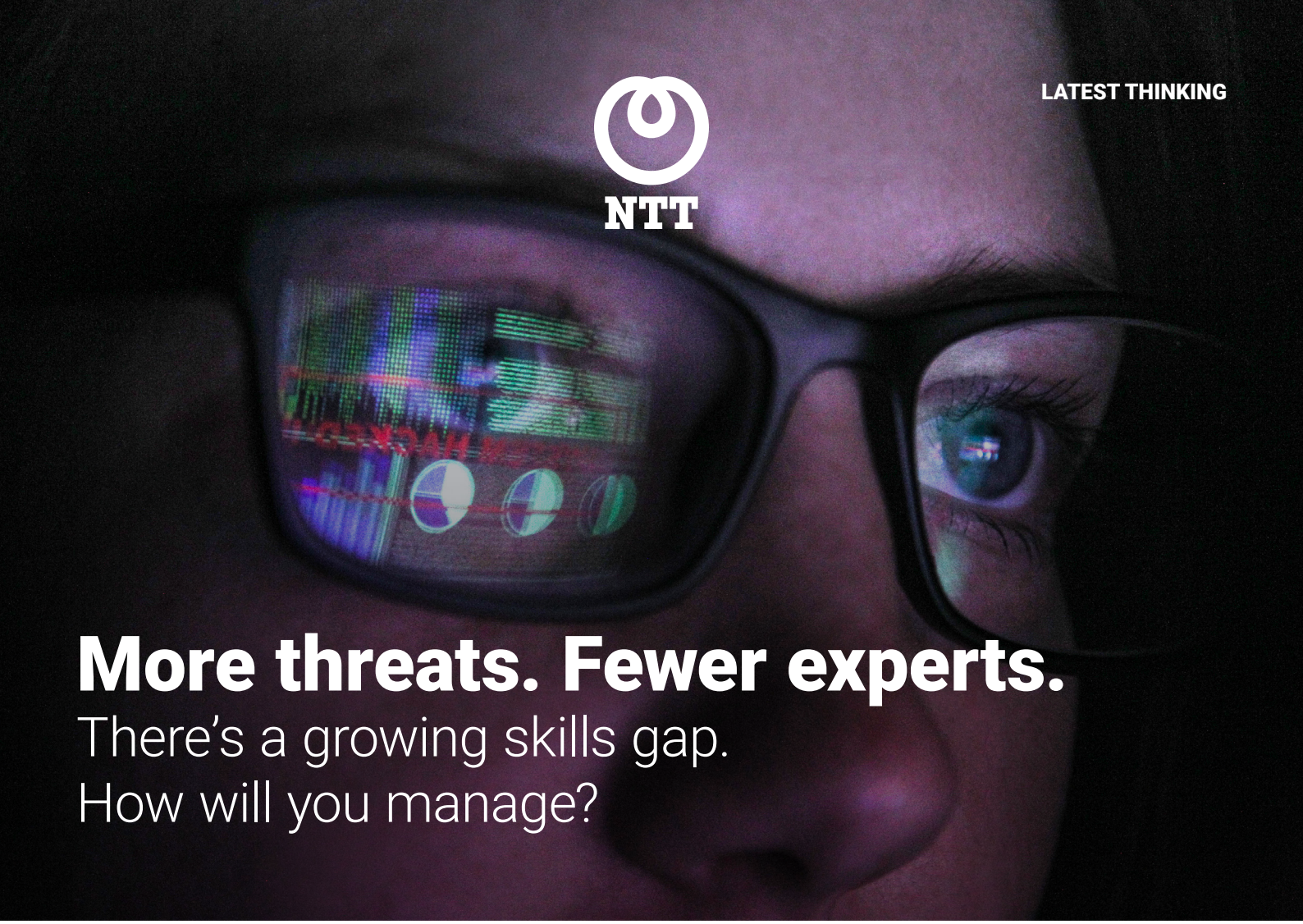

More threats. Fewer experts.

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. The General Data Protection Regulation (GDPR) of 2018, the California Consumer Privacy Act of 2019, Singapore's signing of its Cybersecurity Bill into law in February 2018, Thailand's Personal Data Protection Act of 2019, and the 2018 updates to the Australian Privacy Act were five relatively recent additions to compliance and regulatory requirements. Additionally, on 23 January 2019, Japan's Personal Information Protection Commission (PPC) determined the GDPR has equivalent data protection standards as its Act on the Protection of Personal Information (APPI). The EU likewise determined equivalency between the APPI and GDPR, allowing for the transfer of personal information between Japan and the EU.

What's certain is that 2020 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.

IDC estimates that there will be 41.6 billion connected IoT devices, or 'things', generating 79.4 zettabytes (ZB) of data in 2025[1] – each bringing new security challenges; and the NTT Security Global Threat Intelligence Report for 2019 noted that as cybersecurity perimeters are being rapidly extended, and as attackers continue to launch more sophisticated attacks, conventional perimeter defense is not as effective as once perceived.

44% of organizations do not have **adequate resources or skills in-house to cope with the number of security threats they face**

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 is getting worse. According to international cybersecurity organization (ISC)[2], the current global cybersecurity workforce gap and number of unfilled security jobs is greater than four million. Unfortunately, we're not likely to see an improvement in this number in the near future.[2]

NTT's 2020 Global Managed Services Report stated that 44% of organizations do not have adequate resources or skills in-house to cope with the number of security threats they face.[3]

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 just 42% of respondents indicate that they started their careers in cybersecurity; meaning 58% moved into the field from other disciplines.[2]

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.

Among the key findings from the study[2]:

- The cybersecurity workforce needs to grow 145% to close skills gap and better defend organizations worldwide
- 65% of organizations report a shortage of cybersecurity staff
- 30% of survey respondents are women; 23% of whom have security-specific job titles
- 37% are below the age of 35, and 5% are categorized as Generation Z, under 25 years old
- 59% of cybersecurity professionals are currently pursuing a new security certification or plan to do so within the next year

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.

62% of organizations said they expect an **increase in the need for cybersecurity/IT skills in the next two years[3]**

[1] IDC – press release | [2] The 2019 (ISC)[2] Global Information Security Workforce Study | [3] NTT's 2020 Global Managed Services Report

Internal teams, however, are already stretched. The Frost & Sullivan report[5] highlighted configuration mistakes and oversights as a material concern and 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 2019 report indicated that 52% of organizations globally do not have an incident response plan in place and there was no significant decrease to this figure over the past 12 months.[4] 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 current global cybersecurity workforce gap and number of **unfilled security jobs is greater than 4 million.**

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[5] highlights several areas where organizations could look to improve recruitment strategies, which in turn would enable companies to bridge the worker gap.

The information security sector is overwhelmingly dominated by men – only 30% of the global IS workforce is female.[5] More needs to be done at every level to encourage women to consider cybersecurity as a career option.

Similarly, only 37% of security professionals are below the age of 35 and 5% are categorized as Generation Z. Top recruiting sources outside of the core cybersecurity talent pool include new university graduates (28%), consultants/ contractors (27%), other departments within an organization (26%), security/ hardware vendors (25%) and career changers (24%). We should be reminded that anyone can have a successful career in security no matter their starting point – invest in the training that can help them to be.[2]

Employees with people and business skills can make a great contribution – the ability to listen, empathize and demystify cybersecurity is key to helping organizations make informed decisions and recruiters should take note.

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.'**

[2] The 2019 (ISC)[2] Global Information Security Workforce Study | [4] NTT Security Risk: Value 2019 Report
[5] Frost & Sullivan Whitepaper: The 2019 Global Information Security Workforce Study: Women in Cybersecurity

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 all over again.

Outsourcing security services

NTT's 2020 Global Managed Services Report highlights that security outcomes drive the business case for using managed security and IT services. (see Figure 1).

Figure 1
Reasons for using managed security services[3]

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 timeconsuming and repetitive workload away from your organization, leaving you to get on with managing your business.

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.

'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

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.

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.

'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.'**

[3] *NTT's 2020 Global Managed Services Report*

Together we do great things