

CYBERSECURITY

Protecting your future



EARLY ADOPTERS WIN

The right security talent for new IT risks

The spread of new technologies and data analytics, the digitisation of business and increased digital links between organisations and their employees, is expected to escalate tomorrow's cyber risk as those behind cyberattacks become more sophisticated in their execution. And their endeavours are not diminishing.

According to PwC¹, the average number of global security incidents increased by 38% in 2015, resulting in a 56% increase in the theft of hard intellectual property over 2014. Across the UK, two-thirds of large businesses have been hit by a cyber breach or attack in the past year².

Incidents like these affect the entire business and leave a trail of financial, operational and reputational damage. The days when cybersecurity was viewed as simply an IT problem are over.

The solution demands a resilient IT security strategy that includes a technical response as well as 'the human component'.

Phil Sheridan, Senior Managing Director at **Robert Half** explains: *"In order to successfully confront a proliferating breed of cyber attackers, companies need skilled IT talent who understand the current and evolving cyber threat environment. With a robust strategy in place, companies will be prepared for the future of cybersecurity."*

¹ PwC, [The Global State of Information Security Survey 2016, Turnaround and transformation in cybersecurity](#)

² GOV.UK, [Two thirds of large UK businesses hit by cyber breach or attack in past year](#)

Contents

An enterprise-wide solution	2
Friendly fire	3
Strategies for defeating cyber risk	4
Case study: Cybersecurity for an auto firm to outpace hackers	7
The hackers' stepping stones	8
Talented teams to tackle threats	9
IT security checklist	14
Conclusion	15



An enterprise-wide solution

According to a global analysis of data breaches by the Ponemon Institute³, the average cost of a breach for a company was US\$3.8 million in 2015, an increase of 23% since 2013. The escalating costs of data breaches – together with the operational and reputational damages – have forced C-suite executives and their boards to recognise that the spreading threat must be addressed as part of the broader risk management framework of an organisation, and not be viewed as just an IT problem.



TOP THREE IT SECURITY RISKS FACING ORGANISATIONS IN THE NEXT FIVE YEARS



60%

Data abuse/data integrity



54%

Cybercrime (fraud, extortion and data theft)



39%

Spying/spyware/ransomware (economic espionage)

Source: Independent survey commissioned by Robert Half of 100 UK CIOs.

Seventy-one per cent of UK CIOs say their non-IT senior management have a good to excellent understanding of their company’s information security exposure. **Ryan Rubin**, Managing Director at risk and business consulting firm **Protiviti**, believes it is all about being prepared and providing top-down support: *“Businesses have to take an enterprise-wide approach to tackle cybersecurity. Executives play a key role in identifying the business’s risk appetite, and the priority areas requiring maximum security protection. A company’s board and leaders need to be fully engaged about the company’s security practice in order for cybersecurity measures to be successful.”*

³ Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*





Friendly fire

Traditionally, the response to IT security has been to find the optimum way to protect a business's assets from external security attacks. But a growing risk now faces organisations in the form of potential internal security threats.

One major internal threat is when organisations have a BYOD (bring your own device) policy that allows their employees to bring their own laptops, tablets and smartphones to work. BYOD presents a range of security risks and challenges in terms of securing corporate networks and data, mobile device management and developing security policies. However, more companies are taking steps to balance both their employees' needs and their security concerns. One of those steps includes COPE (company owned, personally enabled) devices where the company can unify its approach while still allowing its employees to use their devices for personal communications.

"Organisations across the UK are quickly recognising that their biggest cause of cyber breaches is through internal sources as the attack surface provides various opportunities for attackers to target. But while internal stakeholders are high threat, they are also part of the solution. If you put the right control practices and arrangements in place to use your internal teams to help detect and report incidents, then you can mitigate that risk," says Ryan Rubin.



98% OF COMPANIES ARE PROTECTING CORPORATE DATA ON EMPLOYEES PERSONAL DEVICES. THESE ARE THE TOP ACTIONS:

- 56%** Train employees on maintaining security on personal devices
- 55%** Request employees sign an acceptable usage policy for keeping company information secure
- 53%** Implement authentication and authorisation to grant access to corporate networks
- 41%** Deploy mobile device management technology to enforce enhanced protection
- 29%** Don't allow employees to access corporate data on their personal devices

Source: Independent survey commissioned by Robert Half of 100 UK CIOs. Multiple responses permitted.





Strategies for defeating cyber risk

“It’s no surprise to companies that they will get hacked. The focus instead is on protecting the most business-critical aspects of business and being able to respond quickly and effectively when a threat presents itself.”

Ryan Rubin, Managing Director, Security & Privacy, Protiviti UK

Just as businesses are constantly transforming themselves with new technology, so are cyber criminals. Tomorrow’s IT security risk is expected to intensify as those behind the attacks become more sophisticated in their execution.

As **Tim Goodwin**, Channel Director EMEA, **CyberArk** has noticed: *“A key trend in the evolution of cyberattacks is the large number of high-value breaches that have come about from compromised privileged accounts being used to gain access to sensitive company data.”*

In response, businesses are designing data security strategies that consider the probable level of threats that the future organisation will face, and not simply focus on the business’s current operations. Without consistent efforts, an organisation is exposed to further risk. Moreover, CIOs and their teams are also looking outward to see how other companies are dealing with these threats.

As **Rubin** observes: *“Companies that operate in the same industry are increasingly sharing information about the threats and risks they face, as well as the measures they take to combat them. Because the threats are similar across the same industry, sharing threat information and security intelligence can enable a quicker and more effective response.”*





TOP MEASURES COMPANIES ARE TAKING TO ENHANCE IT SECURITY

Enhancing cloud security

Implementing multi-factor authentication processes (e.g. tokens, biometrics)

Enhancing/implementing mobile device security

Contracting with third-party vendors or adding tools to enhance security

Managing Advanced Persistent Threats (APTs)

Enhancing the process of vetting firms that have access to data

Companies recognise that they must be vigilant to minimise risks. As **David Allott**, Regional Director at **Intel Security's** Product & Solution Marketing Asia Pacific, notes: *"The landscape is changing so rapidly with new threats emerging every second. The question is how companies can keep up with that evolving threat landscape. The cyber criminal will continue to be more sophisticated, and businesses will have to adapt faster."*





The response? **Tim Goodwin** notes: *“The answer is greater than simply investing in security products and IT solutions. A shift in thinking is required: an approach to detecting and mitigating cybersecurity risks that allows meaningful visibility into what’s going on inside the network.”*



KEY CHARACTERISTICS OF AN EFFECTIVE IT SECURITY PROGRAMME

- 1 Has effective governance in place with an overarching view.** An IT security strategy has an impact on the entire organisation. It needs to align with broader enterprise risk management and business objectives, as well as comply with regulation. It also needs to be reviewed and updated for best practices.
- 2 Adopts a risk-based approach to cover the enterprise’s operations and supply chain, including third-party vendors.** The increase in third-party threats is forcing a growing number of contracting organisations to undertake their own evaluation of a vendor’s cybersecurity arrangements, rather than simply relying on the vendor’s word.
- 3 Has the support of senior management.** Companies with a high level of board engagement are more likely to have security best practices in place and consistently follow them.
- 4 Creates employee awareness.** Employees need to be sufficiently aware of potential security threats. Regular training to all personnel on cybersecurity policies and corporate practices is essential.

Source: Protiviti





CASE STUDY:

Cybersecurity for an auto firm to outpace hackers

The project

Global computer security software company Intel Security undertook a cybersecurity review of an automotive supplier.

Challenges

The automotive supplier relied on management processes, human-based surveillance and continuous enhancement of security education among employees to deal with information and data loss prevention. The IT team monitored the security status of all systems with access to the company's 3,000 terminal network users but lacked a unified picture of security incidents and malware threats.

David Allott says: *"Security is often broken up by separate units: endpoint security, network security and data centre security. The individual units, or subunits, within an organisation ideally should not be siloed even though they are focusing on different aspects. They are all part of the solution."*

Solution

David Allott acknowledges there could have been potential data loss that was a huge risk to the company. The solution comprehensively addressed anti-virus needs, data security, network security, and risk detection with centralised control management. *"In order to keep up with the ever-evolving cybersecurity threat landscape, automation is a fundamental requirement when a company operationalises its security internally,"* he says.

Driven by IT security specialists, the people component is vital when addressing cybersecurity issues. *"IT security is a problem that must be solved by people and technology."* He also highlights the importance of companies investing in their IT staff. *"Because the talent pool of security specialists is limited, both retaining as well as developing existing security individuals can help companies manage their IT security process effectively."*



The hackers' stepping stones

68% of attacks on all UK firms involved viruses, spyware or malware⁴.

In recent years larger companies have invested in cybersecurity measures, and this has encouraged cyber attackers to cast their gaze at more vulnerable entities. "Hackers are looking for stepping stones. And one of the easiest way to get into large enterprises is through the downstream vendors," explains **David Allott**. "Often the biggest hurdle, when we are talking about security to smaller companies, is they don't think what they are doing is important to a hacker. We have to make them aware of their relevance to effective cybersecurity."

For small and medium-sized enterprises (SMEs), the rise of mobile technology, the cloud, the internet of things and other interactive technologies has created more business opportunities by allowing them to connect more easily with larger companies as vendors or contractors. At the same time, it has also created additional risk.

"The boom in the internet of things means a huge number of new devices will be connecting to the network. Where these devices have poorly secured access points it can give hackers a foothold into the network.", **Tim Goodwin** says.

Cyber attackers have gained access to some large companies through supply chains that lacked effective protection. "Third-party vendors – who are usually SMEs – are a risk because they might lack elaborate security systems. They are often, unconsciously, providing sophisticated hackers with the platform to gain access to company information and data. In response, some large companies are becoming more knowledgeable and spend time carrying out due diligence activities or developing and enhancing the IT security systems of their vendors to prevent hackers and other unauthorised individuals or organisations from getting in," **Ryan Rubin** says.

David Allott notes that SMEs should invest in the necessary IT tools and talent to prevent attacks on their own businesses, as well as those on their customers. "Attacks on SMEs continue to be a significant proportion of total attacks, simply because they are not implementing basic security controls. They take those vulnerabilities to their larger contracted customers and introduce those vulnerabilities into their networks."

⁴ GOV.UK, [Cyber Security Breaches Survey 2016](#)





Talented teams to tackle threats



More companies are investing in various platforms and tools designed to protect IT systems and networks. Not surprisingly, the escalating fear of data theft, hacking and fraud, compounded with many staff working remotely and with multiple devices (including BYOD) means an increased demand for IT security specialists.

Cybersecurity experts with the specialist skills needed to help companies recognise and protect themselves against key data security risks are in high demand but, at the same time, challenging to find. *“New technologies raise new security concerns. This trend has resulted in an IT security skills gap since the available expertise has not kept pace with the evolving IT threats,”* says **Phil Sheridan**.

77%

of UK CIOs say they will face more security threats in the next five years due to a shortage of IT security talent.

Ryan Rubin reaffirms that demand for IT security specialists is outstripping the number of people entering the market. *“Due to the dichotomy of technology and the interaction required with the business, there is a skills shortage in national and global markets. As the IT security field hasn’t reached its full maturity, finding professionals with the multidisciplinary skills required can be challenging. As such, retaining these professionals can often be higher on their business agenda for exactly the same reason. One way to ensure a larger influx of available and skilled talent is for the industry to promote IT, especially IT security as an attractive career path. Through strong educational options, IT security professionals will only see their career options improve.”*

David Allott agrees, and Intel Security has begun partnering with universities to create some additional awareness about the future of IT security. *“The goal is to get students involved in learning about cybersecurity. These partnerships will allow us to get students interested in internships and to position cybersecurity as an interesting and rewarding career plan.”*





IT security requires a flexible staffing approach

More companies are hiring permanent IT security professionals. Thirty-four per cent of UK CIOs are planning to increase headcount due to IT risk and security.

The positions that are most in demand are IT Security Analyst (junior), Information Security Officer (mid-level) and Security Operations Officer (mid-level). Companies need to make sure they have the necessary talent to tackle challenges at multiple levels within the organisation.

While having in-house IT security experts is preferable, businesses are changing their hiring strategies to facilitate a mixed workforce of permanent and contract specialists, including external risk consultancies.

New technological investments, business planning systems and migration projects prompt companies to continue to rely on contract and consulting professionals. The appeal of having experts on hand when needed is expected to increase with 27% of UK CIOs saying they will increase the number of contract IT security professionals in the next 12 months. Companies are more attracted to the kind of flexible management method that is achieved by combining permanent and contract employment.



Source: Independent survey commissioned by Robert Half of 100 UK CIOs. Responses do not total 100% due to rounding





CISO, the new IT security power player

Companies are gradually appreciating the importance of hiring a Chief Information Security Officer (CISO) who is not only the key player in efficiently managing the IT security process but also in enhancing internal security awareness across the organisation. Today's CISO is a senior professional with extensive experience in cybersecurity, governance, risk management and compliance, who is able to effectively manage a team and clearly articulate IT security issues and their implications – as well as insights and solutions – to senior stakeholders.



AN EFFICIENT IT SECURITY SPECIALIST:



Understands

the risks related to the security of information or data



Analyses

where security breaches have occurred or where potential security breaches could occur



Strengthens

IT systems and networks to prevent, detect and minimise the impact of attacks



Communicates

IT security risks and implications for the business, thereby increasing overall security awareness





Cybersecurity skills are a hot commodity

Because companies are confronted with additional security concerns, including mobile, application and big data analytics security, several areas are experiencing higher demand for specialised skills. These skills revolve around security prevention, intrusion, access and identity control and malware protection. However, as cybersecurity pervades all parts of an enterprise, IT specialists need to understand the significance of corporate governance, risk management and regulatory compliance if they want to design and build an effective security infrastructure.

“The most sought-after candidates are familiar with new software and hardware, have an understanding of emerging systems and are able to confidently use devices and related applications.”

Phil Sheridan, Senior Managing Director, Robert Half

While IT security professionals are expected to be foremost proficient in cloud security, IT security technologies and big data/data analytics, together with security architecture and hacking/penetration testing, turn out to be the most challenging security skills to find, thereby highlighting the IT security skills gap. **Phil Sheridan** recognises that having a robust talent management programme is essential to efficiently manage the IT security skills shortage. *“If companies want to stay abreast of industry developments and efficiently deal with IT security, they need to assess which expertise is missing in-house and either invest in training programmes for existing IT professionals or hire additional IT security experts.”*






The ever-changing technology environment makes it very important for IT professionals to continuously update their technical skills to stay current with the latest industry developments. Companies are also organising professional development and training programmes.










TOP FIVE TECHNICAL SKILLS IN IT SECURITY

Most in demand

	Cloud security	51%
	IT security technologies*	47%
	Big data/data analytics	37%
	Applications security	30%
	Hacking/penetration testing	30%

Most challenging to find

1		Cloud security	32%
2		IT security technologies*	29%
3		Security architecture	26%
4		Hacking/penetration testing	26%
5		Applications security	22%

Source: Independent survey commissioned by Robert Half of 100 UK CIOs.

*IAM, SIEM/SOC, DLP, malware protection

Along with the technical skills and the expertise that are necessary for a specific position, the so-called soft skills have also become substantially more important. The ability to analyse data and provide insights, as well as have strong business acumen and communication skills, have developed into essential core skills for an [IT security role](#).

In an environment where change is constant, **Phil Sheridan** recognises that well-developed soft skills are in greater demand. *“There is no doubt that highly specialised technical skills are vital. But the ability to clearly articulate cybersecurity issues in a language that senior management and non-IT employees understand will not only increase security awareness but also enhance the reputation of the IT department as business partners who add value across the business.”*





IT security checklist

CIOs and IT directors play a key role in protecting and directing a company's response to IT security risks. They operate in a rapidly changing technological environment that requires constant reviewing of their security programmes. CIOs and IT leaders need to keep in mind six core steps when developing and implementing an effective security programme.



1. Be proactive: develop a policy that will help your company prevent and defend itself against cyberattacks. Instead of waiting for a breach, assume one will happen and plan accordingly. Establish a security baseline with company leaders and key stakeholders to ensure the core business priorities have the highest level of security, as well as the necessary measures to effectively respond to security breaches. The company's overall risk appetite will then be able to help guide the security investment and activity required.



2. Use big data and analytics: use the available data to identify which risks are emerging and receding and in which areas you need to implement additional cyber defences. You need to have a plan in place. There are many IT security tools available and – depending on resources – you need to tick the boxes to make sure you cover all possible cybersecurity risks.



3. Treat IT security as a continuous enterprise-wide process: while conducting thorough risk and threat analyses, consistently test and re-evaluate existing processes and systems that are designed to minimise the inherent risks. Include the management, assessment and monitoring of the potential risks of vendors and suppliers in your analysis. As cybersecurity evolves, your IT security strategies need to evolve.



4. Have the necessary skills: while the demand for cybersecurity experts is outstripping supply, companies are confronted with a global IT security skills gap. In order to secure the necessary expertise, create a talent pipeline by investing in your existing IT professionals through extensive training, or by hiring additional team members. Also, consider the option of using contract IT professionals or an external consultancy.



5. Get everyone involved: make everyone in the company aware of the risks associated with email, social media and confidential information. Not only do you need to make senior management aware of IT security risks; a basic awareness across the entire organisation is essential.



6. Support training: encourage regular training of all personnel on cybersecurity policies and corporate practices. Go beyond the obligatory email to staff informing them of the risks and support training on safe email, password creation and website and social media practices.



Conclusion

Cybersecurity experts assume that a security breach is inevitable. Successfully confronting escalating IT security threats requires an enterprise-wide response based on a strategy that embraces technology and people, and has the support of senior management and company boards. But it doesn't stop there. Continuously reviewing the effectiveness of security controls is essential to managing today's threats and also the threats that organisations will face in the future.

The dramatic rise in cyber breaches has lifted the demand for cybersecurity experts. An insufficient number of new specialists entering the IT market has forced organisations to consider effective retention programmes, training existing staff, recruiting from overseas, partnering with educational institutions and developing flexible hiring policies that include both permanent and contract specialists. **Phil Sheridan** concludes: *"A dynamic IT strategy that brings together the right fit of technology and people is the cornerstone for companies protecting their future."*

Acknowledgements

We would like to thank the following interviewees for their participation and contributions to this report:

David Allott, Regional Director, Product & Solution Marketing Asia Pacific, **Intel Security**

Ryan Rubin, Managing Director, Security & Privacy, **Protiviti UK**

Tim Goodwin, Channel Director EMEA, **CyberArk**

Phil Sheridan, Senior Managing Director, **Robert Half UK**, UAE and South America

Research methodology

This annual study was developed by Robert Half UK and was conducted by an independent research company. The study is based on more than 100 interviews with senior IT and technology executives from companies across the UK, with the results segmented by company size, sector and geographic location.



About Robert Half Technology

Founded in 1948, Robert Half is the world's first and largest specialised recruitment consultancy and a member of the S&P 500. [Robert Half Technology](#) is the leading provider of highly skilled technology professionals for initiatives ranging from web development and multiplatform systems integration to network security and technical support on a permanent and contract basis.

Robert Half is also the parent company of Protiviti, a global business-consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through its Enterprise Solutions practice, the two organisations offer a unique proposition, providing the deep expertise, skills and methodology of a leading global consultancy with the flexibility of responsive recruitment.

0808 169 2340
roberthalf.co.uk



 **Robert Half**[®]
Technology

