today's risk environment is very different than it was even a decade ago. Perimeter defense is no longer enough when untrained employees are unknowingly (or knowingly) ushering malware into the corporate network by browsing the Web or opening an email attachment. Today's security defenses need to cover the perimeter, protect the endpoints, control physical access, and thwart social engineering. Building an effective defensive strategy for meeting the security needs of this new landscape requires corporations to appreciate that information security is not solely a function of information technology, but a strategic component that pervades every department in the enterprise.

Taking that a step further, consider the article that appeared in CSO Magazine in 2013[1], in which the case is made that even a dedicated CISO role is not sufficient to cover the broad range of information security responsibilities, and the myriad levels within an organization those responsibilities must be applied. Instead, the article proposes that the InfoSec role should really be considered at least 3 focused and distinct roles:

[1] “Who should the CISO report to?”, John Kirkwood, CSO Magazine, 03/16/2013

- **The Technical Information Security Officer (TISO) -** The TISO specializes in technical security issues, operations, and monitoring, including managing firewalls, handling intrusion-detection and intrusion-prevention systems, and more. Also, the TISO coordinates and manages technical policies and controls, and assessment activities.

- **The Business Information Security Officer (BISO) -** The BISO specializes in InfoSec issues related to the business, such as how to securely implement customer-facing technologies and appropriately protect customer information. A major responsibility of the BISO is to ensure that the business unit or division understands that InfoSec is a business requirement like any other result. This person also assists in the implementation and translation of enterprise security requirements, policies and procedures.

  Additionally, the BISO should perform business security assessments or, at a minimum, coordinate the resolution of identified business-related security issues. Ideally, there should be a BISO embedded in every major business unit or division, and he or she should report to business management. However, due to size and budgetary constraints for many organizations they may not be able to accomplish this goal. With that in mind it is even more important to segregate the CISO from TISO like functions so he/she can concentrate on the BISO/SISO type roles to bring uniformity to the overall security program.

- **The Strategic Information Security Officer (SISO) -** The SISO specializes in translating high-level business requirements into enterprise security initiatives and programs that must be implemented to achieve the organization's mission, goals and objectives. The SISO must coordinate with the operations officer and the BISO to ensure appropriate progress. The SISO should also be responsible for metrics, dashboards and executive reports, and for presenting assessments of the state of security in the enterprise to the board of directors. The SISO should report to an executive management function such as the chief risk officer, chief operating officer or chief legal counsel, or to an executive management committee.

So, if one dedicated InfoSec role isn't enough, then combining the InfoSec role with the IT role, or any other, clearly ignores a fundamental reality that InfoSec has an essentially different mission than any other role, and that by combining it with another role creates not only a

distinct conflict of interest, it short-changes either role from being able to focus on its own specific priorities.

Splitting the roles, however, requires specific attention and focus as well. While it is important, for what should be obvious reasons at this point, to provide InfoSec with its own autonomy, budget, and executive voice, it is probably even more important to ensure this role (or roles, from above) is created in a manner that ensures a very close relationship with all other roles within the enterprise. As stated earlier, the InfoSec role has functions that pervade every other department in the enterprise, which means this role also has to work in concert with every other role in order to minimize, as much as possible, any negative impact on the efficiency, stability, and performance of the business.

But, let's be honest again. Applying information security technologies, components, and protections within an enterprise will never by "transparent". The hope, is to ultimately make them "seamless", such that the protections an organization designs work fluidly with the operations of the business, and create the least possible negative impact on those operations. To that end, the InfoSec role must be both a strategic and tactical partner to every other role/department in the organization. To be successful in that responsibility, this role requires individuals who are experienced with, and determined to be, strong value-added partners with other executive and operational managers within the enterprise. It is only when that level of collaboration and execution are achieved, will the benefits and rewards of dedicating an InfoSec role within the enterprise be achieved.

Of course, the proof is in the pudding, as they say, and that pudding must be measured in terms of its ability to add value to an organization in a manner executives and Boards will understand. As expected, as more studies are completed on the impacts on organizations of splitting these roles, there is a growing volume of empirical data supporting the argument that having the InfoSec role reporting outside of the IT office, while providing the InfoSec role a meaningful voice within the organization, does, in fact, improve an organization's security when measured against overall enterprise risk, operational downtime, and financial losses. One might say the pudding is tasting pretty good.

Consider these findings from the 2014 Global State of Information Security Survey, conducted each year, for more than a decade, by PwC, CSO and CIO magazine:

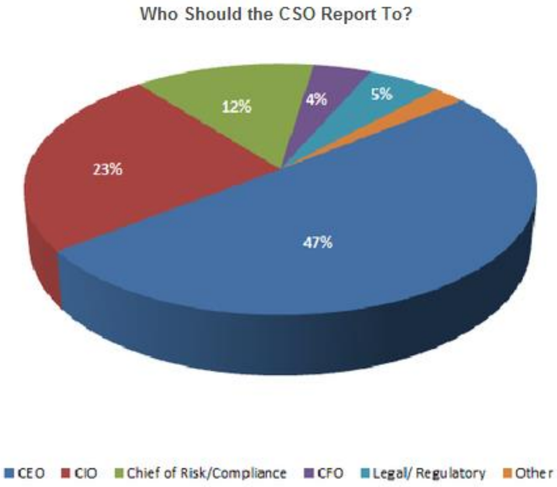
- With more than 9,000 respondents from around the globe, the survey found that those organizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber security incidents than those organizations in which the CISO reported to the CEO; and

- When the CISO reported to the CIO, financial losses were 46% higher than when the CISO reported to the CEO. In fact, having the CISO report to almost any position in senior management other than the CIO (Board of Directors, CFO, etc.), reduced financial losses from cyber incidents.

A 2014 survey published at CSOonline resulted in the same basic conclusion: "Reporting to the CEO or the Board of Directors, instead of the CIO, significantly reduces downtime and financial losses resulting from cyber security incidents."[2]

Further support for this idea was published in 2014 in an article online at Dark Reading reporting the survey results of industry respondents about the ideal reporting structure for ISOs within the enterprise. In this survey, respondents were asked to be specific as to how the InfoSec role should be positioned within the enterprise, and to whom they should ideally report.

"Based on recent studies on whom should the top security officer should report, more than 75 percent of the respondents placed security outside the traditional domain of the CIO, reporting, instead, directly to the chief executive (47 percent) or others with C-level titles in charge of risk or compliance (12 percent), legal (5 percent) or finance (4 percent). Only 23 percent of community members who took our poll endorsed the hierarchy of CISO reporting up to the CIO."



"The results should come as no surprise. In today's threat landscape, the emerging view seems to be that there is an inherent conflict between managing enterprise IT systems that increase productivity and profits (CIO) and protecting sensitive corporate data and customer personal identifiable information (CISO)."[3]

[2] "Maybe it really does matter who the CISO reports to", Bob Bragdon, CSOonline, June 20, 2014

[3] "CSOs Need A New Boss", Dark Reading, Marilyn Cohodas, 8/22/2014

From experience, not every organization is the same and no one model will work everywhere; however, there is a lot to be said for having information security leadership report to the top of the house, and not to the CIO: the reduction in conflict of interest between the CIO’s objectives and the CISO’s objectives, the ability to escalate issues to the top of the house, as well as, the opportunity it provides for security to influence corporate leadership. It's critical that the CISO and the CIO work together towards the common goal of aligning security with the business objectives and risk appetite of the organization, but it's clearly best done when they are peers with an equal voice in the discussion.

So, what keeps organizations from taking this step?

As expected, it boils down to two basic reasons. One is awareness. Most companies are so focused on either their over-arching strategies or their day-to-day operations, that adding another dimension to their mix is the last thing on their mind. Of course, this quickly changes the first time they find themselves in the headlines, or have to contact their customers, because critical, personal information has been breached.

The second reason is “budget”, and the belief that “we just can’t afford” to dedicate the InfoSec role. This is obviously a much greyer area. There is no question that the choice to dedicate an InfoSec role will require an investment; however, given the sheer numbers in privacy breaches and reputational damage within all industries, much less the growing body of evidence that there is money to be “saved” by adding this role, it is also clear that “some” level of investment is warranted by just about all organizations.

So, what is right for your organization? The answer lies somewhere within the understanding of just exactly what your organization does. This understanding may well be resident within your ranks already. This understanding may well be waiting to be understood by a good information security partner. Many smaller organizations are finding great success with “virtual” information security resources, who provide comprehensive security services to their organization, but on a part-time basis. Regardless, prudent organizations are starting to ask the questions, and seek the answers, as to how to better protect their information assets. Splitting the InfoSec and IT roles is the first step. The next…well…to be honest one last time, it depends on how much your organization believes that your client’s trust is as important to you as the services you charge them for.

What’s your next step?

About Trofi Security

Trofi Security, originally Trofi Systems Solutions, was founded in 1999 to provide IT security advisory and compliance services to client organizations, as well as to serve as a security-community contributor in the development of cross-industry security best practices. Trofi Security's methodologies and expertise have been used successfully on more than 1000 projects, nationally, during its 15 year history.

Trofi Security has grown to become one of the preeminent thought-leaders and advisories in the Information Security industry, across a broad range of client industries. With offices in Colorado, Washington D.C., Rhode Island, and Los Angeles Trofi Security has a national capability to help client organizations evaluate, strategize, develop, and test comprehensive information security programs designed to address their specific risk and regulatory environments.

For more information about Trofi Security visit us online:

trofisecurity.com | linkedin.com/company/trofisecurity | @trofisecurity