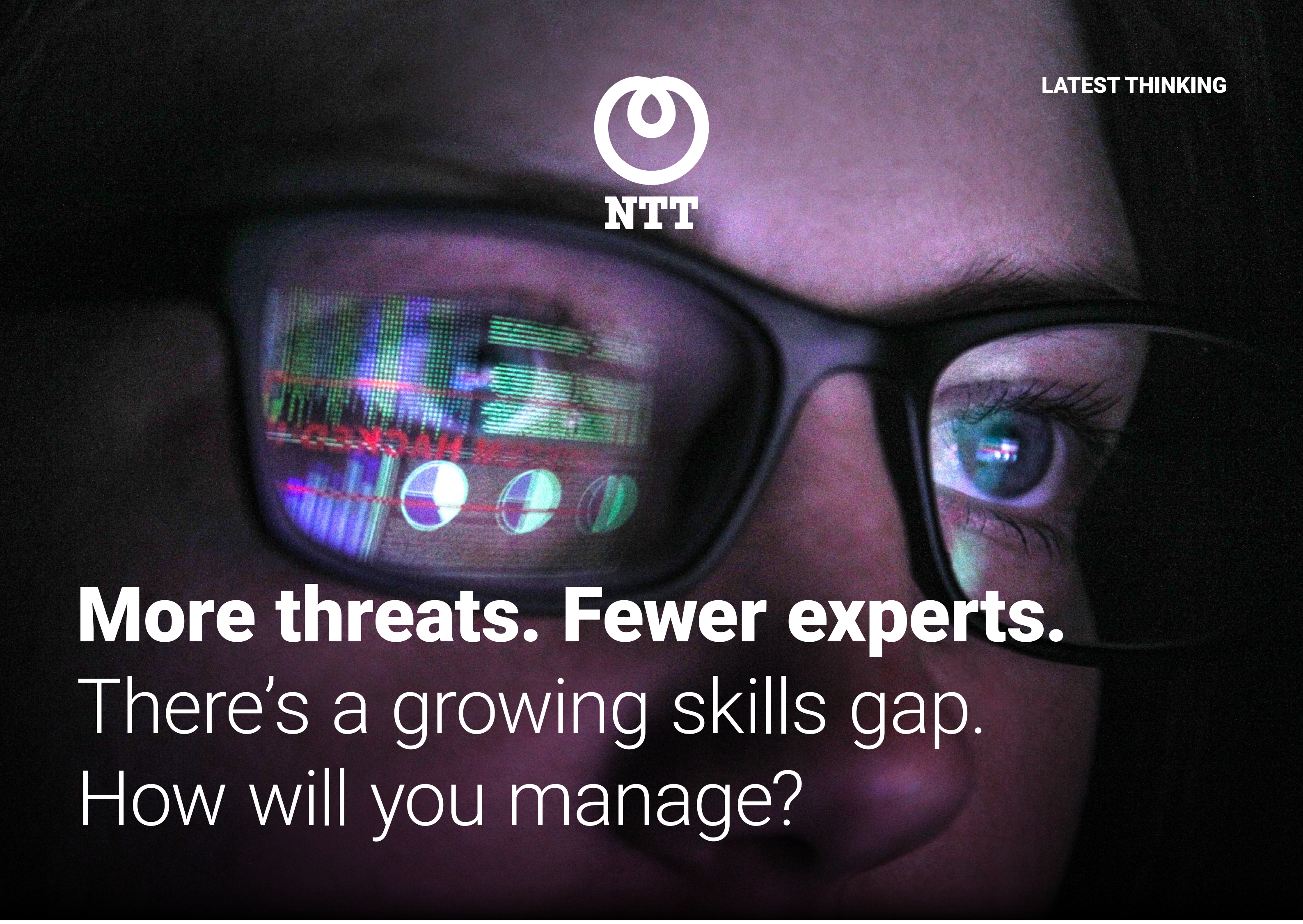
LATEST THINKING

NTT



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.

Our dependency on technology, combined with the sophistication, frequency and creativity of cybersecurity threats, continues to increase our vulnerability at a national, organizational 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, 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.

A changing regulatory landscape

This lack of internal resources to keep pace with a growing problem means that it’s no longer possible for many organizations to tackle all aspects of information security management in-house. Threats are also no longer the domain of small numbers of skilled individuals, with the malware-for-hire phenomenon meaning that cybercriminals with rudimentary IT skills can be successful.

And in addition to the growing frequency and complexity of threats, the regulatory landscape is changing and heightening awareness about the need for cybersecurity professionals. In Europe for example, the General Data Protection Regulation (GDPR) has imposed tough new standards from May 2018, along with punitive fines for failing to protect data, and Germany has recently passed the final stage of the German Data Protection Amendment Act (GDPAA) to align with GDPR. In Australia, the government passed the Privacy Amendment (Notifiable Data Breaches) Act 2017, establishing the Notifiable Data Breaches scheme, and China’s new Cyber Security Law (CSL) took effect on 1 June 2017. 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.

What’s certain is that 2018 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

Today’s organizations are facing security challenges that didn’t exist last year, let alone a decade ago. And with cybercrime now a serious business, organizations are discovering new issues to manage every day.

Gartner's prediction about the Internet of Things is that we'll have 20.4 billion connected devices globally by 2020[1] – each bringing new security challenges; and the NTT Security Global Threat Intelligence Report 2018 noted that ransomware and other endpoint attacks are on the rise, and systems directly exposed to the internet remain prime targets for cyberthreats.

> In 2015 62% of organizations reported **having too few information security workers to meet their needs. In 2017, this has grown to 66%.**

The speed of response required is also challenging IT teams and there's no time for complacency once organizations are given advance warning of new vulnerabilities. Within 24 hours of vendors sending out an advisory for one of the Apache Struts vulnerabilities, for example, we were detecting attacks.
New attacks spread quickly across the hacker community and it's hard for stretched IT departments to keep up as they try to identify, test and apply patches. And that's becoming more of a problem, with a trend towards attackers targeting newer vulnerabilities which are days instead of years old. This move towards 'current year' vulnerabilities requires a rapid response and accurate threat intelligence – skills that organizations don't typically have.

Ongoing global skills shortage

The skills gap meantime is getting worse. It's estimated that there are 1 million unfilled security jobs worldwide, and this is unlikely to change in the near future. According to a recent (ISC)^2 survey, the number of unfilled cybersecurity jobs globally will rise to 1.8 million by 2022,[2] a 20% increase from 2015 estimates.

The same survey of 19,000 cybersecurity professionals worldwide, found 66% of survey respondents (up from 62% in 2015) feel they do not have enough employees to address increasing levels of threat.

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.

Finding the right people

Whatever the reason for the shortage of IT professionals, organizations are faced with a growing volume of cyberattacks. Attackers are highly skilled, well organized and tenacious, while organizations are, in the main, under skilled and undermanned.

We need more resources to manage this. And we need the right resources. On one hand we need IT professionals – people with compliance and 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. But on the other hand, we shouldn't ignore professionals from outside typical IT roles. The (ISC)^2 report highlighted that 30% of employees launched their cybersecurity career after holding a non-technical job such as in business, accounting or marketing.

The complexity of operations is also something that shouldn't be underplayed. In a diverse IT department, an organization needs staff with a range of skills to cover all areas. Yet many companies don't have a broad enough skill set and expect employees to wear many hats. It's not untypical for a Windows administrator to be responsible for firewall management – a skill set they may well have learned from a training manual.

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

The global information security job market[1]

- 66% feel their organization has too few information security workers.
- There will be a 1.8 million worker shortage in information security by 2022.
- 49% of global organizations cite the difficulty in finding qualified personnel as the most common reason for worker shortage.
- Unemployment amongst information security professionals sits at only 2% globally.
- 21% of information security workers have changed jobs between 2016 and 2017.
- Nearly 90% of the global IS workforce is male.

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 cyberthreats 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.

> **68% of organizations agree that additional skilled resources** would help them cope with the number of security threats.

Internal teams, however, are already stretched. The Frost & Sullivan report highlighted configuration mistakes and oversights as a material concern and

[1] *Gartner – press release* [2] *The 2017 (ISC)^2 Global Information Security Workforce Study, Frost & Sullivan*

indicated that remediation time following system or data compromise is steadily getting longer. It's concerning therefore that the number of organizations with formal incident response plans in place is not rising year on year. The NTT Security Risk: Value 2018 Report indicates that 43% of organizations globally do not have an incident response plan in place[3] and there's no significant decrease to this figure over the past 12 months. The net effect is that internal teams are providing a reactionary role, rather than proactively addressing the wider problem. Fewer skilled professionals means that organizations 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 prioritizing 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 resources often means that there is nobody available internally to carry out the assessment in the first place. Risk and security management are important areas for any organization, 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, prioritize 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 cybersecurity. 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.

> The shortfall in the global information security workforce will reach 1.8 million **by 2022 – a 20% increase over the forecast made in 2015.**

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

Address your recruitment strategy

A recent report highlights several areas where organizations could look to improve recruitment strategies, which in turn would enable companies to bridge the 1.8 million worker gap projected for 2022.

The information security sector is overwhelmingly dominated by men – only 11% of the global IS workforce is female,[4] with women being paid less than male counterparts and reporting significantly more incidents of discrimination. That's despite being more qualified than men at entry-level. More needs to be done at every level to encourage women to consider cybersecurity as a career option. We need to educate career advisors in schools and universities, and we need to fundamentally change the macho language of cybersecurity before women will enter a field where they think they don't belong.

The report also highlights that nearly one third of the existing workforce comes from a non-technical background and these workers go on to have successful careers in information security. Employees with people and business skills can make a great contribution – the ability to listen, empathize and de-mystify cybersecurity is key to helping organizations make informed decisions and recruiters should take note.

And there's a revolving door of millennial workers who are leaving their jobs at unprecedented levels and appear to value compensation less than more mature workers.

Recruiters therefore need to look beyond traditional recruitment practices, value workers from diverse backgrounds, and better understand what motivates their workforce. There's a disconnect between a manager's expectations and what a new recruit requires for a successful career and it's a gap that needs to narrow if the anticipated global skills shortage is to be addressed.

> **'We can't ignore the growing skills gap in information security.** From schools to universities and across the industry, we need to promote cybersecurity as work that really matters, offering a rewarding career path, **job stability, good financial remuneration and a huge amount of job satisfaction.'**

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

[3] NTT Security Risk: Value 2018 Report [4] Frost & Sullivan Whitepaper: The 2017 Global Information Security Workforce Study: Women in Cybersecurity

when people leave, there's the challenge of starting the process all over again.

A recent global report from NTT Security highlights a number of reasons for outsourcing including lack of in-house skills and resources (see Figure 1, below).

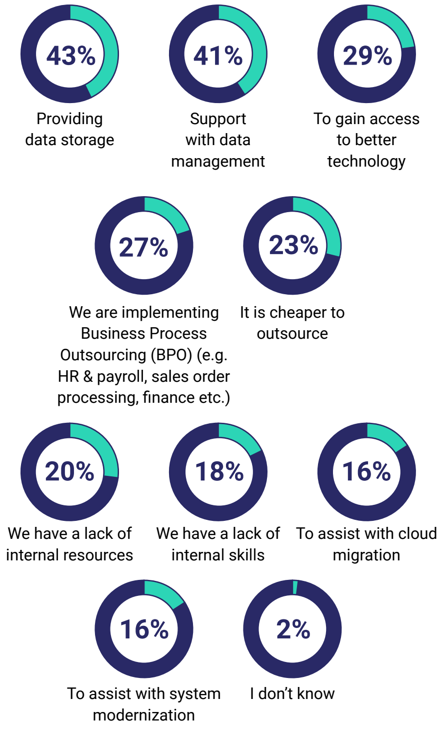


Figure 1
Reasons for using third party services
Source: NTT Security Risk: Value 2018 Report

Outsourcing security services

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 updating 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 organization, leaving you to get on with managing your business.

> '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

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 organizations 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 organization 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.

> 'Identify security commodity areas (log management, for example) that are more routine in nature, where processes and procedures could be replaced by third-party suppliers. **Many resource-constrained organizations are addressing the challenge by adopting managed security services.'**

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.

Conclusion

The threat landscape is evolving too quickly for organizations 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, organizations 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.

Disclaimer: The work described in this thought leadership was performed while the company was known as NTT Security.

NTT