



L'EVOLUZIONE DEL RUOLO DEL CISO IN AZIENDA

Raoul Savastano

Chi è il CISO?



Anche se non espressamente previsto, tutte le organizzazioni hanno un CISO (Chief Information Security Officer). La figura del CISO spesso coincide con il CIO, CSO ed in alcuni casi con il CEO, anche qualora ci sia un Information Security Officer / Director.

L'ampiezza e la profondità delle tematiche relative all'Information Security sono tali da far ricadere inevitabilmente l'autorità e le responsabilità richieste in capo ai livelli executive. Pertanto la responsabilità legale si estende di default fino al top management e ai Consigli di Amministrazione.

Un mancato riconoscimento di queste tematiche e la mancanza di un'apposita struttura di governance potrebbe quindi far sì che il senior management aziendale non sia consapevole delle proprie responsabilità. Generalmente ne consegue una mancanza di efficace allineamento delle attività di security con gli obiettivi di business.

Il ruolo del CISO



Il ruolo del CISO si è nel tempo evoluto passando da un focus principale rivolto alle attività tecniche verso una maggiore attenzione ed integrazione con attività di business, con particolare riferimento alla gestione dei rischi IT (business continuity management, privacy, data protection, ecc.) e alla Compliance (SOX, Legge 262/05, ISO27001, ISO25999, PCI-standard, ecc.).

I più recenti framework identificano infatti un ruolo apposito per il CISO e prevedono un'integrazione delle attività ad esso specificatamente assegnate in un contesto più ampio che coinvolge tutti gli executive.

Ruoli e responsabilità



Al fine di stabilire un collegamento diretto e costante tra le strategie di Security e gli obiettivi aziendali le leading practice definiscono un modello organizzativo che attribuisce a diversi livelli di Senior Management specifiche responsabilità in tema di sicurezza.

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Integration
Board of directors/ trustees	Set direction for a demonstrable alignment.	Set direction for a risk management policy that applies to all activities and regulatory compliance.	Set direction for reporting of security activity costs and value of information protected.	Set direction for reporting of security effectiveness.	Set direction for a policy of knowledge management and resource utilisation.	Set direction for a policy of assuring process integration.
Senior executives	Institute processes to integrate security with business objectives.	Ensure that roles and responsibilities include risk management in all activities. Monitor regulatory compliance.	Require business case studies of security initiatives and value of information protected.	Require monitoring and metrics for reporting security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all management process functions and plans for integration.
Steering committee	Review and assist security strategy and integration efforts, ensure that business unit managers and process owners support integration.	Identify emerging risks, promote business unit security practices, and identify compliance issues.	Review and advise adequacy of security initiatives to serve business functions and value delivered in terms of enabled services.	Review and advise the extent to which security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	Identify critical business processes and management assurance providers. Direct assurance integration efforts.
Chief information security officer	Develop security strategy, oversee the security programme and initiatives, and liaise with business unit managers and process owners for ongoing alignment.	Ensure risk and business impact assessments, develop risk mitigation strategies, and enforce policy and regulatory compliance.	Monitor utilisation and effectiveness of security resources and reputation and the delivery of trust.	Develop and implement monitoring and metrics collection and analysis and reporting approaches. Direct and monitor security activities.	Develop methods for knowledge capture and dissemination. Develop metrics for effectiveness and efficiency.	Liaise with other management process functions. Ensure that gaps and overlaps are identified and addressed.

Board of directors / executive management

Definizione dell'Information Security Governance

Senior Executives

Assicurare l'implementazione efficace della governance e definire gli obiettivi strategici in tema di security

Steering committee

Assicurare che tutti gli stakeholder coinvolti direttamente o indirettamente sulle tematiche dell'Information Security siano coinvolti nei processi decisionali

Fonte: ITGI, Information Security Governance: Guidance for Information Security Managers, 2008

Principali trend organizzativi



La crescente importanza della figura del CISO è inoltre confermata da recenti survey e ricerche di mercato.

Uno dei più chiari trend si rivela essere l'incremento delle posizioni di gestione della sicurezza in azienda:

- Chief Information Security Officers (dal 29% nel 2008 al 44% nel 2009)
- Chief Security Officers (dal 27% al 41%)
- Chief Privacy Officers (dal 21% al 30%).

	2008	2009
Employ Chief Information Security Officer	29%	44%
Employ Chief Security Officer	27%	41%
Employ Chief Privacy Officer	21%	30%
Have an overall information security strategy	59%	65%
Have an identity management strategy	41%	48%
Link security to privacy and/or regulatory compliance	44%	53%
Conduct compliance testing	44%	51%
Conduct personnel background checks	51%	60%
Conduct risk assessments via third parties	26%	36%
Use tiered authentication levels based on user risk classification	36%	42%
Integrate privacy and compliance plans	36%	44%
Have incident response process to alert third parties handling data	27%	35%
Automated account de-provisioning	27%	38%
Security event correlation software	35%	43%
Biometrics	19%	30%

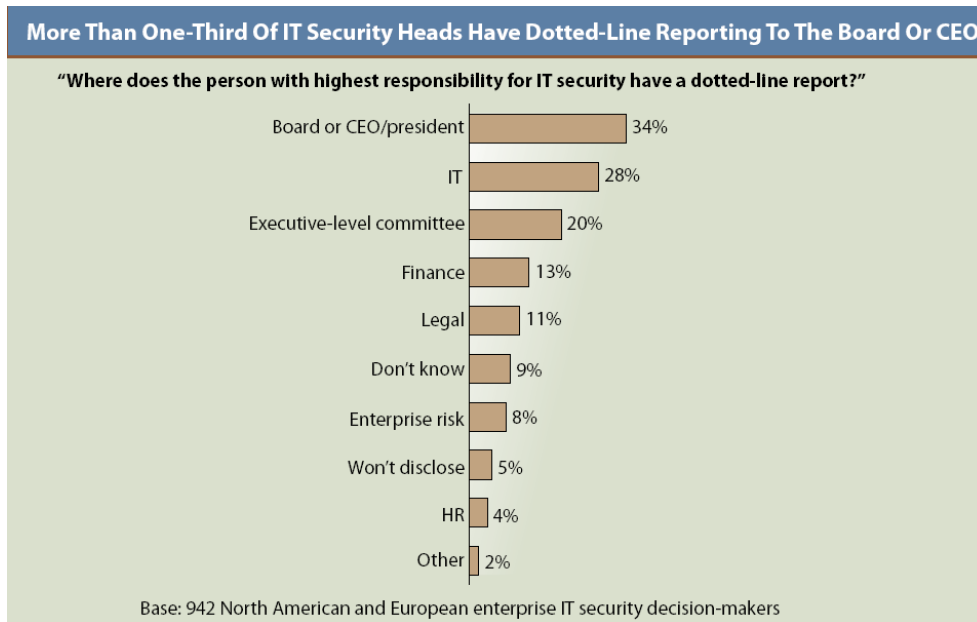
Fonte: PWC, The Global State of Information Security Survey, 2010

Livelli di riporto



Le ultime ricerche mostrano come i decision-maker in ambito di IT Security abbiano una linea di riporto che va orientandosi sempre di più verso livelli gerarchici non IT, in particolare verso i Consigli di Amministrazione, i CEO, i presidenti o le commissioni di executive.

I gruppi di IT security rimangono tuttavia principalmente o completamente responsabili della sicurezza infrastrutturale, della gestione delle minacce e delle vulnerabilità logiche, della sicurezza fisica e della compliance, lasciando poco tempo da dedicare ad iniziative strategiche.



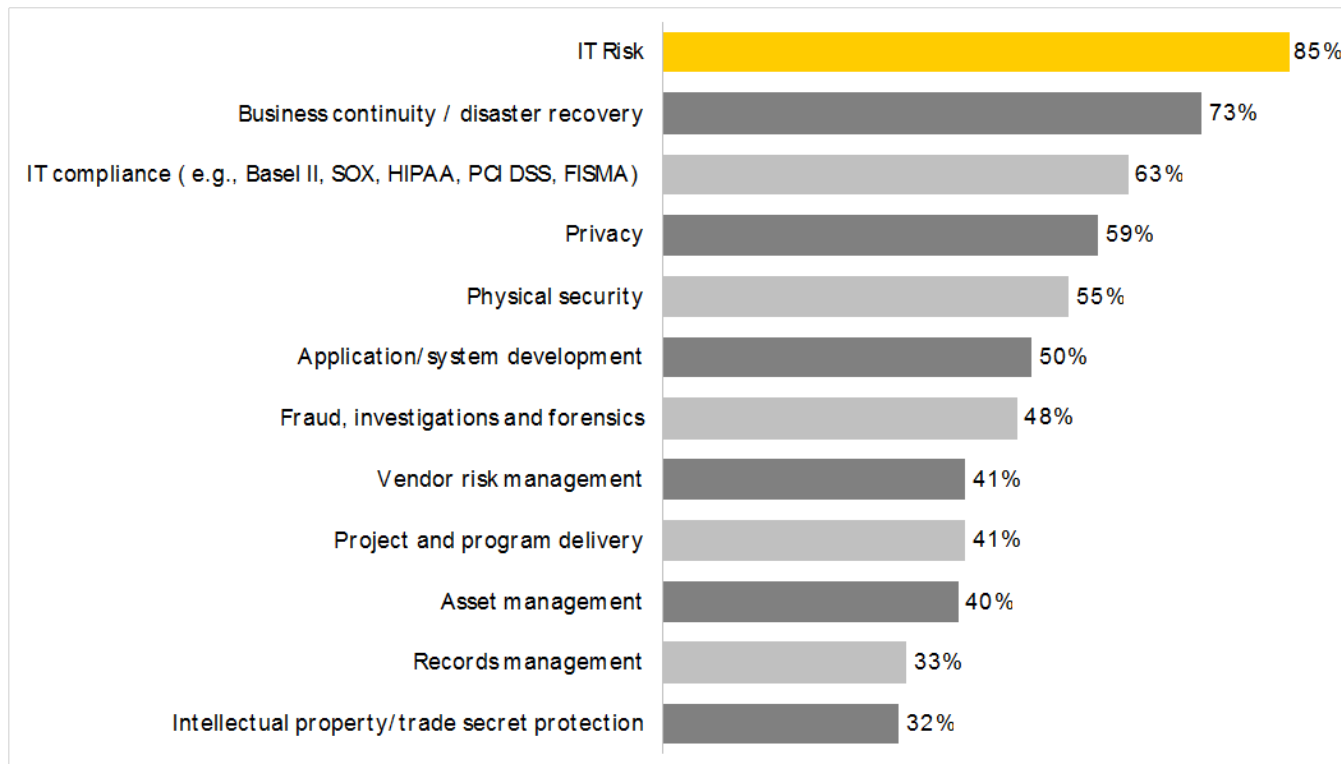
Fonte: Forrester: *The State Of Enterprise IT Security: 2008 to 2009*

Aree di responsabilità



Il riporto verso livelli gerarchici non IT è strettamente correlato alla varietà delle aree di cui la funzione Information Security risulta completamente o parzialmente responsabile.

Which of the following areas is the information security function in your organization either fully or partially responsible for?



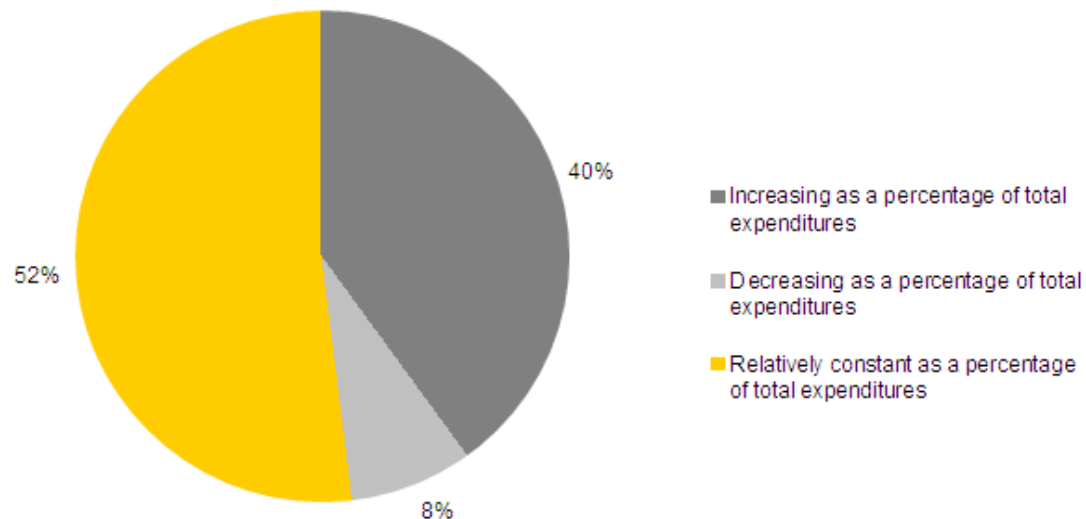
Fonte: Ernst & Young's 12th annual Global Information Security Survey, 2009

Budget e priorità di spesa



Nonostante la crisi economica abbia ridimensionato i budget di spesa per la sicurezza IT per il 2009, la maggior parte delle aziende prevede in ogni caso di non ridurre o addirittura di aumentare i budget di spesa.

Which of the following statements best describes your organization's annual investment in information security?



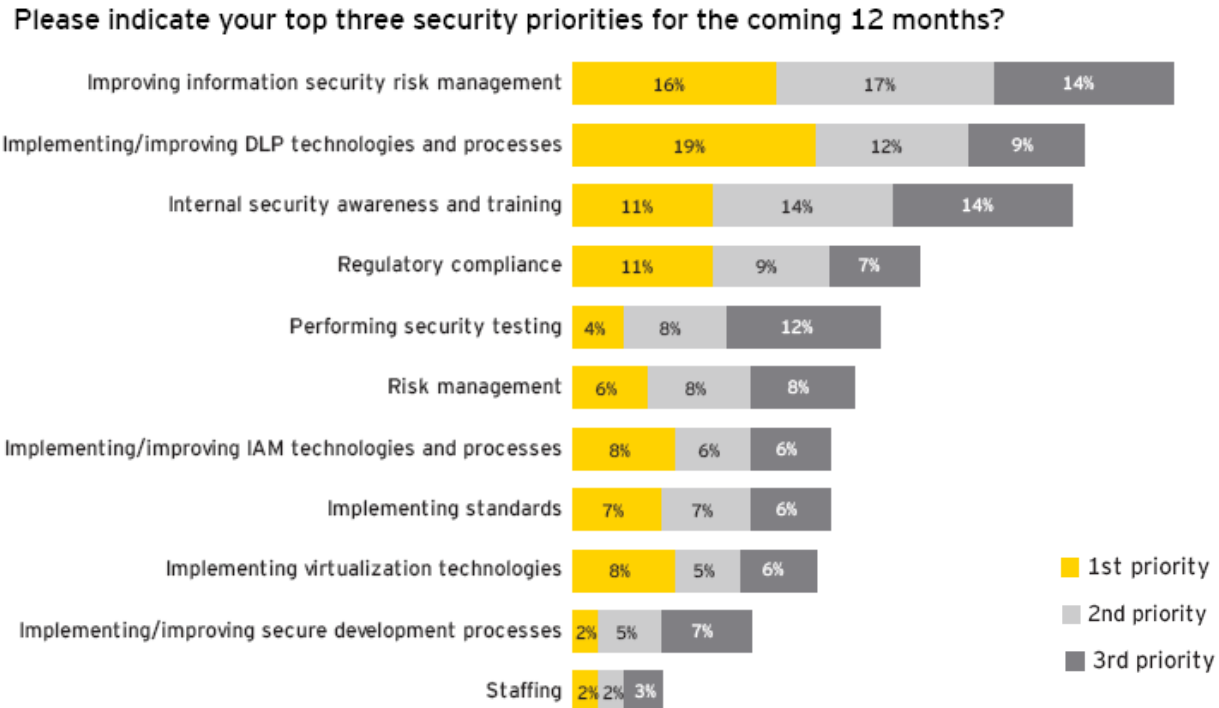
Shown: percentage of respondents

Fonte: Ernst & Young's 12th annual Global Information Security Survey, 2009

Aree prioritarie di intervento



Le aree prioritarie di intervento si rivelano essere l'implementazione / il miglioramento dei processi e delle tecnologie a supporto della protezione dei dati e del miglioramento dei processi di gestione del rischio relativo alla sicurezza informatica



Ernst & Young's 12th annual Global Information Security Survey, 2009