Understanding the new cyber reality
Information Security Study 2015
Deloitte China and ACCA
Introduction

Our world is digital and digitalisation has altered all elements of our day-to-day life. We have more access to news and information, more ability to research, a vast range of entertainment options and freely accessible modes of communications. As individuals this has changed our interactions and our consumption patterns.

In response, businesses have had to change their models and processes. In doing so they have become more open by introducing multiple touch points for stakeholders wanting to interact with them through websites and social media.

Boundaries are being broken down as markets are no longer defined by location but by consumer interest and behaviours. New players are emerging with business models that tear up the textbook, and the opportunities to create and reach new online communities are expanding each and every day.

There are now over 3.4 billion Internet users in the world, which is over 46% of the population. In 1995, only 1% of the population had Internet access. Even as growth of the penetration rate slows, it is still expected to expand year-on-year by around 7% on current trends. More importantly, nearly half of this strong growth is coming from Asia, home to some of the most appealing consumer bases in the years ahead.

With this new opportunity comes threats.

The growing points of contact between the digital world and the physical world offer more opportunities than ever for attacks on businesses and individuals. These cyber attacks are constantly evolving, meaning that defining them is complex. Hacking is becoming a phenomenon that can be purposeful or purposeless. Data security of companies and their clients, access to internal or private correspondences, theft of identity, branding or IP are all new and dynamic risks.
Statistics revealed at the Cyber Security Summit Hong Kong in May 2016 showed that the number of computer crime cases in the city increased from 1,506 in 2009 to 6,862 in 2015, resulting in a financial loss of US$234.5 million.

Globally in 2014, five out of every six large companies (those with more than 2,500 employees) were attacked, a 40% increase on the previous year. Small and medium-sized businesses also saw an increase, with attacks rising 26% and 30% respectively. More than 317 million new pieces of malware were created in 2014, meaning nearly one million new threats were released into the digital world each day.\(^2\)

The soaring costs of cyber attacks should not only be measured in monetary terms such as revenue, costs of litigation and insurance premiums. Victims will also suffer from the intangible loss of customer trust and loyalty. According to a global insurer, cyber attacks cost businesses as much as US$400 billion a year, which takes into account the initial damage as well as ongoing disruption. By 2020, research firm Gartner expects companies across the globe to spend about US$170 billion on cyber security, a growth rate of almost 10% during the next five years.\(^3\)

It is with this landscape in mind that Deloitte China and the Association of Chartered Certified Accountants (ACCA) conducted a survey to gather the views of a range of business leaders throughout Mainland China and Hong Kong to take a pulse check. We wanted to know what cyber attacks they had experienced, how they were reacting to these and what the future trends might be.

Cyber threats are here and what we see today will have fast evolved by tomorrow. To defend your business from those threats and increase your company’s cyber resilience, we encourage you to prepare, anticipate, learn and evolve.

We hope that this report will provide some insight and some fuel for the internal conversations that need to happen in a wide range of businesses.

Eva Kwok  
Partner, Enterprise Risk Services  
Deloitte China

Eunice Chu  
Head of Policy  
ACCA Hong Kong
Cyber threats have become part of the new normal.

For years companies broke out digital strategies as an independent business focus, but this is no longer practical or realistic. All businesses big or small are now digital through building product, research, logistics, distribution, marketing or selling.

The pace has been relentless and so it is inevitable that some areas have failed to keep up, this would seem to be the case for cyber resilience. Technology has plunged into new areas of hardware and software, presenting a battleground with multiple points of potential weaknesses in any business operating model. Those who are the brave adopters of emerging technologies, and in the vanguard of development, are at risk if they are not working to develop their levels of protection at an equal pace.

Beyond the loose term of ‘cyber threats’ there are a multitude of different aspects that need to be understood. These include denial of service, hacking, identity theft, data misappropriation, fraud and online misrepresentation, to name some of the more familiar types. These can come from anywhere in the world at any time. They can be launched as planned and controlled attacks for political or economic reasons, or by talented individuals for whom it is a pastime without malicious intent.

However, the nature of the threats is not always external. Many of the threats come from within a firm, often from its own employees. There are incidents of these being intentional, but the threat can equally come from negligence or a lack of security awareness that opens a system up. Examples could be visiting an unsafe website, clicking on a link from an unknown source or being tricked into providing personal data and passwords. The weak spots in the physical infrastructure, such as a server room, could also be a source of threats.

The nature of cyber threats is multi-faceted and complex, and to date insufficiently regulated. Legal systems and governance are racing to keep up with the developments in technology. The cross-jurisdictional and multi-disciplinary nature of cyber security makes it harder for governments to come up with an effective regulatory framework.

This puts more onus on the individual firm to take responsibility for protecting themselves as the options for recourse are insufficient. Given the evolving nature of cyber threats, protection is not an off the shelf product, but an ongoing commitment throughout the journey.
Five key insights
The Deloitte China and ACCA Information Security Study 2015 gathered the views of over 300 individuals in Hong Kong and Mainland China - most of them CFOs and CIOs from a range of industries including consulting and CPA firms, consumer business, global financial services industry, manufacturing, energy & resources, life sciences & healthcare, public sector, real estate and technology, media & telecommunications (TMT).
The findings highlighted what the respondents had experienced and how they reacted to cyber threats, as well as their strategy for strengthening their organisation's cyber resilience. The following insights were drawn from a thorough analysis of the survey findings:

Insight 1: There is no place to hide.
An alarming finding from our research was that all industries were potentially under cyber attack to a greater or lesser degree, showing that no firm has a place to hide. On a positive note, however, the results showed that there is an increasing awareness of cyber threats, whether they have actually been experienced or not.

Later in this report we look at a few vulnerable industries and analyse why they are often the targets of attack.

Insight 2: Defensive frailties.
The survey found that organisations are still taking tactical decisions around the implementation of cyber security. There are not many instances where the entire firm is joined up in defence. This may lead to actions being taken that are too narrow in scope to have a big impact, or leave the firm exposed around the ill-protected edges of a development.

Insight 3: Need for speed.
Although one third of the respondents’ organisations were able to resolve a security breach or incident in less than a month, there were plenty of examples of incidents dragging on without being fixed and subsequently incurring increased costs.

While a quick reaction will help reduce the financial losses incurred by an information security incident, many failed to acknowledge the intangible factors and under the surface costs that companies might suffer if they are on the wrong side of an attack.

Insight 4: Investment falling behind.
More trends show that developments in emerging technology are attracting more and more attention and investment dollars. Consequently information security may not be an easy sell in the boardroom. Other technologies may have clearer benefits for growth and risk prevention is not always a positive conversation to have. This may be placing a larger burden on practitioners who need to position themselves appropriately to pitch for resources and persuade decision-makers.

Insight 5: Legal matters.
The consequence of handling an attack poorly goes beyond IT system breakdowns, as there is now a risk of regulatory punishment.

In Hong Kong there is an increasing focus amongst the regulators on enhancing the legal structure to support information security. Compared to other jurisdictions, Hong Kong and Mainland China do lag behind in terms of the development of an established approach to cyber security. This is partly due to the shortage of talent to support its wider progress currently.
Recommendations

Based on the analysis of the findings, the following practical recommendations are offered for firms to consider, no matter whether they are advanced or just starting to establish a robust corporate approach to cyber threats.

i) **Cyber threats are company-wide high profile business issues** that require executive and board level attention with leadership identified at all points of the business. Companies should:

- Develop a cyber risk heat map
- Develop key risk and performance indicators
- Undertake a cyber incident simulation
- Consider the risk element of innovation

ii) **Protect what matters.** Understand the biggest threats, and which assets are at the greatest risk. This will also help bring the concept of cyber threats to reality for internal stakeholders.

iii) **Preparing now isn’t an option, it’s essential.** Companies should realise that they must take action now in order to face information security challenges. Establishing practices on cyber resilience only after experiencing an attack has proven to be an invalid strategy with companies learning the hard way.

iv) **Prevention from within** is a necessary starting point. When it comes to mitigating the risk of malicious or accidental insider threats, organisations need to focus on employee education and data loss prevention. Firms should adopt data loss prevention (DLP) technology and Security Incident Event Management (SIEM) technology to locate, monitor, and protect their data and network—wherever it is within the organisation—so that they know who is doing what, with what data, in real time.

v) **Collaboration is key.** The concept of ‘I can manage and handle all’ is no longer possible, as many organisations lack the resources to defend themselves from cyber threats on their own. Integrating the efforts of an internal cyber security team, a third party security consultant and product vendor to secure, update and remediate a company’s cyber resilience will be an effective approach for managing threats in the new cyber reality.
Insight 1: There is no place to hide

Cyber crime is a growth industry. The returns are potentially high, and the risks are low. McAfee Secure estimated that the likely annual cost to the global economy from cyber crime is more than US$400 billion.⁴

All companies, big or small could be a target. According to a recent UK study, becoming a victim of cyber crime costs smaller firms between £65,000 and £115,000, and those worst hit suffered up to six breaches a year, pushing the total cost even higher.⁵

Malware has been released into the world at the rate of one million programmes per day and is evolving in its forms. In the past three years, ransomware has been spreading through e-mail attachments, infected programmes and compromised websites. It affected all organisations regardless of size and business nature. There were 50 new ransomware ‘families’ released in the first five months of 2016 alone.⁶

Criminals may execute fraudulent transactions with unauthorised access from system loopholes or encrypt your data and ask for a ransom to get the image removed or regain access to your files. According to the US Federal Bureau of Investigation’s Internet Crime Complaint Center, nearly 1,000 complaints were received between April 2014 and June 2015 against CryptoWall, a type of ransomware. During that period, victims reported more than US$18 million in losses.⁷

Computer crime cases in Hong Kong have been growing at a compound annual growth rate of 28.8% between 2009 and 2015. Financial losses due to technology crime have even increased by 85.4% annually between 2009 and 2015, reaching a historical height of HK$1.8 billion.

Our survey found that 28% of the respondents’ organisations had experienced an information security breach or incident in the past 12 months. Despite the seemingly low percentage, an important finding from our research was that within this figure, all industries were affected. Some firms have experienced as many as two or more incidents per month on average, highlighting the threat of repeated attacks.
On a positive note, the results from our survey showed that there is an increasing awareness of cyber threats whether the individuals have actually experienced one or not. About one third (28.9%) of the respondents rated data breaches as the biggest cyber threat to their companies in the next 12 months. 21.3% of the respondents believed their organisations are at high risk of receiving privacy complaints and 17% of them believed that hacktivism is the biggest threat to their organisation’s information security.

Some clear targets but no one is safe

Manufacturing
A comparatively high number, 41.8%, of the respondents from the manufacturing sector have experienced one or more information security breaches or incidents in the past 12 months. This is not an obvious target sector for cyber attacks, but could highlight a higher than average level of vulnerability.

Ricky Tung, Industrial Products and Services Leader, Deloitte China

As a team based in Beijing serving the wider region, we have been very aware of the increase in cyber attacks in the manufacturing industry reflected in this latest survey. Unlike the Financial Services industry the attacks tend not be overly sophisticated or serious, with the consequences perhaps being production halting – but clearly affecting businesses with alarming frequency. From our perspective, there are a couple of basic factors contributing to this.

Firstly, the ERP (Enterprise Resource Planning) systems in use tend to be highly efficiency driven with cost saving infrastructure setup and therefore not particularly security sophisticated, making them easy targets. Secondly, cyber threat awareness is not high across the industry and needs to be raised.

The Chinese government is encouraging a number of relevant industry initiatives such as ‘Intelligent Manufacturing’ and ‘Made in China 2025’. In pursuing these, the technology will inevitably improve and the amount of data being used will increase. This will force the hand in increasing the attention on cyber security.

When we talk to clients, we describe it as a transitional phase for the manufacturing industry. The initiatives will require more awareness of new and emerging technologies that are not on the firms’ radar currently. There will need to be more education on the developing risks involving important areas such as trade secrets.

The numerous cyber attacks in the industry that may have been shrugged off previously as insubstantive cannot be for much longer.
Life sciences and healthcare
There are other sectors where it is no surprise that the volume of attacks is high, for example the life sciences and healthcare sector. 40% of the respondents from the life sciences and healthcare sector we surveyed have experienced one or more information security breaches or incidents in the past 12 months.

Intellectual Property (IP) of pharmaceutical companies has always been the target of sophisticated Internet criminals. According to a report released by Deloitte’s Japan practice, cyber theft of IP cost the UK an estimated £9.2 billion, of which £1.8 billion was attributed to theft of pharmaceutical, biotechnology and healthcare IP.8

Cyber crimes committed against pharmaceutical companies were not just a ‘big company’ problem. A study by US-based technology company Symantec Corporation found that more than half of the malware targeting pharmaceutical and chemical companies affected firms that employ fewer than 2,500 people and 18% employed fewer than 250.

The higher percentage of incidents that took place within this sector could also be due to stricter rules within the industry regarding the reporting of breaches. As a result of the relatively high risk, the life sciences and healthcare sector saw some insurance premiums triple.9

Financial institutions
When we examine the targets of cyber attacks, it is impossible to overlook the financial sector, partly due to the high profile cases reported in the media and the high potential financial losses.

Another reason why the industry is such a prime target is that the business and technology developments that financial services companies are embracing in their quest for growth, innovation, and cost optimisation, are in turn presenting heightened levels of cyber risks.10

These innovations have most likely introduced new vulnerabilities and complexities into the financial services technology ecosystem, especially when the knowledge of the new technologies and cyber resilience of the systems were not jointly developed across the organisation.

An alarming report in May 2016 unveiled that the Hong Kong Monetary Authority received at least 22 cases of hacktivism from four local banks in May alone in which a total securities transactions of HK$46 million was made without the knowledge of the account holders. Only four similar cases were reported the month before.11

In the same month, a case of hacktivism in January 2015 against SWIFT was reported. Over the highly secured SWIFT network which allows banks to process transfer money internationally, unidentified hackers stole US$12 million in 10 days by sending false transfer instructions.12
Interview with a respondent from a Hong Kong-based multinational financial institution

In an interview with one of the survey respondents, we gained more colour on the topics from an individual dealing with this day to day.

Information security is now much more at the front of the public’s attention and a result of this is that it has become a business problem for the board. One of the drivers for this has been increased coverage in both trade and mainstream media. There has been more discussion and that has boosted awareness significantly. But in our experience, the fact that it reaches the board is just a step rather than the end result.

There is a lack of knowledge around information security among decision makers for a number of reasons, not least it is a new and evolving area. That has been one of my main challenges to try and educate the board directors and management as to the importance of cyber resilience in order to secure necessary funding. This is no easy task due to a general lack of knowledge in the area from the executives at this level.

You are competing with numerous other strategic imperatives so the pitch for resources, and the way it is positioned, needs to be thought through carefully. Even within the IT budget, cyber resilience is not a priority for many.

I’m led to believe that a number of our peers also lack crisis management plans and implementing one has been a particular area of focus for me. I believe that this is an important step for the management team to take responsibility and acknowledge that cyber resilience is not an IT issue, but a strategic one across all business lines. In terms of the budget I’m looking to secure 4-10% of IT spend to be allocated to information security based on current plans.

If I take a step back and look at the whole industry I think that as a collective body we lack the expertise, and in many places the resources, to solve this. There needs to be a bigger focus on training to increase the number of individuals involved in this important area.
Sound defence against cyber attacks requires a joined up effort across the firm, from the leadership to employees of all level, supported by a comprehensive build-out of hardware and software.

But our survey findings showed that only 50% of the respondents’ organisations had executive responsibility for enterprise-wide information security, either in the form of setting up the role of chief information security officer or escalating information security as a topic in the boardroom. This may lead to actions that are too narrow in scope to have an effective impact or exposure of the companies to cyber risk if the actions are not fully integrated.

Another point of interest from the survey was the fact that 60% of the respondents’ organisations do not provide training to employees to raise their information security awareness, or only do so when mandated by laws or regulations. Cyber threats could impact the entire business chain and well-trained employees who are risk aware are an integral part of the defensive solution. Not engaging individuals throughout the business will leave points of weakness.

In a sign that there are still a sizable number of organisations that are not giving sufficient attention to information security, nearly one in four had allocated no budget for information security in the coming three years. Even if budget had been allocated, whether this would be spent effectively would go back to the fundamental question of whether the right leadership and strategic planning are in place.

We had asked the respondents what their top five challenges were with regards to supporting information security within their firms:

**Insight 2: Defensive frailties**

**Chart 1: Top five information security challenges**

- Lack of documented or out-dated security policies and supporting guidelines and procedures
- Information leakage
- Lack of compliance to privacy regulations
- Lack of sufficient segregation of duties
- Insufficient monitoring and controls over third party outsourced vendor
Our survey didn't quantify the information security capabilities of respondents. However, the challenges identified by the respondents gave hints to a fundamental gap in capability.

We found from our survey results that organisations are still taking tactical decisions around the implementation of cyber security instead of an integrated approach to deal with cyber threats. The nature of the challenges identified shows that companies were still lacking some fundamental information security processes such as documented security policies. The views of the respondents showed a low level of maturity in companies’ defence against cyber threats.

This echoes the findings from security capabilities provider RSA’s Cybersecurity Poverty Index 2016 where the strongest reported maturity levels were in the area of protection - this function forms the basis of conventional security doctrine that is proving less and less effective over time in the face of advanced threats.13

Detection, response and recovery, which form the backbone of today’s effective security strategies, were not given enough consideration.

Only 50% of the respondents’ organisations had executive responsibility for enterprise-wide information security.
Insight 3: Need for speed

The cost to individual companies of recovery from cyber fraud or data breaches is increasing. Any cost of dealing with the aftermath of a cyber attack is often more expensive than the direct loss caused by the attack.

One study of the cost of cyber crime for Italy found that while the actual losses were only US$875 million, the recovery and opportunity costs reached US$8.5 billion.14

Speed is important in managing these issues. However, the gap in fundamental information security capabilities, as discussed in Insight 2, may lead to a longer lead time in detecting the attack, responding to it and recovering from it. This often results in significant damage to the organisation.

When we also asked in the survey about the length of time it takes to fix a security breach or incident, although many said it took less than a month, there were plenty of examples of incidents going well beyond this and subsequently incurring more costs. A separate study by Deloitte found that the average amount of time needed to resolve a cyber attack was 32 days with an average total cost of a little more than US$1 million.

Chart 2: Do you know the average time required for your organisation to resolve a security breach or incident?

- Less than 1 month: 33.4%
- 2 – 5 months: 2.0%
- 6 – 12 months: 15.0%
- More than 12 months: 3.3%
- Do not know: 46.3%
Another perspective on time vs cost in relation to resolving such an incident is that the impacts from a cyber attack can reverberate over many years. Legal costs can cascade as stolen data is leveraged in various ways over time; it can take years to recover pre-incident growth and profitability levels; and brand impact can play out in multiple ways.\(^\text{15}\)

The same is true for some of the intangible factors that firms who find themselves on the wrong side of a cyber attack might suffer. 22% of the respondents believed damage to the company's reputation was one of the major impacts to the organisation due to security breaches.

Above the surface cost impact for companies that have experienced a cyber attack may include technical investigation, customer breach notification, post-breach customer protection, regulatory compliance, public relations, attorney fees and litigation and cyber security improvement.

However, when a company tries to put a price-tag on the impact of a cyber attack, under the surface costs will also need to be taken into account. These costs include increased insurance premiums and cost of raising debt, impact of operational disruption and loss of customer relationship or contract revenue, devaluation of trade name and loss of intellectual property.\(^\text{16}\) The above and beneath the surface costs are a good indication to show that information security is not an IT problem alone.

While speedy reaction and remediation is desired, the quality of the fix is equally important. Trying to develop the processes for handling information security threats in the middle of an incident means a high chance of failure. Quick fixes are unlikely to be sustainable and the best way for a firm to manage a cyber threat is to have the policy framework in place and an agreed plan of action.

Just as preparation can help the speed of reaction to keep financial loss down, some intangible damage can be mitigated. Knowing who is responsible for communicating to the stakeholders and through what channel can go a long way to avoiding damaged relationships.

### Chart 3: What were the impact(s) to your organisation due to any security breaches over the past 12 months?

- **Loss of sensitive data**: 30.5%
- **Unauthorised public release of data**: 29.8%
- **Company reputation**: 22.2%
- **Not applicable**: 12.6%
- **Do not know**: 4.9%

The cost of a cyber attack may be the headline grabber, but in the end the real long term impact on the firm comes from elsewhere. In another recent Deloitte report, the costs or 'damage seen above the surface' is recognised much more widely. Cases of intellectual property theft, espionage and data destruction, as examples of those below the surface, are less understood and inadequately discussed.\(^\text{18}\)

Responding slowly, often due to a lack of preparedness, exponentially increases financial loss.
Anthem's Breach Response Evaluated

A blogger on the Wall Street Journal website critiqued Anthem's communications regarding a data breach. What did it do right?

A few weeks after Anthem Inc., one of America's leading health benefits companies announced it had been breached with nearly 80 million customers and employees potentially affected, Andrea Bonime-Blanc, CEO, GEC Risk Advisory was asked to evaluate the company's response. And here's her evaluation:

Anthem's immediate corporate response to its cyber breach crisis appears to be close to a textbook case of effective immediate crisis management and preparedness.

First, Anthem actually discovered the breach themselves – they weren't extorted by the hackers or outed by the media or others. This is good reputation risk management.

Second, Anthem immediately advised federal authorities of the breach and hired reputable cyber consultants to deal with immediate damage control. This too denotes the existence of internal preparedness.

Third, although applicable regulations appear to allow for a 60-day reporting window, Anthem decided to publicly announce its crisis within days of its first discovery. While perhaps risky, such a move can provide Anthem with longer-term reputation enhancement with key stakeholders, restoring and building trust and customer loyalty over time.

Fourth, the company provided clear and coherent messaging of what happened—down to the kind of information that might have been compromised—in easily available and clearly written materials, including special instructions and a website for the occasion.

Fifth, the CEO letter is an effective letter, addressing the concerns of key stakeholders (employees, customers, regulators and investigators) and providing them with immediate resources. In the letter, the CEO also apologises and brilliantly shows empathy with his customers and employees by referencing the fact that his personal data was stolen as well.

The only downside that I can discern from what has been reported doesn't have to do with Anthem’s crisis response but more with its risk preparedness regarding the apparent lack of encryption on the data that was stolen. However, this is more of a risk management issue that Anthem and its executives and board will now surely be focusing on as they begin build stronger cyber resilience.
Understanding the new cyber reality | Insight 3: Need for speed
Insight 4: Investment falling behind

The survey showed that 23% of respondents’ organisations had allocated no budget to information security for the coming three years. In the meantime, the findings showed that companies are more ready to spend on other emerging technologies more connected to business growth.

The preference is alarming. The company system is exposed to threat when information security is not keeping pace with technology adoption and business model changes, not to mention that adoption of emerging technologies is likely to increase the range of security threats.

Given some of the other findings, this lack of commitment to spending on this key area is surprising. But this was also backed up by Deloitte’s 2015 Global CIO (Chief Information Officer) Survey in which 58% of the CIOs picked cyber security as an area that will have the most impact on the business in the future, but current investments in the area was low. Only 23% of the CIOs placed high investment in cyber security. Levels of awareness seem to be high, but this is not reflected in spending. A plausible explanation is the greater appeal of other technologies in the boardroom. Information security needs to compete for IT budget and there are more popular trending developments in emerging technologies that are attracting attention and investment dollars. 71.4% of the respondents’ organisations have implemented emerging technologies such as mobile devices, analytics and cloud for example.

Investment in information security should go hand in hand with other technological investment and not be seen as an 'either, or' decision. Levels of awareness seem to be high, but this is not reflected in spending. A plausible explanation is the greater appeal of other technologies in the boardroom. Information security needs to compete for IT budget and there are more popular trending developments in emerging technologies that are attracting attention and investment dollars. 71.4% of the respondents’ organisations have implemented emerging technologies such as mobile devices, analytics and cloud for example.
Information security is not such an easy sell in the boardroom. Other technologies may have clearer benefits for growth, but risk prevention is not always a positive conversation to have. This may be placing a larger burden on practitioners who need to position themselves appropriately to pitch for resources and persuade decision-makers.

The Board preferences to favour investment options involving emerging technologies is likely to increase the range of security threats that the organisation faces by the fact that this is expansion into new territory. This 'adopt first, manage later' phenomenon could create significant challenges for the already insufficient information security to protect the future organisation.

It seems clear that firms should move more towards investment in information security should go hand in hand with other technological investment and not be seen as an 'either, or’ decision.

Some emerging technologies have risks of their own.²⁰

Mobile devices continue to grow in numbers and ubiquity, which inevitably makes them appealing to cyber criminals. Personal data contained on mobile devices will continue to be targeted for identity theft, but the range of expected threats will widen to include new areas in which mobile devices will be increasingly used, such as access to cloud data vaults, various business applications facilitated by flexible ‘bring your own device’ (BYOD) business policies, online banking and payment services, etc. This presents IT departments with new challenges, as they can no longer contain valuable data and hardware within a rigid perimeter that is easier for them to monitor and protect.

Cloud is expected to play a key role in the future development of IT; consequently, cloud data breaches, along with surveillance, will remain a major concern. New advisory and regulatory frameworks, as well as methodologies for due diligence checks and testing of performance and resilience are being developed to mitigate the risks.

Big data is going to present new opportunities for cyber crime because it potentially allows the so-called ‘salami slicing’ technique, whereby a large number of seemingly unrelated small data items can be tied together to reconstruct an overall picture and identify patterns that can be used for identity fraud, with devastating effect. There are also concerns over protection of sensitive information stored within big data.

The Internet of Things (IoT) is also likely to introduce quite a few surprises. For instance, someone with access to IoT data can get a very detailed view of a life in a so-called ‘smart home’, which could turn into a big privacy issue. Another potential issue is that poorly conceived hardware and firmware security can present hackers with gateways leading right into the hearts of private networks, with potentially disastrous results.
Insight 5: Legal matters

The implications of a cyber attack may be more than internal and financial. The potentially significant damage that can be done to reputation and client trust has been touched on above. But beyond this there is a risk of regulatory punishment.

In our survey, 14% of respondents experienced complaints related to non-compliance of data security measures or privacy breaches. Lack of compliance to privacy regulations was rated by the respondents as one of the top five information security challenges.

In Hong Kong there is an increasing focus amongst the regulators around enhancing the legal structure to support information security. The Personal Data Privacy Ordinance (PDPO) is a key piece of legislation that is evolving and putting the security of individuals at its centre. The philosophy of this has changed in recent years as well, with there being more emphasis on organisations to self-govern to an extent. The PDPO offers guidelines and best practices in most areas as opposed to mandatory measures, but there are fines and punishments available to the Commissioner if they determine that breaches of these have been made.

Legislative enactments relating to cyber security in Hong Kong are dealt with by both the PDPO and the criminal law. The Computer Crimes Ordinance was enacted in 1993 and its scope has been expanded to include computer related criminal offences. These include unauthorised access to any computer; damage or misuse of property (computer programme or data); making false entries in banks’ books of accounts by electronic means; obtaining access to a computer with intent to commit an offence or with a dishonest intent; and unlawfully altering, adding or erasing the function or records of a computer.

There is currently no mandatory data breach notification requirement in Hong Kong. The Office of the Privacy Commissioner for Personal Data (PCPD) has provided data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved.\(^1\)

Compared to other jurisdictions, Hong Kong and Mainland China do lag behind in terms of the development of structure and processes around
Tightening regulations will drive development of structure and processes around cyber security.

An often neglected aspect in information security regulation is the disclosure of information. Symantec suggested in the latest Internet Security Threat Report that the actual number of information security breaches could be much higher due to the increasing tendency of organisations to limit the information released about the extent of the breaches they suffer. It is estimated that the total number of identities exposed is likely to be at least half a billion.23

Government regulators, such as the US Securities and Exchange Commission (SEC), are now increasing their attention on the question of adequate disclosures in the event of cyber security breaches. This does not mean, however, that information will be quickly made available in order to help other potential victims. There have been attempts by some governments and their agencies to create information-sharing services.24

In view of this, the Hong Kong Monetary Authority (HKMA) has launched an initiative in May 2016 to strengthen the collective learning in the industry and for a recognised and officially endorsed set of professional qualifications. The financial industry is an important sector given its high vulnerability for attacks, and may be a vanguard for others to follow suit.

There are numerous cases of best practice in this area available, and recognising the global nature of these issues along with the benefits that could be gained from pooling resources, these developments will hopefully be aligned and not managed in isolation. This means collaboration with other countries and also across the public and private sector.

Cybersecurity Fortification Initiative – announced by Hong Kong Monetary Authority in May 2016*

The Cybersecurity Fortification Initiative (CFI) is a new, comprehensive initiative which aims to raise the level of cybersecurity of the banks in Hong Kong through a three-pronged approach:

First, a central element of the CFI is a Cyber Resilience Assessment Framework, which seeks to establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defence and resilience required;

Second, there will be a new Professional Development Programme, which is a training and certification programme in Hong Kong which aims to increase the supply of qualified professionals in cyber security; and

Third, a new piece of infrastructure, the Cyber Intelligence Sharing Platform, will be developed to allow sharing of cyber threat intelligence among banks in order to enhance collaboration and increase cyber resilience.

*Under consultation period and target to be effective by end of 2016
The survey and interviews have provided some key areas of insight that reflect some of the real challenges that companies across various sectors in Hong Kong and Mainland China are facing. Based on this we have a number of practical recommendations for firms to consider, no matter whether they are advanced or just starting to establish a robust corporate approach to cyber threats.

**Recommendation 1: Cyber threats are company-wide high profile business issues that require executive and board level attention with leadership identified**

Cyber threats are becoming more sophisticated and penetrating every aspect of the business. The infusion of cyber threats with traditional business risks result in a largely unfamiliar form of risk management, which executives and any board will be challenged by. Managing such risks is no longer the sole mandate of IT departments or CIOs and should be one of collective responsibility.

**Tonny Xue, National Leader of Cyber Risk Services, Enterprise Risk Services, Deloitte China**

There is no such thing as standing still in the cyber environment, which is moving in many directions simultaneously. It is without a doubt complex, you only need to look at the potential of the Internet of Things (IoT) to see how this makes it an invigorating but problematic area to work in.

I find myself talking more than I ever have before to companies about the nature of the risks from the cyber threats and how to handle the operational and reputational aspects. And one of my biggest concerns is that firms are not doing enough to raise their staff’s awareness of proper data handling which would effectively lower the chance of data breach incidents.

My most frequent pieces of advice that I give currently are listed below, and they are focused on how to increase understanding of the systematic approach that needs to be taken:

01. To develop a comprehensive cyber strategy

02. To perform maturity assessments against cyber threat readiness (see P.21)

03. To design protection plans based on the results of the maturity assessments to optimise and improve
Understanding the new cyber reality

Access your maturity level

01. Do the board and C-suite demonstrate due diligence, ownership and effective management of cyber risk?
02. Do we have the right leadership and organisational talent?
03. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
04. Are we focused on, and investing in, the right things?
05. How do our cyber security programme and capabilities align to industry standards and peer organisations?
06. Do we have an organisation-wide cyber-focused mindset and cyber-conscious culture?
07. What has management done to protect the organisation against third-party cyber risks?
08. Can we rapidly contain damage and mobilise diverse response resources should a cyber-incident occur?
09. How do we evaluate the effectiveness of our organisation’s cyber security programme?
10. Are we helping to protect our industry, the nation and the world against cyber risks by taking a holistic approach to knowledge and information sharing?

Depending on the level of maturity, organisational complexity and culture, some actions to consider when engaging business and executive leadership on cyber issues might include:

Develop a cyber risk heat map
Bring senior business leaders together with threat intelligence experts to identify the top areas of cyber risk. This can serve to both generate decisions on key areas of focus, or to begin an ongoing education and dialogue. Through the process, leaders may emerge who can spearhead pilot projects or play an ongoing role in building a corporate education programme.

Develop key risk and performance indicators
When communicating cyber risk, security leaders should highlight the most serious risks the business faces and the methods being employed to manage them. One way to achieve this is to shortlist the top cyber risks your company faces, establish risk indicators that signal your company’s level of exposure to them, and track how these trend.

Undertake a cyber incident simulation
Testing the ability of the top leaders to respond to a staged attack can identify areas for improvement. The greatest initial outcome may be to wake people up to the complex challenge and importance of being prepared.

Consider the risk element of innovation
The next time you build a new application or digital service, require that a cyber risk report be submitted before finalising the project plan that adequately addresses key risks. Mandate progress reports to enforce periodic risk evaluation once the initiative is rolled out. Identify key risk indicators associated with the innovation, and use this as a pilot for ongoing reporting requirements.
**Recommendation 2: Protect what matters**

To bring the concept of cyber threats to reality for stakeholders requires a clear view of the biggest threats and the assets that are at greatest risk.

Ask probing questions like who could potentially target your organisation, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack, and what is the potential impact to your business?

Questions such as these can help determine how advanced and persistent the cyber threats to your business are likely to be and work both internally and externally to reduce the risk exposure to acceptable levels. We have already noted that internal investment may be difficult to obtain, so it is important to have a clear view on what should be spent on first.

---

**Eunice Chu, Head of Policy, ACCA Hong Kong**

Cybersecurity is a complex issue. It can only be handled properly when companies and individuals understand they play an important role and take ownership of their responsibility, because neither governments and law enforcement nor IT professionals can be solely relied upon, to provide adequate protection.

According to a research report 'Cybersecurity- Fighting Crime's Enfant Terrible' jointly issued by ACCA and IMA in February 2016, professional accountants are well-positioned within business to help in dealing with risk management issues as they possess industry knowledge and understand the overarching strategy and end-to-end business operations. They can help in:

- Identifying the critical assets that are at risk and require protection,
- Assessing the cost-effectiveness of different security measures,
- Defining different levels of access rights,
- Quantifying the potential financial, operational and reputational damage and regulatory penalties.

In view of the rapid adoption of BYOD in businesses, cloud application, big data and the internet of things, ACCA understands the challenges that future accountants face and is determined to equip them with necessary training and knowledge to deal with the challenges. Cyber and information security training is incorporated into its examination syllabus (Paper P3) to equip accounting students with essential knowledge. Ongoing seminars and workshops on various topics, collaborated with multinational technology companies, are offered to its ACCA students and members. With all these measures, our well-trained accountants will prove to be valuable assets to the future business world.
Understanding the new cyber reality

**Recommendation 3: Preparing now isn’t an option, it’s essential**

The word ‘breach’ has been used more in an information technology context in the last two years more than it had ever been in the previous 20 years. Research and surveys around the globe have shared the same view that cyber attacks are happening in a more frequent, sophisticated manner and gaining a tremendous momentum. Mishandling of these threats has cost billions of dollars and this is set to increase.

All sectors and sizes are at risk and companies should realise a shift must take place now to adequately combat the challenges. Waiting to establish practices or make decisions on cyber security only after an attack has occurred is poor governance.

Beware also the existing dormant threat of malware that might be in your firm’s systems already as noted in the Deloitte report, *Beneath the surface of a cyberattack*. Any approach needs to secure the present as well as being resilient about the future.

**Recommendation 4: Prevention from within**

When it comes to mitigating the risk of malicious or accidental insider threats, organisations need to focus on employee education and data loss prevention. Basic security ‘hygiene’ should be drilled into employees.

Organisations should also be making use of DLP technology to locate, monitor, and protect their data—wherever it is within the organisation—so that they know who is doing what, with what data, in real time. DLP can block certain types of data from leaving an organisation, such as credit card numbers and other confidential documentation.

**Recommendation 5: Collaboration is key**

When managing cyber threats there is a need to act together. The concept of ‘I can manage and handle all’ is not possible and many organisations lack the required resources to be self-sufficient.

Very often, an extended team, including third party vendors, is deployed to perform operational and attestation tasks. But very rarely are they then integrated into the overall cyber security framework to enhance the secure and response capabilities of the organisation. This observation is common both in the commercial and public sectors across the Asia Pacific region.

A lack of integration creates unnecessary blind spots that are taken advantage of by cyber criminals who may be sharing and coordinating their attempts to compromise an organisation.

There is a need to rethink our outdated notions and apply this to plan how security practitioners should operate: integrating and coordinating among all three parties (internal cyber security team, extended cyber security team, third party product vendors) to secure, update and remediate an organisation’s prized assets.
Survey methodology

The Deloitte China and ACCA Survey was carried out in Q4 2015 and over 300 individuals in Mainland China and Hong Kong were surveyed. The respondents were mostly CFOs and CIOs from a range of industries including consulting and CPA firms, consumer business, global financial services industry, manufacturing, energy & resources, life sciences & healthcare, public sector, real estate, technology, media & telecommunications. The survey was conducted by sending out online questionnaires to collect feedback.

The purpose of the survey was to take a snapshot of how companies were managing cyber security, how recent attacks had manifested and what the trends in approaching the area were.

Deloitte China and ACCA, with a wide range of experience between them of the financial and operational challenges that cyber attacks cause, felt that this was an important time to conduct this research and to encourage more action and understanding of what cyber security needs to mean.
Understanding the new cyber reality | Survey methodology
Understanding the new cyber reality | Key survey findings

Key survey findings

Types of threats

Chart I: Rate the following threats according to how you view their impact on your organisation over the next 12 months (%)

![Chart showing rate of threats](image_url)
Understanding the new cyber reality

Chart I: Top five information security challenges

- Lack of documented or out-dated security policies and supporting guidelines and procedures
- Information leakage
- Lack of compliance to privacy regulations
- Lack of sufficient segregation of duties
- Insufficient monitoring and controls over third party outsourced vendor

Who is responsible for information security?

Chart III: Does your organisation have executive responsibility for enterprise-wide information security?

- Yes, have an executive responsible (eg Chief Information Security Officer)
- Yes, cybersecurity is one of the discussion topics at board meetings
- No
- Do not know

Chart IV: Does your organisation provide training to employees to raise their information security awareness?

- Yes
- Yes, only when mandated by laws/regulations
- No
- Do not know
Information breaches/incidents by sectors

Chart V: How many times has your organisation experienced an information security breach or incident in the past 12 months?

Chart VI: How many times has your organisation experienced an information security breach or incident in the past 12 months? (By sector)
The costs of security breaches

Chart VII: Do you know the cost to your organisation due to any security breaches or incidents over the past 12 months?

- Less than USD 64,999: 47%
- USD 65,000 – USD 149,999: 17%
- USD 150,000 – USD 350,000: 4%
- Over USD 350,000: 1%
- Nil: 1%
- Do not know: 30%

What were the impact(s) to your organisation due to any security breaches over the past 12 months?

Chart VIII: Are you aware of this situation?

- Aware: 69%
- Unaware: 31%

Chart IX: Bridge 'Aware' to the statistics below

- Loss of sensitive data: 12.6%
- Unauthorised public release of data: 4.9%
- Company reputation: 30.5%
- Not applicable: 22.2%
- Do not know: 29.8%
Understanding the new cyber reality | Key survey findings

Resolving security breaches takes time

Chart X: Do you know the average time required for your organisation to resolve a security breach or incident?

Investment in information security

Chart XI: Has your organisation implemented any emerging technologies over the past 12 months?

Chart XII: Has your organisation allocated any budget for information security in the coming three years?
Deloitte and ACCA contacts

**Eva Kwok**  
Partner, Enterprise Risk Services  
Deloitte China  
Tel: +852 2852 6304  
Email: evakwok@deloitte.com.hk

**Edmund To**  
Manager, Enterprise Risk Services  
Deloitte China  
Tel: +852 2852 5650  
Email: edt@deloitte.com.hk

**Eunice Chu**  
Head of Policy  
ACCA Hong Kong  
Tel: +852 2973 1108  
Email: Eunice.chu@accaglobal.com

**Yuki Qian**  
Head of Policy  
ACCA China  
Tel: +86 21 5153 5241  
Email: Yuki.qian@accaglobal.com
Endnotes

5. Cybersecurity – Fighting Crime’s Enfant Terrible, ACCA and IMA
13. RSA Cybersecurity Poverty Index 2016
19. 2015 global CIO survey: Creating legacy, Deloitte University Press
20. Cybersecurity–Fighting Crime’s Enfant Terrible, ACCA and IMA
24. Cybersecurity–Fighting Crime’s Enfant Terrible, ACCA and IMA
25. Cyber security: everybody’s imperative-A guide for the C-suite and boards on guarding against cyber risks, Deloitte
Deloitte Global

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (‘DTTL’), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as ‘Deloitte Global’) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte in Greater China

We are one of the leading professional services providers with 24 offices in Beijing, Hong Kong, Shanghai, Taipei, Changsha, Chengdu, Chongqing, Dalian, Guangzhou, Hangzhou, Harbin, Hefei, Hsinchu, Jinan, Kaohsiung, Macau, Nanjing, Shenzhen, Suzhou, Taichung, Tainan, Tianjin, Wuhan and Xiamen in Greater China. We have nearly 13,500 people working on a collaborative basis to serve clients, subject to local applicable laws.

About Deloitte China

The Deloitte brand first came to China in 1917 when a Deloitte office was opened in Shanghai. Now the Deloitte China network of firms, backed by the global Deloitte network, deliver a full range of audit, consulting, financial advisory, risk management and tax services to local, multinational and growth enterprise clients in China. We have considerable experience in China and have been a significant contributor to the development of China’s accounting standards, taxation system and local professional accountants. To learn more about how Deloitte makes an impact that matters in the China marketplace, please connect with our Deloitte China social media platforms via www2.deloitte.com/cn/en/social-media.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the ‘Deloitte Network’) is by means of this communication, rendering professional advice or services. None of the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. It offers business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its 188,000 members and 480,000 students in 178 countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of 100 offices and centres and more than 7,110 Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conduct relevant research to ensure accountancy continues to grow in reputation and influence.

As the first global accountancy body entering into China, ACCA now has 24,000 members and 71,000 students, with 10 offices in Beijing, Shanghai, Chengdu, Guangzhou, Shenzhen, Shenyang, Qingdao, Wuhan, Hong Kong SAR, and Macau SAR.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. It believes that accounting professionals bring value to economies in all stages of development and seek to develop capacity in the profession and encourage the adoption of global standards. ACCA’s core values are aligned to the needs of employers in all sectors and it ensures that through its range of qualifications, it prepares accountants for business. ACCA seeks to open up the profession to people of all backgrounds and remove artificial barriers, innovating its qualifications and delivery to meet the diverse needs of trainee professionals and their employers.

More information is here: www.accaglobal.com