# CYBER-SECURITY

## Defending your future

## EARLY ADOPTORS WIN

### The right IT talent for new security risks

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

According to PwC[1], the average number of global security incidents increased by 38 per cent in 2015, resulting in a 56 per cent increase in the theft of hard intellectual property over 2014.

Incidents like these impact the entire business and leave a trail of financial, operational and reputational damage. The days when cyber-security 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'.

**David Jones**, Senior Managing Director, Asia Pacific 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 cyber-security."*

[1] PwC, *The Global State of Information Security Survey 2016. Turnaround and transformation in cybersecurity*

## Contents

# An enterprise-wide responsibility

According to a global analysis of data breaches by the Ponemon Institute, the average cost of a breach for a company was $US3.5 million in 2014, an increase of 15 per cent over the previous year[2]. 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 an organisation's broader risk management framework, and not be viewed as just an IT problem.

**69%** of Hong Kong CIOs say the number of detected security threats has increased compared with 12 months ago

## TOP 3 IT SECURITY RISKS FACING ORGANISATIONS

**64%**
Data abuse/data integrity

**55%**
Spying/spyware/ransomware (economic espionage)

**44%**
Cyber-crime (fraud, extortion and data theft)

Source: Independent survey commissioned by Robert Half among 100 CIOs in Hong Kong – multiple answers allowed.

Seventy-four per cent of Hong Kong CIOs say their non-IT senior management has a good-to-excellent understanding of their company's information security exposure. **Chris Grant**, 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 on an enterprise-wide approach to tackle cyber-security and executives play a key role. A company's board and leaders need to be fully engaged with the organisation's security practice in order for cyber-security measures to be successful."*

[2] 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 the business from *external* security attacks. But organisations now face a growing risk in the form of potential *internal* security threats.

One major internal threat is when organisations have a Bring Your Own Device (BYOD) policy that allows their employees to bring their own laptops, tablets and smartphones to work. BYOD arrangements present 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.

*"Many organisations overlook the biggest source of cyber-breaches because they assume a mutual interest in the success of the company will provide automatic immunity against any cyber-threat. Employees are the biggest security threat, but also part of the solution. If you put the right control practices and arrangements in place, then you can mitigate that risk to some extent,"* says **Ewen Ferguson**, Managing Director at **Protiviti**.

**74%** of Hong Kong companies allow their employees to access corporate data on their personal devices

## TOP ACTIONS TO PROTECT CORPORATE DATA ON EMPLOYEES' PERSONAL DEVICES

**57%** Deploy mobile device management technology to enforce enhanced protection

**56%** Request employees sign an acceptable usage policy for keeping company information secure

**51%** Provide training to employees on maintaining security on personal devices

**45%** Implement authentication and authorisation to grant access to the corporate network

Source: Independent survey commissioned by Robert Half among 100 CIOs in Hong Kong – multiple answers allowed.

# Strategies for defeating cyber-risk

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.

In response, businesses are designing data security strategies which consider the probable level of threats that organisations will face in the future, rather than simply focusing on the business' 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 **Ewen Ferguson** observes: *"Companies that operate in the same industry are increasingly sharing information about the threats and risks they face, and the measures they take to combat them. Because the threats are often similar across the same industry, sharing information can enable a quicker and more effective response."*

## KEY CHARACTERISTICS OF AN EFFECTIVE IT SECURITY PROGRAM

1. **Has effective governance in place with an overarching view.** An IT security strategy has an impact on the entire organisation and needs to be aligned with broader Enterprise Risk Management and business objectives, compliant with regulation, and reviewed and updated for best practices.

2. **Takes a risk-based approach to cover the enterprise's operations and supply chain, including third-party vendors.** The increase in third-party threats are forcing a growing number of contracting organisations to undertake their own evaluation of a vendor's cyber-security 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 cyber-security policies and corporate practices is essential.

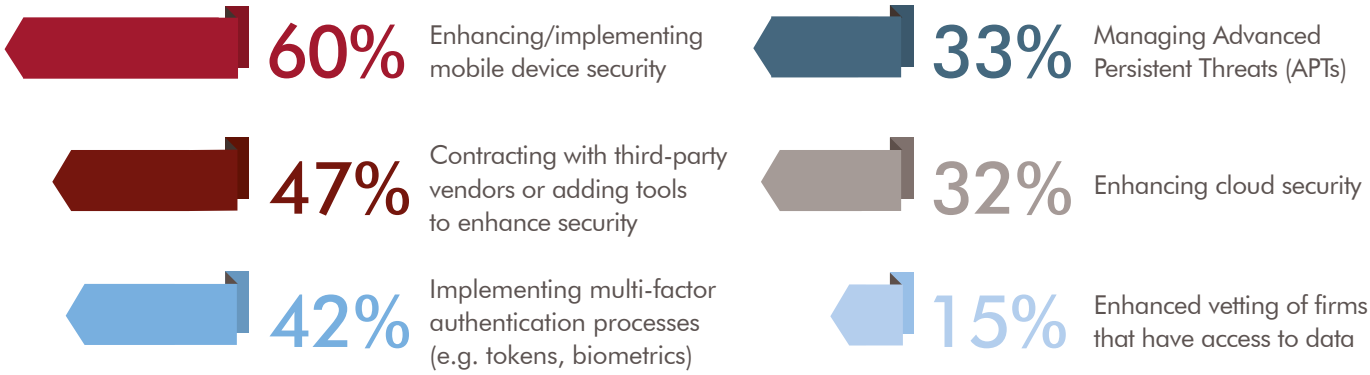
Source: Chris Grant and Ewen Ferguson, Managing Directors at Protiviti

> *"The thrust of the last couple of years in security has been about protecting the organisation from security breaches. That has now changed. Companies know they are going to get hacked. They therefore need to be able to respond."*
>
> **Chris Grant, Managing Director at Protiviti**

Companies recognise they must adjust their approach to today's business life. 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 for many companies is to rethink their IT security practices and to implement an integrated approach to preventing, detecting and mitigating cyber-security risks.

**7 out of 10:** The average score companies in Hong Kong give themselves when it comes to how well their company is prepared for protecting itself against security breaches

## MEASURES COMPANIES ARE TAKING TO ENHANCE IT SECURITY




Source: Independent survey commissioned by Robert Half among 100 CIOs in Hong Kong – multiple answers allowed.

# CASE STUDY:
# Cyber-security for auto firm to outpace hackers

## The project
Global computer security software company, Intel Security, undertook a cyber-security 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,** Regional Director at **Intel Security's** Product & Solution Marketing Asia Pacific says: *"Security is often broken up by separate units: endpoint security, network security and data centre security. These individuals or sub-units 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 which 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 cyber-security threat landscape, automation is a fundamental requirement when a company operationalises its security internally,"* he says.

Driven by IT security specialists, he agrees that the people component is vital when addressing cyber-security 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

In recent years larger companies have invested in cyber-security 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 ways 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 cyber-security."*
>
> **David Allott, Regional Director,**
> **Product & Solution Marketing Asia Pacific at Intel Security**

For SMEs, the rise of mobile technology, the cloud and other interactive technologies have 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.

Cyber-attackers have gained access to some large companies through their supply chain that lacked effective protection. *"Third-party vendors – who are usually SMEs – are at risk because they may lack elaborate security systems. They are often – unconsciously – the reason why companies get hacked. In response, some large companies spend time developing and enhancing the IT security systems of their vendors to prevent hackers and other unauthorised individuals or organisations from getting in,"* says **Chris Grant**.

**David Allott** agrees with this trend: *"Attacks on SMEs continue to be a significant proportion of total attacks, simply because they are not implementing basic security controls. They take vulnerabilities to their larger contracted customers and introduce those vulnerabilities into their networks."* This trend highlights the need for SMEs to invest in the necessary IT security tools and specialised IT talent.

# 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.

Cyber-security experts with the niche 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 **David Jones**, Senior Managing Director, Asia Pacific at **Robert Half**.

**82%** of Hong Kong CIOs say they will face more security threats in the next five years due to a shortage of IT security talent

**Ewen Ferguson** reaffirms that demand for IT security specialists is outstripping the number of people entering the market. *"Many companies resort to overseas recruitment because the talent pool in their national market is not sufficiently large. They also place staff retention higher on their business agenda because of exactly the same reason. One way to ensure a larger influx of available talent is for the industry to promote IT, especially IT security and computer science, as an attractive career path."*

**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 cyber-security. These partnerships will allow us to get students interested in internships and to position cyber-security as an interesting and rewarding career plan."*

## IT security requires a flexible staffing approach

More companies are hiring permanent IT security professionals. Almost half (45 per cent) of Hong Kong CIOs say that most extra jobs will be created in IT security, compared with 38 per cent who refer to software development, 33 per cent to data/database management and 30 per cent to technical support/helpdesk. Only applications development precedes IT security with 51 per cent who say most jobs will be created in this functional area.

The positions that are most in demand are Cyber-security Engineer (junior to mid-level), IT Auditor (junior to mid-level), Lead Security Architect (mid-level to senior), Information Security Analyst (junior to mid-level) and IT Risk Officer/Manager (mid-level to senior). 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 strategy to include a blend of permanent and temporary specialists plus 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 rise with 20 per cent of Honk Kong 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.

### HIRING PLANS FOR IT SECURITY PROFESSIONALS IN THE NEXT 12 MONTHS

| Permanent positions | | Contract positions |
|---|---|---|
| **20%** | EXPANDING | **20%** |
| **60%** | MAINTAINING | **51%** |

Source: Independent survey commissioned by Robert Half among 100 CIOs in Hong Kong.

## CISO, the new IT security power player

Companies are gradually appreciating the importance of hiring a Chief Information Security Officer (CISO), who not only takes the lead in efficiently managing the IT security process, but also enhances internal security awareness across the organisation. Today's CISO is a senior professional with extensive experience in cyber-security, 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.

### COMMON TRAITS OF AN EFFICIENT IT SECURITY SPECIALIST


**Understanding**
the risks related to the security of information or data.

**Analysing**
where security breaches have occurred or where potential security breaches could occur.

**Strengthening**
IT systems and networks in order to prevent, detect and minimise the impact of attacks.

**Communicating**
IT security risks and implications for the business thereby increasing overall security awareness.

## Cyber-security skills, a hot commodity

Because companies are confronted with additional security concerns, including mobile, application and Big Data analytics security, specialised skills are in higher demand. These skills revolve around security prevention, intrusion, access and identity control, and malware protection. However, as cyber-security 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 security software and hardware, have an understanding of emerging protection systems and are able to confidently use devices and related applications."*
>
> **David Jones, Senior Managing Director, Asia Pacific at Robert Half**

While IT security professionals are expected to be foremost proficient in cloud security, this skill is also the most challenging security skill to find, thereby highlighting the IT security skills gap. **David Jones** recognises that having a robust talent management program 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 programs 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 programs.

## TOP 5 TECHNICAL SKILLS IN IT SECURITY

| | Most in demand | | Most challenging to find | |
|---|---|---|---|---|
| 1 | Cloud security | 49% | Cloud security | 37% |
| 2 | Application security | 41% | Regulation and compliance | 30% |
| 3 | IT audit | 36% | Hacking/penetration testing | 29% |
| 4 | Hacking/penetration testing | 35% | IT audit | 28% |
| 5 | Big Data/data analytics | 34% | Big Data/data analytics | 26% |

Source: Independent survey commissioned by Robert Half among 100 CIOs in Hong Kong – multiple answers allowed.

Along with the technical skills and expertise 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 a strong business acumen and communication skills, have become core skills for an IT security role.

In an environment where change is constant, **David Jones** 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 cyber-security 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 technology environment that requires constant reviewing of their security programs. These six core steps can help them develop and implement an effective security program.

- **1. Be proactive:** Develop policies and processes that will help your company prevent and defend itself against cyber-attacks. Instead of waiting for a breach, assume one will happen and plan accordingly. Ensure that the organisation has the necessary measures to efficiently respond to security breaches. Procrastination is not an option in today's market.

- **2. Use Big Data:** 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 have covered all possible cyber-security risks.

- **3. Treat IT security as a continuous enterprise-wide process:** To conduct 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 cyber-security evolves, your IT security strategy needs to evolve.

- **4. Have the necessary skills:** As the demand for cyber-security experts is outstripping supply, companies are confronted with a global IT security skills gap. 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 cyber-security policies and corporate practices. Go beyond the obligatory email to staff informing them of the risks and support training on safe email, password creation, website and social media practices.

# Conclusion

Cyber-security experts assume a security breach is inevitable within most companies. 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 manage today's threats and also the threats that organisations will face in the future.

The dramatic rise in cyber-breaches has raised the demand for cyber-security experts. An insufficient number of new specialists entering the IT market has forced organisations to consider effective internal training and retention programs, recruiting from overseas, partnering with educational institutions and developing flexible hiring policies that include both permanent and contract specialists. **David Jones** concludes: *"A dynamic IT security strategy that brings together the right mix of technology and people is the cornerstone for companies defending their future."*

### Research methodology

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

# 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

Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world.

**Ewen Ferguson**
Managing Director, Protiviti

Protiviti, a wholly owned subsidiary of Robert Half, is a global business consulting and internal audit firm. Protiviti helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance.

**Chris Grant**
Managing Director, Protiviti

Protiviti, a wholly owned subsidiary of Robert Half, is a global business consulting and internal audit firm. Protiviti helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance.

**David Jones**
Senior Managing Director, Robert Half Asia Pacific

Robert Half is the world's first and largest specialised recruitment consultancy and a member of the S&P 500. Founded in 1948, the company has over 325 offices worldwide providing temporary, interim and permanent recruitment solutions for accounting and finance, financial services and technology professionals.

# About Robert Half

Robert Half is the world's first and largest specialised recruitment consultancy and a member of the S&P 500. Founded in 1948, the company has over 325 offices worldwide providing temporary, interim and permanent recruitment solutions for accounting and finance, financial services and technology professionals.

roberthalf.com.hk

Robert Half®