KASPERSKY lab

THE CYBERSECURITY SKILLS GAP: A TICKING TIME BOMB

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW

A word from Eugene Kaspersky

"We're living in an age where businesses and public sector organisations are facing ever more sophisticated security threats. From enterprises to critical national infrastructure and financial services, it's widely accepted that if organisations don't have employees with the skills needed to combat cybercriminals, they'll be fighting a losing battle.

Tech-savvy young people can plug the widening skills gap as employers seek to combat the growing threat of cybercrime and avert mass disruption of public and private lives.

Concerns about the cyberskills shortage, plus a deep desire to address the problem, have driven Kaspersky Lab to commission a study and start understanding the issue better. We wanted to discover how young people view cybersecurity as a career, and the potential implications for business and society as a whole if the skills gap continues to grow.

The results in this report are striking. They suggest that young people today are highly capable online. They're curious about large-scale cyberhacks and are interested in finding ways to put their skills to use.

However, the study also indicates that the cybersecurity industry is failing to capture this generation's attention and provide a clear path for young people to find work, hone their skills, and serve society. Instead, many are tempted to use their skills on the 'dark side' by engaging in the development, rather than prevention, of cyberthreats.

With the frequency and notoriety of teenager-led cyberattacks growing, more should be done to encourage young people to enter cybersecurity careers and use their skills for good. We need to channel the interests of the new generation in the right way – before it's too late and we're left with an even wider skills gap."

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

KEY FINDINGS FROM OUR RESEARCH

One-in-four (27%) have considered a career in cybersecurity, with many (47%) regarding it as a good use of their talent. However, others admit an inclination to engage in more questionable activity, such as using their skills for fun (17%), secretive activities (16%) and financial gain (11%) instead.

23% of 18-year-olds are aware of someone they know undertaking cyber-activities (eg: hacking) that could be illegal.

Over half (57%) of under-25s consider hacking to be an 'impressive' skill.

Three quarters (73%) of businesses agreed it was difficult to find enough IT security professionals.

87% of businesses believe that it is important that young people join the cybersecurity war.

Introduction

Organisations are realising that it is not a matter of ***if*** a cyberattack will happen but ***when***. This is causing executives to take a growing interest in what is being done to protect their organisation and, as a result, support for growth in cybersecurity is now well established. The problem is that the pool of skilled cybersecurity talent is not growing alongside it.

Global demand for cybersecurity experts is forecast to outstrip supply by a third before the end of the decade, with Frost and Sullivan's latest Global Workforce Survey predicting a shortage of 1.5 million security professionals by 2020, based on current trends. Priorities need to quickly shift towards plugging this cybersecurity skills gap before it is too late.

Is the industry doing enough to encourage more young people into cybersecurity careers? Should employers be doing more to channel young people's interests and talent in the field? Or perhaps educational institutions should be better at preparing students with more advanced cyberskills?

Global demand for cybersecurity experts is forecast to outstrip supply by a third before the end of the decade...

To find out, Kaspersky Lab conducted a study of over 12,000 consumers and IT professionals across the US and Europe (UK, the Republic of Ireland, France, Germany, Italy, Spain and the Netherlands). We wanted to find out how to plug this growing skills gap and who should be responsible for plugging it.

The results show that the skills gap needs to be bridged by a combined effort of both industry and education if we are to enthuse young people about entering cybersecurity careers. This generation is closer to technology than any before, and the danger is that if it is not properly channelled, tech talent could soon be tempted to use their skills for criminal intent. Young people should be made more aware of the career opportunities that exist in cybersecurity and encouraged to develop their skills for society's good. Through a combination of education and learning on the job, we need to nurture and entice young people into the profession before the gap widens even further.

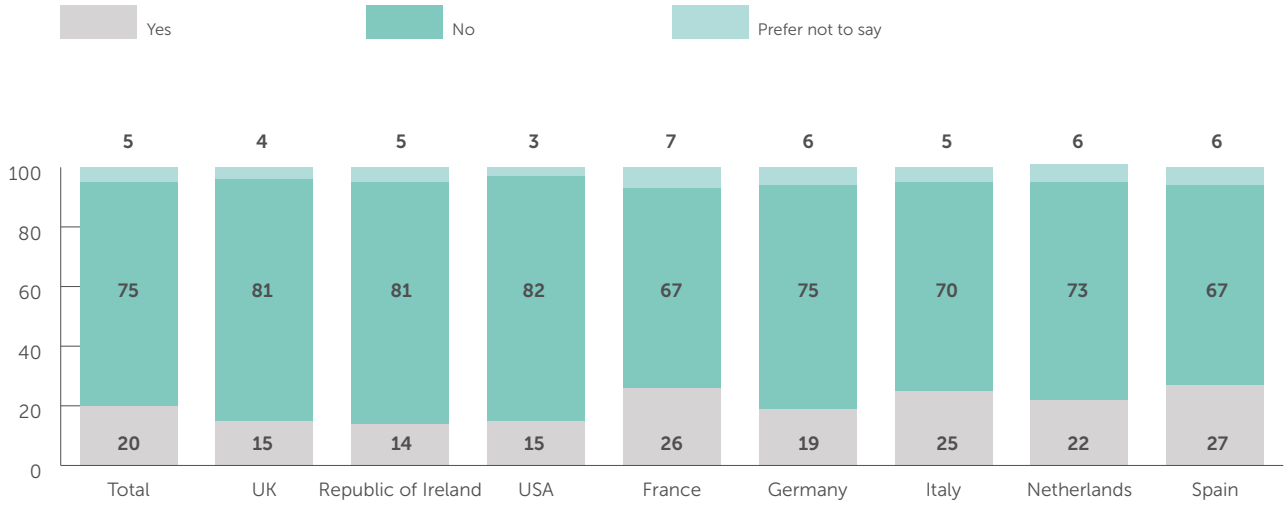
The research findings

Young people are being tempted into potentially illegal activities, exacerbating cybercrime, rather than preventing it

Today's young adults are highly skilled but also highly impressionable as they embark on the next chapter in their lives – be it further education, moving away from home or starting a new job. As digital natives, these people are thoroughly immersed in the digital world but they've also become accustomed to the shock of large-scale cyber hacks.

We found that 23% of 18-year-olds are aware of someone they know undertaking cyber-activities (e.g. hacking) that could be illegal. These activities are more prevalent among young people at university (24%) and those who have just left university and are employed (23%). That's compared to unemployed school leavers – only 15% of whom know of someone undertaking cyber-activities that could be illegal.

Are you aware of anyone you know undertaking cyber-activities (for example, hacking) that could be illegal?



Their concern only marginally outruns their curiosity, and even regard, for these types of crimes. Just under half (47%) of under 25s are 'impressed' when they hear about a company being hacked, and a third (33%) are interested in how the hack was conducted. We also found that concern increases with age. 40% of 21–25-year-olds said they are concerned about how much damage was done and how the company will respond, compared to just 36% of 16-year-olds.

Alarmingly, over half (57%) of under-25s consider hacking to be an 'impressive' skill. A significant number would use their skills for fun (17%), secretive activities (16%), and financial gain (11%) instead.

Many are already adept at blurring the lines, with a third of under-25s (31%) able to hide their IP address, for example. And with only 50% saying they would actually join the fight against cybercrime, clearly there's a lack of engagement in young people in terms of using their cyber-skills to combat crime.

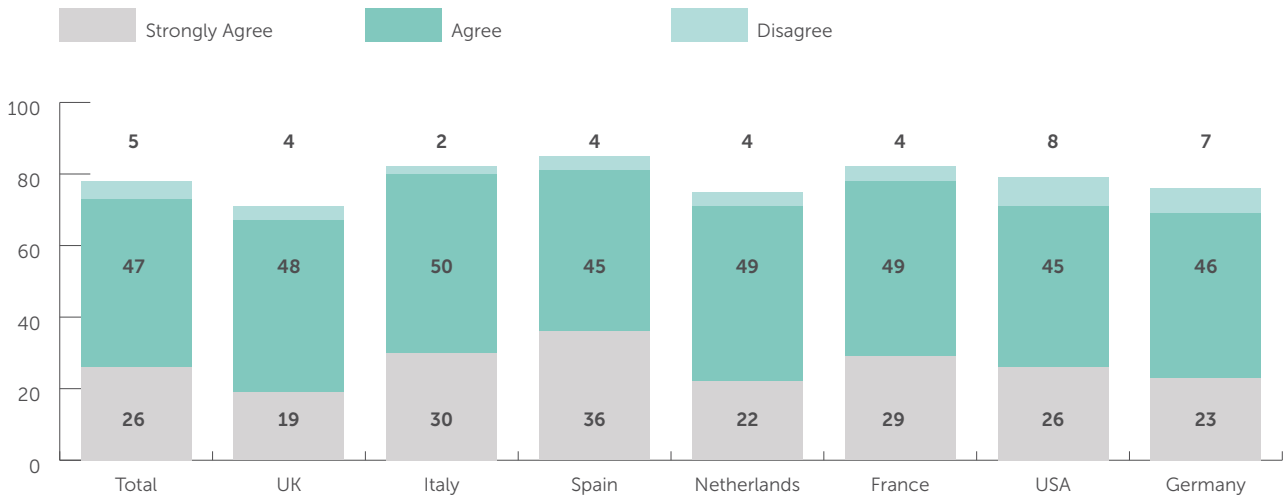
Businesses need young people to help fight cybercrime

With an ever-widening cyber-skills gap emerging, young IT enthusiasts hold the key to filling new job roles on the cybersecurity frontline. This group has the base knowledge and the drive to learn but employers are failing to channel young people's interests and talent in the field.

An overwhelming number of industry professionals (93%) recognise the profession needs to evolve with the current and future landscape, and 87% agree it is important that young people join the cybersecurity war.

The problem is that many employers do not have any entry-level cyber security roles; most promote from within (72%), providing internal training as necessary, and recruit externally (53%) for seasoned security professionals.

To what extent do you agree with the statement: 'It is difficult to find enough IT security professionals to recruit'?



It is important to recognise that, as with any discipline within the IT field, security skills are developed over time, just as with other professions. You are assigned a position that is consistent with your skill level, learn on the job and receive appropriate training. But with nearly three-quarters (73%) of businesses finding it difficult to recruit appropriately skilled IT professionals, perhaps it's time to re-think traditional pathways into the cybersecurity profession?

KEY FINDINGS FROM OUR RESEARCH

An overwhelming number of industry professionals (93%) recognise the profession needs to evolve with the current and future landscape.

87% believe that it is important that young people join the cybersecurity war.

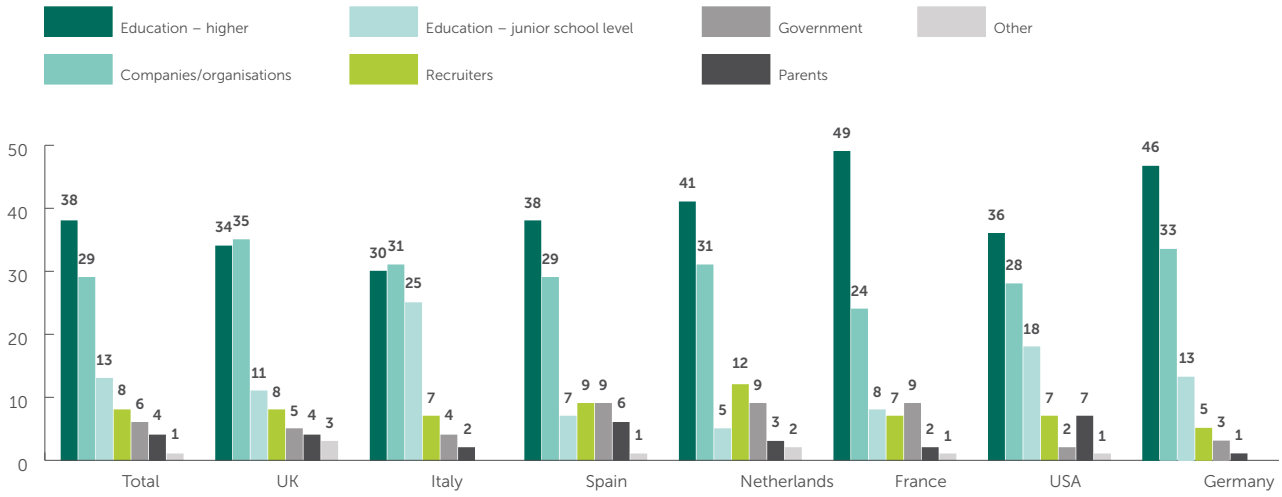
The problem is that many employers do not have any entry-level cybersecurity roles; most promote from within (72%), providing internal training as necessary.

Does responsibility lie with employers or educators?

The question of who is responsible for engaging the next generation of cyber-defenders is important because the scale of the challenge is clear. We need a plan which builds on the obvious interest before it leads to bright and inquisitive minds turning their back on security to use their skills for criminal gain.

According to the IT industry, the education system has a key part to play in encouraging young talent into the profession and equipping it with the necessary skill level. Our research found that almost two thirds of IT professionals (62%) felt that it was primarily education establishments that should be responsible for preparing the future generations of cybersecurity professionals. The industry also has a clear role in protecting its own future, with 27% placing primary responsibility at the feet of business.

Who should be most responsible for encouraging young talent into the profession?



Interestingly, the research found significant regional differences in attitudes on whether education or business is responsible for encouraging young people to enter the industry. Companies are most likely to be held to account in the UK, with over a third (35%) saying employers should be doing more to help young people into cybersecurity roles. In contrast, Italy (25%) and the US (18%) placed a high emphasis on junior school level education, compared to a 13% average.

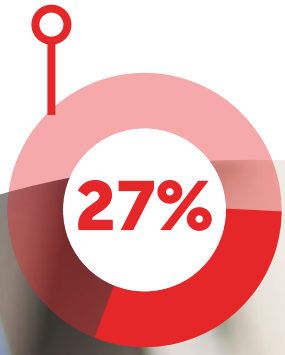
In terms of ensuring that young people have the right skills in place, overall the greatest emphasis is placed on higher education (49%) and companies and organisations (27%). But, again, we see regional differences, with more expectation placed on employers in the Netherlands (40%), for example.

Clearly, differences exist due to differing education systems and government priorities but, in truth, we need a joined up approach between employers and education to equip and develop the skills of a tech hungry generation.

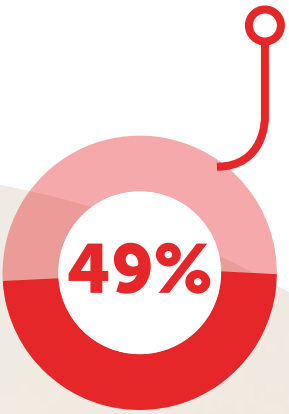
KEY FINDINGS FROM OUR RESEARCH

Our research found that almost two thirds of IT professionals (62%) felt that it was primarily education establishments that should be responsible for preparing the future generations of cybersecurity professionals.

The industry also has a clear role in protecting its own future, with 27% placing primary responsibility at the feet of business.



In terms of ensuring that young people have the right skills in place, overall the greatest emphasis is placed on higher education (49%).



Securing the future of the security industry

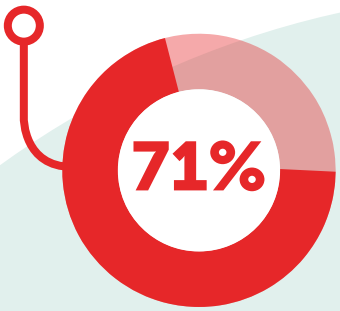
More needs to be done to nurture and attract young talent within the industry, because a burgeoning cybersecurity skills gap is a time bomb waiting to happen.

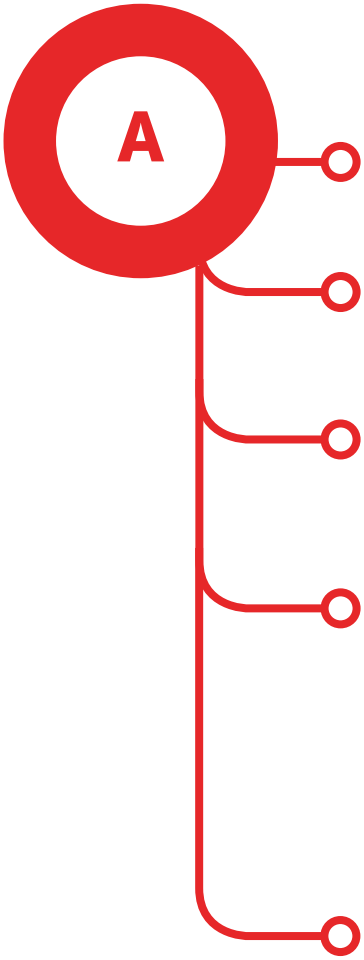
We must make it easier and more attractive for these skilled young people to enter the field. We found that nearly three-quarters of young people (71%) are not aware of any IT security graduate opportunities or internships.

Although businesses argue that new entrants do not have the hands-on cybersecurity skills or necessary experience, very few currently offer entry-level roles or internships that can help harness talent. In fact, only 45% have entry-level roles or a graduate scheme in place.

Three in ten (30%) admit they don't have the internal resources to nurture graduates in a cybersecurity role. And worryingly, only one in five (20%) respondents felt that a dedicated cybersecurity team would have responsibility for IT security in five years' time, with half (50%) believing it would fall to the wider IT team to tackle cybercrime.

We found that nearly three-quarters of young people (71%) are not aware of any IT security graduate opportunities or internships.





What is the answer?

From our perspective at Kaspersky Lab, this report is the start of a long journey to plug the cyber skills gap, as solving a problem of this scale requires co-ordinated efforts from industry, education and government.

We believe more should be done at an employer-level to encourage young people to enter cybersecurity careers. Even among IT security professionals, 27% admit organisations themselves must do more to offer training and graduate schemes.

Industry-led initiatives can help to promote cybersecurity careers. International competitions for university students and young professionals, for example, encourage young talent to use their skills by undertaking various cybersecurity challenges, giving them a taste of how they could be valuable for industry and wider society.

Working closely with universities, our industry can be instrumental in developing the talent pipeline and ensuring the theory and practical learnings live up to expectations and future needs. By consulting on course materials, taking guest lectures, showcasing technology and collaborating on research, industry can help to enthuse, engage and most importantly enlighten and educate the next generation of cyber defenders. Offering placements, internships and graduate positions will help cement the relationship between industry and education, ensuring valuable skills don't slip through the net when we need them most.

The findings in this report illustrate the scale of the challenge facing the industry but also point to some areas where progress can be made. We must take these steps to de-activate the cybersecurity time bomb before it goes off.

i Research note: Kaspersky Lab commissioned Arlington Research to survey a total of 2,120 IT professionals in the UK, Italy, Spain, the Netherlands, France, Germany and the USA. In addition, Kaspersky Lab commissioned Arlington Research to survey 11,531 young consumers, aged 16-25 in the UK, Italy, Spain, the Netherlands, France, the Republic of Ireland, Germany and the USA, and. Both sets of research were completed in July, 2016.

KASPERSKY LAB

Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK

www.kaspersky.co.uk

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW