More threats. Fewer experts.
There's a growing skills gap. How will you manage?

Threats are not going away, and globally, the information security workforce shortfall is increasing – a combination of facts that continues to trouble CIOs.

The global dependency on technology, combined with the ceaseless sophistication, frequency and creativity of cybersecurity threats, continues to increase our vulnerability at a national, organisational and individual level. Left unchecked, these incidents will rise and become more sophisticated and harder to detect. And with a broadening footprint that includes cloud-based services, mobile devices, big data, and the Internet of Things (IOT), traditional network boundaries are dissolving – and leaving us with new challenges in how we keep secure across all locations. It's a challenge that is compounded by the need for sufficient skilled resources and a backdrop of significant resourcing challenges across the globe.

This lack of internal resource to keep pace with a growing problem means that it's no longer possible for many organisations to tackle all aspects of information security management in-house. And in addition to the growing frequency and complexity of threats, the regulatory landscape is also changing. In Europe for example, the European Union is set to impose tough new standards in 2018, along with punitive fines for failing to protect data. In the US too, there is talk of a national data-breach law requiring companies that have been hacked to reveal this within 30 days if personal data may have been taken. In the Risk:Value 2016 report[1], 43% of respondents highlighted regulatory requirements and fines as the biggest motivator for implementing information security processes.

> **Many who engage NTT Group incident support do so because they have little investment in their own incident response capabilities and don't have the technical knowledge to respond.**
>
> NTT Group Global Threat Intelligence Report 2016

Cyber attacks have evolved from those that caused low level nuisance to more sophisticated incidents including disruption of networks; attacks on infrastructure; DDoS attacks and theft of personal data. With the growth of Bring Your Own Device (BYOD) in the workplace and multiple connected devices in homes and offices, we're all targets and there's no room for complacency.

What's certain is that 2016 and beyond will provide in-house security teams with significant resourcing challenges and a growing scrutiny of how they deal with regulatory issues, the challenges presented by the Internet of Things, and criminal threats.

Changing threats require a range of skills

There are many theories about why we're facing a hiring shortfall for information security workers, but one thing is certain – it's not about budget. A 2015 survey[2] highlighted that budgets were available to hire more personnel, but there's an insufficient pool of suitable candidates with the relevant skills and industry experience.

Today's organisations are facing security challenges that didn't exist last year, let alone a decade ago. And with cybercrime now a serious business, organisations are discovering new issues to manage every day – it's now as easy to buy an exploit kit online, as a book from Amazon; Gartner's prediction[3] about the Internet of Things is that we'll have 25 billion connected devices globally by 2020 – each bringing new security challenges; and the NTT Group Global Threat Intelligence Report 2016[4] noted that organisations are still not defending themselves against existing vulnerabilities and less advanced threats – let alone new and sophisticated attacks. The report highlighted that end users have become a huge liability and a major component of all attacks. 21 percent of vulnerabilities detected in client networks were more than three years old and more than five percent of them were over ten years old.

1. Vanson Bourne, Risk:Value 2016 Report, commissioned by NTT Com Security *2. The 2015 (ISC)² Global Information Security Workforce Study, Frost & Sullivan*
3. Gartner – 25 billion connected devices press release *4. NTT Group Global Threat Intelligence Report 2016*

Stretched IT departments are struggling to keep on top of information security and the consequences can have a serious impact on the vulnerability of the business.

We need more resources to manage this. And we need the right resources – not IT generalists, but people with forensic skills, industry expertise, incident handling experience, an understanding of mobile security demands, up-to-date compliance knowledge, experts in cloud security and people with the analytical skills and experience to see what others might miss.

Ongoing global skills shortage

Geographical location too plays its part in explaining the skills gap. In Europe, much of the skills shortage can be attributed to the move towards offshoring technology operations to India in the mid-90s. As a result, between 1998 and 2000 it's estimated that 70 per cent fewer graduates attended courses that were core to entering IT professions – such as science, technology, engineering and maths (STEM). The result is a skills gap that may take generations to fill – 20 years according to the UK's National Audit Office.[5]

And in the US, the Bureau of Labor statistics shows that the number of graduate-level security experts needed will rise by 37 per cent in the next decade, double the rate of the IT sector overall. For now, that leaves a widening gap in the number of IT security experts needed to manage a greater number of threats. And security sprawl is adding to the challenge globally – with a growing number of security technology products and an increasing number of security vendors and management consoles.

Too many threats and not enough professionals

Whatever the reason for the shortage in IT professionals, organisations are faced with a growing volume of cyber-attacks. The bad guys are highly skilled, well organised and tenacious, while organisations are, in the main, under-skilled and undermanned.

The shortfall in the global information security workforce will reach 1.5 million in five years.

Frost & Sullivan

1 in 5 organisations has experienced an APT attack[6]; 3.6 billion records have been exposed since 2013 as a result of a data breach[7], and it's calculated that US $3 trillion is the total global impact of cybercrime[8]. Yet it's estimated that there are 1 million unfilled security jobs worldwide[9]. This is unlikely to change in the near future, with Frost & Sullivan predicting that there will be 1.5m unfilled jobs by 2020[10]. And the 2015 Global Cybersecurity Status Report[11] reveals that 86% of organisations globally believe that there is a shortage of skilled cybersecurity professionals.

There are simply not enough IT security professionals and organisations need to urgently review their resourcing options.

We have a resourcing challenge. What are the options?

Do nothing

It's always an option to sit tight and do nothing about finding the right resources. But all the indicators are that the security skills gap will be with us for some time. The frequency and sophistication of cyber-threats will continue, networks are becoming increasingly complex and the sheer volume of available data is a perpetual challenge, with not enough skilled people available to analyse data and turn it into actionable threat intelligence.

During 2015, 21% of identified vulnerabilities were more than 3 years old, and more than 5% of them were over 10 years old.

NTT Group Global Threat Intelligence Report 2016

Internal teams, however, are already stretched. The Frost & Sullivan report[2] highlighted configuration mistakes and oversights as a material concern and indicated that remediation time following system or data compromise is steadily getting longer. And the Global Threat Intelligence Report 2016 indicated that an average of 77% of organisations did not have a formal incident response plan in place – possibly as a result of lack of the right resources or in-house skills. The net effect is that internal teams are providing a reactionary role rather than proactively addressing the wider problem. Fewer skilled professionals means that organisations will continue to struggle to do anything beyond keeping the lights on. Doing nothing really isn't an option.

Understand your risk exposure

Perhaps you accept that something needs to be done, but you're not quite sure what that might be. Understanding your risk exposure across all areas of the business and prioritising the areas on which to focus is another option. Following this, you can make a more informed decision around resource requirements to help mitigate risk. However, a lack of resource will often mean that there is nobody available internally to carry out the assessment in the first place. Risk and security management are important areas for any organisation, and as the threat landscape evolves, your business needs to consider its current risk exposure in the context of its commercial objectives. An independent assessment could help you understand your risk exposure, consider best practice, prioritise activities and articulate these at all levels of your business. The recommendations may mean that it makes good commercial sense to hire additional people or potentially outsource some, or all, of your requirements.

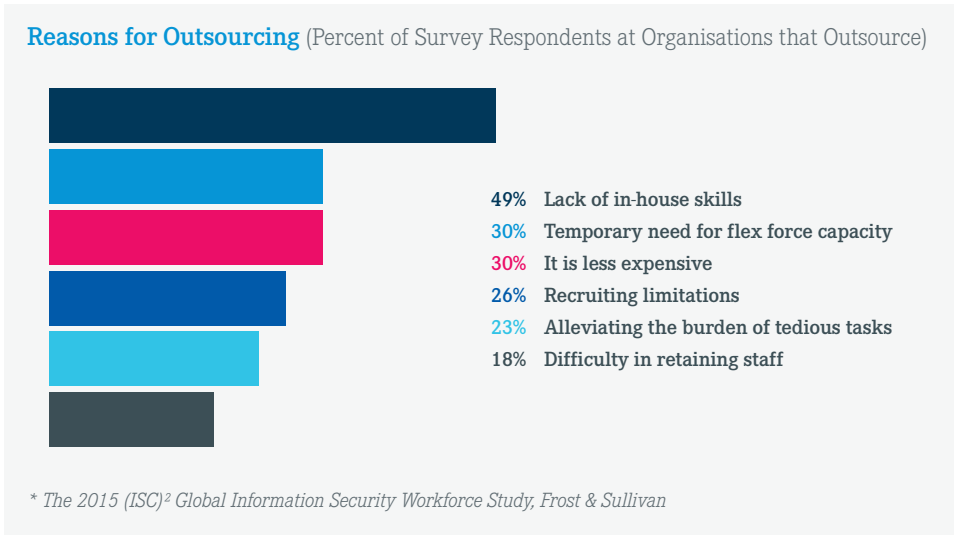
Invest in internal resources

Your internal IT team will be grounded in IT fundamentals and versed in your day-to-day operations and therefore perfectly placed to take on roles in cyber security. But remember that these are skills honed over many years and developing them is less of a quick fix to the resourcing challenge and more of a long-term goal. Security experts need a great mix of technical and soft skills; they need to know how to communicate effectively with non-IT colleagues; they need to understand business processes, compliance and analytics; and they need to have a genuine interest in information security.

Training your own staff could be a great investment in the long term, but information technology products are changing faster that you'll be able to train your team and a commitment to training and professional development is a strategic decision needing high budgets. In the short term, however, it won't be enough.

5. The UK cyber security strategy: Landscape review 6. ISACA 2014 APT Survey 7. 2015 Breach Level Index, Gemalto 8. ©Increased Cyber Security can save global economy trillions: World Economic Forum, McKinsey 2014 9. ©2014 Cisco Annual Security report 10. The 2015 (ISC)² Global Information Security Workforce Study, Frost & Sullivan 11. ISACA 2015 Global Cyber Security Status Report

Figure 1 Reasons for outsourcing (percent of respondents at organisations that outsource)



Invest in external resources

Recruiting and managing a team of security professionals brings its own challenges. There's the obvious cost of recruitment and the length of time it takes to fill each position. Plus the perennial requirement to train the team and keep skills and certifications up-to-date. And when people leave, there's the challenge of starting the process over again. A recent global report† suggests that the increasing use of managed and professional services to address the skills shortage is predicted by nearly one-third of the survey respondents, with the reasons for outsourcing highlighted in Fig 1. The lack of in-house skills was cited by almost 50% of respondents.

Outsourcing some or all of your security operations to a professional security services provider will alleviate the problem of there not being enough resources in-house. These providers know how and where to find the right experts for your industry; they invest in training and improving professional qualifications; they continuously monitor your networks round the clock, every day of the year; and they take all the time-consuming and repetitive workload away from your organisation, leaving you to get on with managing your business.

Outsourcing security services

Managed security services continue to evolve. For a start, a relationship with a professional security services provider can be limited to any service that you are struggling to resource internally such as risk assessment, developing an incident response plan or managing a compliance project. Alternatively, many organisations choose to fully outsource security operations to the experts.

And a fully outsourced service is no longer just a case of managing complex networks from a 'lights on' perspective. It's about proactively protecting your organisation against multiple, complex security threats – around the clock – and providing added value such as insight and analytics, over and above managing your devices. Choosing a third party can mean gaining access to their collective global knowledge and systems as well as their highly-experienced people.

Security services providers keep their fingers on the pulse of current and next generation threats and vulnerabilities, and they also have access to regional and global threat intelligence. All of which enables you to be proactive and keep one step ahead of the game, rather than simply reacting to what has already happened. The right third-party provider can manage the most complex of infrastructures and diverse applications: on-premise, in the cloud or a hybrid model.

Skills and Outsourcing quick facts

- 30% expect to see an increased spend in outsourced or managed services
- 62% feel their organisation has too few information security workers
- 46% highlight security analysts as a staffing deficiency in their organisation
- 50% believe that a shortage of IS workers has a detrimental impact on security breaches
- When asked why organisations outsource, 49% think it's down to lack of in-house skills; 30% think it's due to a temporary need to flex the workforce
- Top three areas to outsource are threat intelligence, detection, forensics and remediation (40%); security asset management and monitoring (37%); risk and compliance management (28%)

** The 2015 (ISC)² Global Information Security Workforce Study, Frost & Sullivan*

"A big benefit to subscribing to a managed service is that these service providers often have a better understanding of what's going on globally as opposed to just the network underneath the security team's purview."

Dark Reading

Conclusion

The threat landscape is evolving too quickly for organisations to keep up. And the broadening footprint of cloud-based services, mobile devices, big data, and the Internet of Things is adding to the problem. There are simply not enough qualified information security experts entering the workforce and there's no silver bullet in terms of training internal resources or hiring new people to alleviate the problem. Information security needs to be seen as a career choice and there must be greater awareness in schools and colleges globally in order to attract more people into the profession. Until then, organisations need to think carefully about a future that relies on getting by with existing resources versus outsourcing some or all of their security operations to a trusted advisor. There's never been a more important time to make that decision.

We see a more secure world

NTT Com Security is in the business of information security and risk management. By choosing our WideAngle consulting, managed security and technology services, our customers are free to focus on business opportunities while we focus on managing risk.

The breadth of our Governance, Risk and Compliance (GRC) engagements, innovative managed security services and pragmatic technology implementations, means we can share a unique perspective with our customers – helping them to prioritise projects and drive standards. We want to give the right objective advice every time.

Our global approach is designed to drive out cost and complexity – recognising the growing value of information security and risk management as a differentiator in high-performing businesses. Innovative and independent, NTT Com Security has offices spanning the Americas, Europe, and APAC (Asia Pacific) and is part of the NTT Group, owned by NTT (Nippon Telegraph and Telephone Corporation), one of the largest telecommunications companies in the world.

To learn more about NTT Com Security and our unique WideAngle services for information security and risk management, please speak to your account representative or visit: **www.nttcomsecurity.com** for regional contact information.