FIFTH STEP WHITE PAPER

Navigating the Cybersecurity Storm while Building Enduring Trust

Cyber security resources are in high demand. The challenge for organisations is that there is a shortage of the right kinds of resources for security roles. In this white paper I examine the reasons for the growth in cyber roles and the rise of co-sourcing as a preferred option for today's CIOs.

Postings for cyber roles have grown by 91% in the period 2010 – 2014 in comparison to 28% growth for general IT postings. Indeed, cyber roles also have a salary premium of around $6,500 over general IT roles.

Financial services and healthcare (unsurprisingly with their focus on sensitive information) have seen some of the largest increases in roles being posted, up by 131% and 118% respectively. Security roles tend to have a higher demand for experience, with 48% of roles requiring a minimum 3-5 years of experience.

> "64% of organisations of all sizes lack the time to manage all of their security activities*"

The impact

64% of organisations of all sizes lack the time to manage all of their security activities*. This figure also tallies with Fifth Step's own figures that say 64% of our engagements are as a result of a lack of bandwidth within the organisation.

Meanwhile, 45% of organisations lack the ability to test existing security plans fully and 38% of organisations say they lack investment in creating effective security processes.* Organisation therefore do not have the time or the ability to do the basics. As a result they are doomed to continue to repeat their mistakes, leaving them more exposed to cyber-attacks.

In today's environment, organisations are under an increasing amount of scrutiny from regulations and from global regulation (FATCA, SOX, Solvency II, HIPPA, PIPPA, GDPR, Data Protection, NIS and a plethora of others), requiring them to be able to not only protect their assets but evidence to third parties that they're doing so.

Ultimately, over stretched security departments may be leaving their organisation's vulnerable both to cyber-attack and regulatory action.

Cyber security is different

Hackers, malware and other attack vectors often don't discriminate between the size, industry sector or other variables of organisations. Everyone is fair game. This is a constantly evolving threat. To my knowledge, the evolution of house-breaking techniques has really not changed hugely in the last couple of hundred years, however, cyber burglaries or cyber squatters are constantly evolving.

Unlike other risks that organisation's face and mitigate, Cyber knowledge is always on the move. To stand still in information security and cyber security is to become more vulnerable relative to the market. You don't want to be a comparatively soft target. Remember that security teams are often small - 66% of organisations have a team of 10 people or less.* While not unique to information security, the cross business aspects of this area makes it different, and often more complex.

* Statistics from the SC Magazine MarketFocus May 2016 – Co-Sourcing SIEM.

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com

Magnifying cyber resources

When it comes to leveraging your cyber resources it is important not to forget the technology, however, the key point to make here is do not simply continue to do what you have always done. That can just lead to "busy work" and essentially you can't solve all the problems in security just by employing technology, no matter how state of the art it is.

The security field is one that is ripe for greater adoption of technology tools to magnify the abilities of security teams – an obvious starting point is EventTracker's website, which offers to process hundreds of millions of discrete log messages to deliver vital and actionable information. Organisations such as this claim to enable businesses to identify and address security risks, improve IT security, and maintain regulatory compliance requirements with simplified audit functionality.

Under use of technology solutions, or doing what you've always done can lead to work that keeps a person busy but has little value in itself. People used to run a disk defrag on a regular basis, now the computer OS takes care of this for us. Resourcing, however, is a spectrum. There are many tools in the tool box so the art is to make sure you use the right ones.

"Organisations need flexibility in their operations. Flexibility to plan, but also to react as situations change..."

Flexibility is key

Organisations need flexibility in their operations. Flexibility to plan, but also to react as situations change, if you only consider one tool in the toolbox then you're limiting your flexibility and ability to get the job done effectively and efficiently. The old saying: When you have a hammer everything looks like a nail, is still very true today.

The least flexible strategy, as follows, in descending order:

- FULL TIME EMPLOYEE
- PART TIME EMPLOYEE
- Consulting / INTERIM
- Consulting / INTERIM
- CO-Sourced Service

Full time employees and part time employees

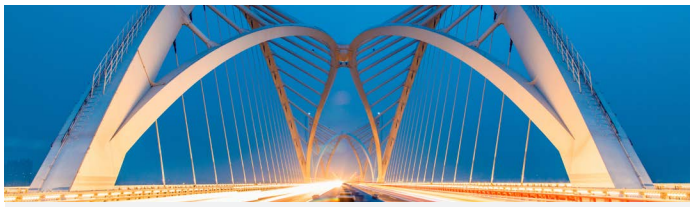
Full Time Employees and Part Time Employees are good for maintaining appropriate in-house resource for core competencies, maintaining a key level of knowledge and understanding and for managing and ensuring organisational responsibility for the functions, be they in-house or provided by a third party.

Consulting and Interim

Consulting and Interim resources are good for specific pieces of work or projects that need to be undertaken, those with a clearly defined deliverable are my personal preference. Interim resources are particularly useful where you know the resource in question. Consulting resources are particularly useful in not only increasing team bandwidth, but also bringing external knowledge, experience and expertise.

Outsourcing

Out-sourcing is particularly good for (non-core) functions where there is a specific function to be performed. Good contract negotiations and vendor management is key to maintaining a good relationship, whilst realising the business case for entering into outsourcing.



"Co-Sourcing allows a greater flexibility than the other options whilst offering many of the benefits of consulting resources."

Co-sourcing

Co-Sourcing allows a greater flexibility than the other options whilst offering many of the benefits of consulting resources. Co-sourcing differs from out-sourcing in that you will look for a co-sourcing partner to work more closely with your teams, augmenting their bandwidth and capabilities.

Co-sourcing is the way to go. It provides organisations with greater flexibility, better cost control and access to a greater breadth of knowledge and resources than any of the other models whether that is hiring full time or part time employees or even the consulting model for doing specific pieces of working. The co-sourcing model, however, is about getting close to an organisation working closely with existing employees supplementing and magnifying their capabilities.

Whereas a consulting arrangement might look at a specific project that can be benchmarked – saying the introduction of new software in a business – co-sourcing arrangement might seek to keep a company secure over a two-year period and evolves working with the existing team. Co-sourcing partners seek to augment existing capability and bandwidth.

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com

Considering the flexible co-sourced arrangement

Many businesses have used a third-party services provider at some point to carry out either part of their cyber security arrangement or offer technical skills that do not exist in-house. Oftentimes, the relationship is good – but when the relationship goes wrong, it can be a challenge for CIOs explaining to the Board why the money they have spent buying in cyber resource has not delivered the required benefits.

There are good reasons why businesses should consider the flexible co-sourced arrangement. When it comes maximising your cyber resources, we can choose from a spectrum ranging from full time employees – a vital resource but the least flexible – to co-sourcing.

Choosing from the spectrum

A useful question that CIOs and IT departments should be asking: "Is the function in question a core competency?" Will it remain this way in the short through to medium term? Do you need this function performed only for a set period of time? It is important to be cautious when answering this because Yes can become No after a period of time.

Do you know when the start and stop points are? Are you looking at resourcing options because of a bandwidth constraint? Are the resources only available in a certain formats (Consultancy, Outsource or Co-Sourcing)? Is the function clearly defined? Do you need flex-up and flex-down flexibility?

Should you be considering technology solution to help magnify your resources to mitigate this need or to backfill existing resources?

Selecting a Co-sourcing partner

Be proactive in creating a deals principles document – a list of the needs, criteria, requirements and budget that your organisation have for this function. Talk to more than one potential vendor and make sure that you consider cultural fit as part of your criteria.

"The key point to make is that you should consider flex-up and flex-down as part of your requirements."

The key point to make is that you should consider flex-up and flex-down as part of your requirements. Take input from your short-listed potential partners, how might they help you refine your criteria and requirements to best meet your needs? A good co-sourcing partner will be happy to work with you on a flexible basis to help you assess the fit and to make the adjustments to make a successful partnership, and to continually improve.

"As a rule you shouldn't be looking to external partners to provide core functions other than on a temporary and tactical basis."

What should stay internal?

Know your organisation's core business. Knowing what your organisation's core business is, allows you to answer this question in the most effective way. As a rule you shouldn't be looking to external partners to provide core functions other than on a temporary and tactical basis. If you need to do this then the partner and the service provision must be well managed. What security functions work when co-sourced?

Functions to Co-source

First up, let's consider the tactical option and how to improve your cyber security quickly. Perform a security assessment to act as a benchmark and to provide focus for your continual improvement. Test security plans. 45% of companies said they didn't have the time/ability to do this well. Test escalation policy/incident response.

31% of companies have either never tested it or their last test was more than a year ago. Write and/or test policies. 26% of organisations have a formal policy that is tested and reviewed annually.

Strategic – Continual Improvement

Implement a framework or standard to help demonstrate improvements and adherence to standards while improving your organisation's incident response plan. Implement a security orientated continual improvement process to ensure the effectiveness of your organisation's security function. Then provide a fully flexible security officer (SO) service to augment your existing capability if/where it exists. At the same time, arrange for a flexible chief information security officer (CISO) service to augment your existing capability if/where it exists.

* Statistics from the SC Magazine MarketFocus May 2016 – Co-Sourcing SIEM

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com

The eight steps to good Co-sourcing governance

From a governance perspective, any co-sourcing or outsource contract can only outsource the function not the responsibility. Maintain/implement a vendor management system. This doesn't have to be overkill, but ensure that you have regular vendor meetings, document the meetings and hold the vendor to account to the contract and the service levels.

Know, maintain and review the reasons for entering into an out-sourcing or co-sourcing arrangement. If the situation changes then flex-up or flex-down accordingly.

Good supplier security

Learn Target's Lessons. If the Target breach taught us anything it is that vendors are a threat vector. Choose your vendors well, and ensure that they are following and meeting your security standards/expectations.

Key Points

- Security should be part of your vendor selection criteria
- Security should be part of your vendor contract
- Brief your vendors on your security standards and expectations
- Take your vendors through your security awareness training
- If your vendors or the services they provide are part of your BCP or incident response capability, ensure they have this information

"No matter how good, efficient or effective, no single part of the company can secure the whole company alone."

Eight steps to Cybersecurity – A Whole Company Issue

Cybersecurity is the responsibility of the whole company. No matter how good, efficient or effective, no single part of the company can secure the whole company alone. That is a key point. Ensure your small security teams are engaging with the rest of the organisation. Running regular cybersecurity awareness training can protect your staff both at work and at home.

That concludes this white paper on how businesses can magnify their cyber resources, flex up or down according to their requirements and the beauty of co-sourcing arrangements.

The key take aways are:

1. Cybersecurity is an evolving and maturing threat.
2. Magnify your resources using technology and co-sourcing.
3. Organisation's security teams often don't have the bandwidth or expertise, a different approach is needed.
4. Pick the right partner for your organisation.
5. Choose the right functions to seek help with.
6. Maintain good governance, outsource function not responsibility.
7. Ensure your suppliers and partners maintain your security.
8. Ensure that the whole organisation is working together to mitigate the vulnerabilities.

The key message is that co-sourcing is the way to go. It provides organisations with greater flexibility, better cost control and access to a greater breadth of knowledge and resources than any of the other models whether that is hiring full time or part time employees or even the consulting model for doing specific pieces of working.

The co-sourcing model, however, is about getting close to an organisation working closely with existing employees supplementing and magnifying their capabilities. Whereas a consulting arrangement might look at a specific project that can be benchmarked – saying the introduction of new software in a business – co-sourcing arrangement might seek to keep a company secure over a two-year period and evolves working with the existing team. Co-sourcing partners seek to augment existing capability and bandwidth.

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com