Who really owns risk in your organisation?

In their annual compensation survey, across the regions of Asia, UK, Europe, Middle East, and North America, SSR® Personnel incorporating Executive Profiles review over 4,000 profiles and interview a number of respondents from the senior and mid executive levels to understand corporate priorities over the medium horizon.

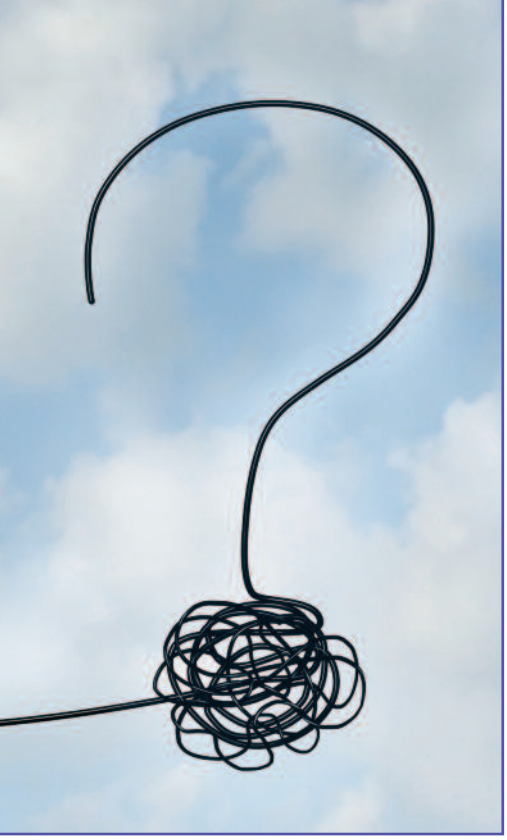
The trend for most corporate security functions is that salaries in 2014 have increased by up to 3.2%, bonuses have increased year-on-year in value by 25% and those who are part of the executive management long term incentive scheme have averaged a bonus pool payment of 45% of salary. Executive salaries across many functions remain relatively flat amongst many organisations in Northern Europe, whilst salaries in Southern Europe have been subject to reductions or serious restraint. Many fiscal policy sources envisage that it will take 2 years to return to pre-2008 income levels, taking into consideration inflation and increased taxation representing a 30% drop in real terms, against a back drop of high unemployment.

In Asia and the Middle East the downgrading of expatriate terms, such as schooling and closed community accommodation, is promoting the employment of local professionals at one of the fastest rates ever seen. Whilst 2013 was the year that we learnt in Europe that food security was seriously lacking, 2014 has seen Cyber security flash up on most company board members' dashboards. With Europol estimating that global online loss to governments, companies and individuals is €244bn per annum, countries are taking notice and action with the establishment of Cyber Offices.

Once a victimless crime, online fraud is rightly now a priority within many law enforcement jurisdictions. In 2014 the US Conference Board reported CEOs now rate 'Cyber Risk' as one of the 'hot button' issues in their businesses, over 50% consider that they lack the expertise in-house to deal with it. In CEO opinion surveys, security functions were considered by the majority to not be in tune with the business or understand what keeps the C-suite up at night or at least waking early.

Convergence for quality

The ownership of cyber risk is hotting up with many in the physical space losing out to IT administrators. Articulation of the issues and subject matter requires those in the physical space to wake up and 'smell the coffee', otherwise their share of board room influence will be limited. CSO and CISO practitioners should understand that cyber remains a key dashboard indicator for non-executive directors. Why is this key?
IT drives the technology competitiveness and business imperatives, faster, and perhaps



smarter. But there are stark differences in the way organisations deal with events: from a recent CSO survey less than 27% have an in-house forensic capability; over 60% have an investigations function mainly through analysts and less than 11% would classify these as cyber investigators. Entry-level cyber analysts from the public sector fraud investigations or intelligence command starting salaries of £50k (€75k). Most business surveys point out that the highest risk to organisations remains the insider. In the Quocirca 2014 report 41% of organisations rate the ignorant user as the biggest risk to their business, many IT departments continue to spend the majority of their budgets on the outsider, of which most of the actual threat is from viruses that will enter through inappropriate web surfing and directed malware.

In Europe we have had a number of incidents where banking organisations' IT spending, even those under regulatory oversight, has been very poorly invested, creating organisations that can be a danger to customers and shareholders. Fraud prevention in the physical aspect is around robust approvals, understanding geographic trends, criminal demographics and the ability to respond quickly. In a recent SSR® assignment, using analysts with standard investigations software, they identified that an organisation's online fraud was being enacted through a very small geographical footprint. Providing timely intelligence event streamers showed an organised group was purchasing stolen credit cards from the UK and USA, but their 'purchases' were being completed from URL's in Latvia and the Ukraine, stealing more than €30m.

Convergence in the parlance of business equals savings.

Many corporations are having this discussion, across the broadest range of services. Maybe through Facilities Management specialists, outsourced probably, but trying to take out cost.

Many respondents to this year's survey are concerned that these processes remove specialist skills where procurement does not value the key deliverable of service integrity. Vendor organisations are not accepting that they have an opportunity to be the knowledge providers. We see a strong indication that from 2016 many outsourced contracts will revert back to in-house, or at least be separated from bundled processes, with greater client management oversight. Which will send us back to the business cycle pre 2008.

There is also a realisation that in the drive for flexibility in their cost base through employing contractors, many organisations have exposed their 'crown jewels' to non-employees. Certainly within most compliance regimes this practice is frowned upon. It certainly is considered, with some informed opinion, that if Snowden had been an employee he would not have been able to steal the sensitive information he did, not because he would have had more loyalty, but because at his pay grade no employees had that level of access.

In security whether it will be CSO to CISO roles or vice versa that will be merged is out with the jury at the current time, but the best chance for survival is envisaged for the individual that delivers the best business case. SSR® observing on a global basis can predict that this will be a close corporate call but certainly the non-executive board members will be a key influence.

Bonuses are rapidly returning

Good news across a number of sectors including financial sector, extractives, pharmaceuticals and logistics. Predictions are that in 2015 bonus pools will exceed those of 2008. The UK Office for National Statistics predicts that employees in the FS sector accounting for 3.8% of total workforce picked up 30% of the £40bn paid in year to April 2014, which is 10 times more than the average bonus paid across both the public and private sectors.

Are those from the public sector more risk averse than private sector colleagues?

Speaking at a recent seminar a leading CSO articulated the differences between those from public and private sectors. He reasoned that those in the public sector were subject to such media oversight and investigation that their organisations had become risk averse. Does that make them good leaders when transferring to the private sector? Whereas those graduating through from the private sector, identified in the post-mortem of the banking crisis as working in compliance & audit, accepted increasing levels of risk as part of their organisation's evolution – when many knew this was plainly wrong.

Whilst the banks are being reformed by being fined billions of dollars from quasi regulators, board room compliance will not be changed until those in charge are prosecuted. Was paying US$16bn by BoAML more helpful to market order than prosecuting senior managers at Merrill Lynch? This might help prevent the next financial bubble from bursting, probably in Asia.

Current projections for all European economies to rebuild to 2008 levels of activity by 2016 look to be promising, certainly outside the Eurozone, but we need to see confidence return, which will free up corporate budgets for investment.

If you are a survivor of the richest recession ever experienced to return to sustained growth we need a corporate mind change from cost cutting to maintain profitability, to a return to investment-led strategies for profitability. This certainly affects the corporate security function where it sits in corporations as a cost, rather than a revenue enhancing service.

Mergers and Acquisitions, limited public offerings and equity sales will reach pre-crash levels by the end of 2014 for the UK, USA and Asia exchanges. In the era of more for less those security departments that are providing services to the M&A teams, such as due diligence, are mitigating risks for the organisation that should have learned the lessons of previous excesses. Whilst most boards want a big bang purchase, many US corporations seeking cheaper tax regimes, inversion can increase ROI by 20% as they re-domicile from the US 35% corporate tax rate. It is estimated that US corporations hold in non-taxed foreign reserves 2 times the current US fiscal deficit. Yet again corporate restructuring will look at what can be cut.

Are you relevant on the Board room dashboard?

Security professionals that do not have indicators on the dashboard are irrelevant to the organisation. How can professionals just allow their function to become absorbed into a mire of functions that cannot demonstrate value? This is probably because the organisation has not had a security champion before and from a senior management prospective has a perceived lack of professionalism. The Chartered Security Professional Register has nearly 100 registrants reaching to the 4 corners of the globe.

Continued on page 13 with a European salary survey for 2014-15.

continued from page 11.

This is not a degree; this is peer review, understanding what makes your organisation and your professionalism stand out.

This is perhaps the start of a doubling of membership every 2 years, promoted by the Security Institute. But this is key for the corporate sectors to demonstrate their professionalism to the C-suite.

The successful applicants are those that understand the corporate business environment, and increasingly the public sector.

How does that translate?

A common trait has to be that leadership is paramount (a person to be relied upon in a time of crisis), a personality that is open (understanding the options), knowledgeable, understands all areas of the firms operation (when does Ebola become our problem?).

So what keeps your CEO awake at night?

From the Conference Board 2014 survey they found that the top 5 CEO issues were: Retaining and attracting talent - most thought that their HR processes need refining to keep pace with change; Customer relations - now in the top 5, up from 5 years ago; Innovation - with so much competition, you could be a market leader today, 3rd place tomorrow with an inflated cost base to shed; Operational excellence - delivering the same high standards in a global market; Corporate brand and reputation - with so many stakeholders and regulators.

Are you aligned or interwoven into the corporate structure?

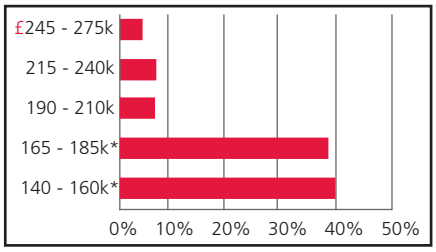
If you wanted to be a success you used to speak of alignment with the company's vision; now corporations have moved on, you now need to be 'interwoven' into the corporate structure and key to this is making the Board understand that, in today's world having capable business security is one way of keeping risk controlled.

How, from a security prospective, do you influence all those thoughts and processes?

Successful professionals will state: have concise briefings; intelligence reports that reflect the operation of the business; keep people at the heart of your motivation. Generation Z will soon be arriving work with a totally different set of personal priorities; is email and Facebook going to still be relevant? How will we develop understanding about employment longevity with a generation that does not want long term employment commitment? Utterly polarised from 50 years ago we need to manage these groups until they take over!

Peter French, MBE
Managing Director, SSR Personnel
www.ssr-personnel.com

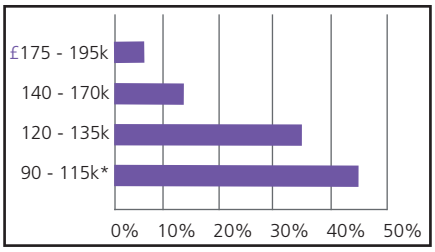
EUROPEAN SALARY SURVEY 2014 - 2015



CHIEF SECURITY OFFICER

Responsible for policy, executive board briefings. Dotted line or direct responsibility for subsidiary CSO / Head of Security position. Oversight budget responsible of £30m+. Revenues of £2bn+.

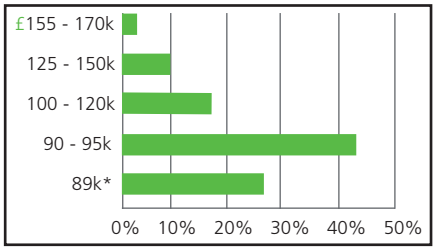
* Included in Executive Long Term Incentive Plan



INTERNATIONAL CSO / HEAD OF SECURITY

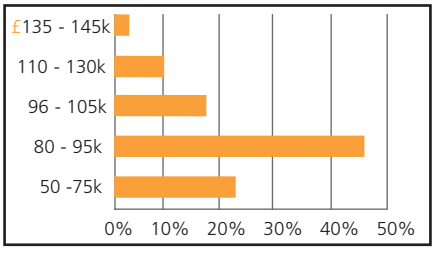
Responsible for delivering localised policy, executive board briefings. They are a driver for change and service expansion.
Budget responsibility £10M – £30m.
Revenues of £1bn+.

* Included in Executive Long Term Incentive Plan



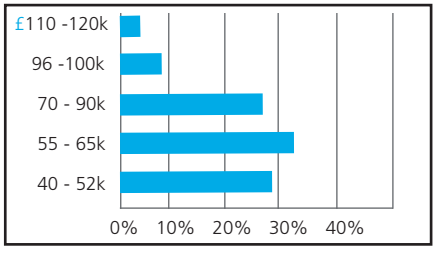
EMEA SECURITY HEAD

Regional policy development, executive reporting, promulgating corporate policy, overview of physical and intellectual protection.
Budget responsibility £10m – £30m.



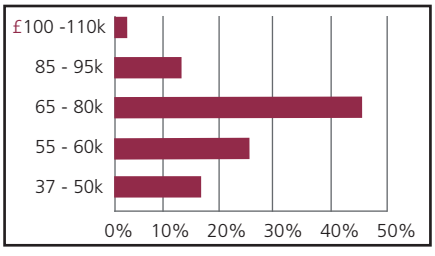
EUROPEAN SECURITY HEAD

Regional reporting, policy implementation, promulgates corporate policy. Responsible for physical and information security.
Budget responsibility £5m – £10m.



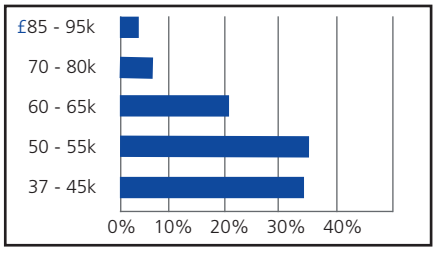
NATIONAL SECURITY HEAD

Responsible for all physical aspects of corporate security and maintaining standards across an estate.
Budget responsibility £2m – £10m.



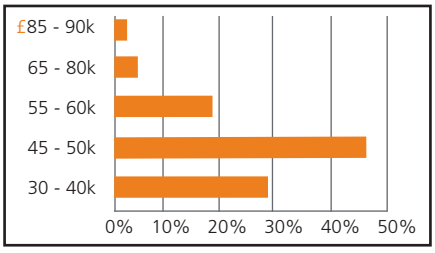
SENIOR INVESTIGATOR

Responsibility for more than one country's operations. Active across all security breaches, due diligence, product diversion, counterfeit and auditing functions for the corporation.



MAIN HQ SITE SECURITY MANAGER

Physical and information protection, proactive, local policy implementation and development.
Budget responsibility £2m – £5m+.



REGIONAL INVESTIGATOR & DUE DILIGENCE MANAGER

Supply chain management, implementing corporate procedures.