# GHOSTS THE

# IN MACHINES

The incidence of cybercrimes is rising worldwide, and Hong Kong is not immune. George W. Russell asks experts about the latest weaponry on both sides and finds out how CPAs can be frontline soldiers in the battle against computer hacking

Illustration by Martin Megino

Once the purview of information technology departments constructing firewalls from obscure office corners, cyber-security has become a priority concern for companies large and small.

Recent headlines, including accusations last month by the United States that the Chinese military launched cyber-attacks on major U.S. corporations, have brought computer crime to the fore. (China denied the charges and accused the U.S. of orchestrating cyber-attacks on its territories.)

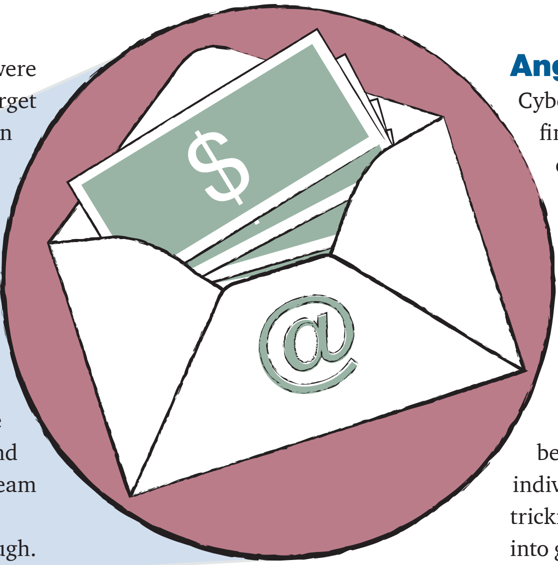
The diplomatic spat followed several high-profile data breaches in the U.S., including the compromise of more than 100 million customer accounts at retail giant Target in December 2013.

Some cyber-security experts say the decision last month by Gregg Steinhafel to resign as chief executive officer of Target is a wake-up call for local executives. "This is the first time I've seen accountability at this level," says Ramesh Moosa, a Forensic Services Partner with PricewaterhouseCoopers in Shanghai.

"Both the chief information officer and the CEO resigned on the back of a very big cybercrime incident, which I think is fairly pivotal," Moosa says of Target, adding that such concerns are now the talk of Hong

Kong boardrooms. (The resignations were followed by angry demands from Target investors calling for the defeat of seven members of Target's 10-person board at a meeting scheduled for early June.)

Repercussions such as the resignation of Steinhafel, a 30-year company veteran, have helped to focus the minds of directors in Hong Kong, Moosa suggests. "A lot of senior management and those sitting on the board, as they become aware of these high-profile cybercrime incidents, do tend to ask questions of their management team as to what is being done."



The answer, most likely, is not enough. "As the Red Queen found, in *Alice in Wonderland*, it takes a lot of running to stand still, although here the defenders are actually backsliding," says Colum Bancroft, Managing Director of Financial Investigations at Kroll Advisory Solutions and a Hong Kong Institute of CPAs member.

While Hong Kong and the Mainland step up the battle against cybercrime – (See *China reacts to growing cyber threat* on sidebar below) – statistics show alarming growth of such problems. The Hong Kong Police Force estimates that the number of reported cases rose 70 percent in 2013, while financial losses totalled HK$916.9 million last year, nearly four times as much as the previous year.

While individuals continue to be targeted, cyber-criminals are concentrating more on companies than individuals, mainly through email deception. Of those total financial losses from cybercrime, about HK$760 million was siphoned off from corporate targets, compared with HK$180 million in 2012.

## Angles of attack

Cybercrime is broadly, if imprecisely, defined. Not all computer attacks steal data, and not all data stolen is taken via computers, experts say. Moosa at PwC defines cybercrime as "crime committed using computers or crime committed against computers used to capture the information stored there and derive some economic gain from it."

According to Kroll, the main cybercrimes include online scams against individuals who use social engineering – tricking administrators or account holders into giving up their credentials – to gain access to credit card numbers, with resultant financial loss; and blackmail, particularly "sextortion," in which individual victims are blackmailed to prevent the release of racy photos or videos they might have been persuaded to make.

For companies, there has been an increase in so-called CEO engineering. "Employees are told of a secret task given to them by the chief executive officer or other senior executive, which invariably calls for them to transfer money to a new account set up by the

## CHINA REACTS TO GROWING CYBER THREAT

Cybercrimes are increasing in the Mainland as well, although accurate data are elusive. A study by the People's Public Security University of China estimated that losses from cybercrime totalled ¥289 billion in 2012, a year in which public security departments investigated more than 118,000 Internet-related crimes.

The National Computer Network Emergency Response Coordination Centre in Beijing reported in March that hacking attacks on Mainland computers in 2013 rose by more than 50 percent compared with the previous year. The centre claimed the main sources of attacks were the United States, Hong Kong and Korea.

The Hong Kong police say they have stepped up cooperation with Mainland authorities, as many cyber-attacks do originate in China. Beijing has rapidly modernized its anti-cybercrime regulatory regime in recent years, although obstacles to cross-border investigation remain.

For example, Mainland cooperation with the U.S. is on hold since the May indictment of five Chinese military officials for allegedly stealing U.S. trade secrets. A joint cyber-security working group met most recently in July 2013, but China cancelled this year's meeting and its future is now uncertain.

Some experts say Chinese companies have among the most advanced protections against cybercrime. "By most measures, China eclipses other [Asia-Pacific] countries in security practices and policy," according to a recent report by PwC, The Global State of Information Security Survey 2014. "What's more," the report added, "no country has implemented security policies for mobile devices, [bring-your-own-device] and social media at a higher rate than China."

Part of the reason is the rapid deployment of advanced technology in Mainland retail, one of the most frequently targeted sectors because of the repositories of customer financial data. "I think China is probably leading the world in terms of the use of e-commerce in daily life, through Taobao and JD.com," says Ramesh Moosa, a Forensic Services Partner with PricewaterhouseCoopers in Shanghai.

Mindful of "state secrets" and other laws preventing the transmission of data outside China, PwC, for example, maintains data analysis centres in the Mainland. "There are a lot of considerations in cross-border investigations and you need to respect data privacy laws," says Moosa.

criminal," explains Sam Olsen, Managing Director and Head of the Asia Security Practice at Kroll. "Because the employee feels privileged to be taken into the confidence of the CEO, these crimes are often successful."

Olsen says one increasingly widespread tactic is "ransomware," a type of malware that locks computers and systems and demands that the individual or company pay money to unlock them. "This included several cases where the infection not only encrypted the local user data but also encrypted data on the server, making it inaccessible to any user," Olsen warns.

Another major motivation for cybercrime is information theft. This is usually data critical to a company's value, such as intellectual property, client lists or sales forecasts. These attacks often come from within a company.

According to Peter Koo, National Leader of Security, Privacy and Resiliency at Deloitte Greater China in Hong Kong and an Institute member, more than 75 percent of data security breaches are internal. "It could be some disgruntled workers. It could be errors. It could be social engineering," he says.

Employees constitute one of four major threat groups, according to Jack Jia, Director, Fraud Investigation and Dispute Services, at EY in Hong Kong. "There are unsophisticated hackers, such as kids experimenting," he says. "Then you have sophisticated attackers who know what they're doing because you have information that they're trying to steal. You can have employees stealing data and then you have state-sponsored attacks."

## Action stations

Jia says finance professionals, such as Institute members, can do much to not only prevent attacks, but to minimize their disruptive effects. *(See page 19)*. The first line of defence, he notes, is ensuring adequate IT resources. "[CPAs] have to design and allocate budgets to fight this," says Jia, a member of the New Zealand Institute of Chartered Accountants.

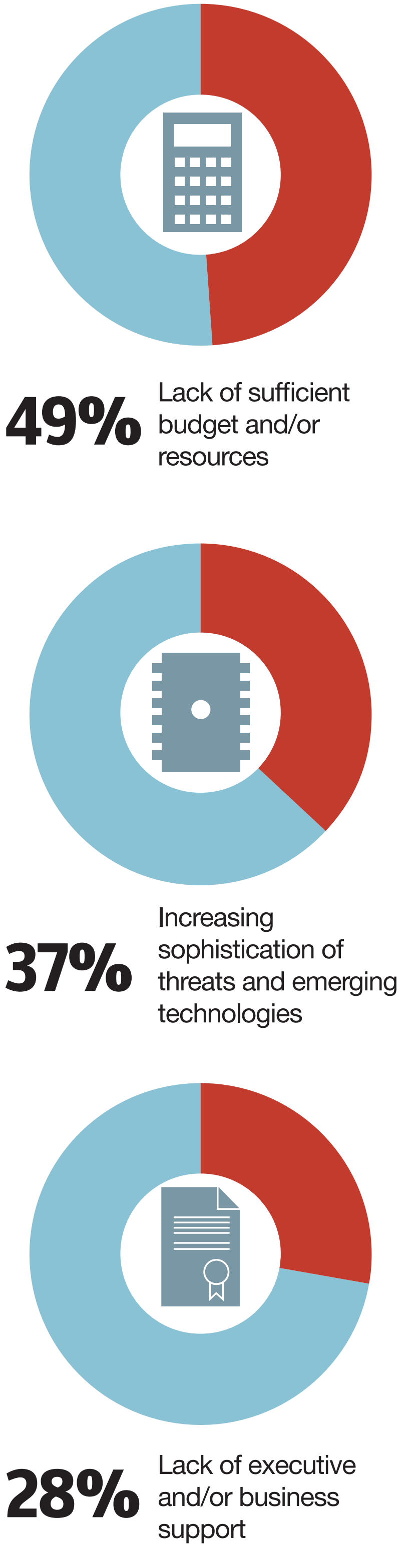
In recent years, the majority of cybercrime investment has been on prevention, such as creating corporate firewalls. "Now the realization is more about, if you're breached, how to make sure you reduce the window of opportunity and make sure the impact of the entrance is minimized," says Jia.

For Institute members who are CFOs, their first step should be ensuring that they are aware of the main issues. "Accountants in organizations must raise their knowledge level about cyber-security and play an active role in the involvement of security programmes," says Moosa at PwC.

From there they can educate the rest of the company's management. "There are so many controls and solutions designed for prevention, detection and mitigation of cybercrime risks," says Henry Shek, a KPMG China Partner specializing in cyber-security. "However, it is more important for management to understand the actual risk that the organization is facing."

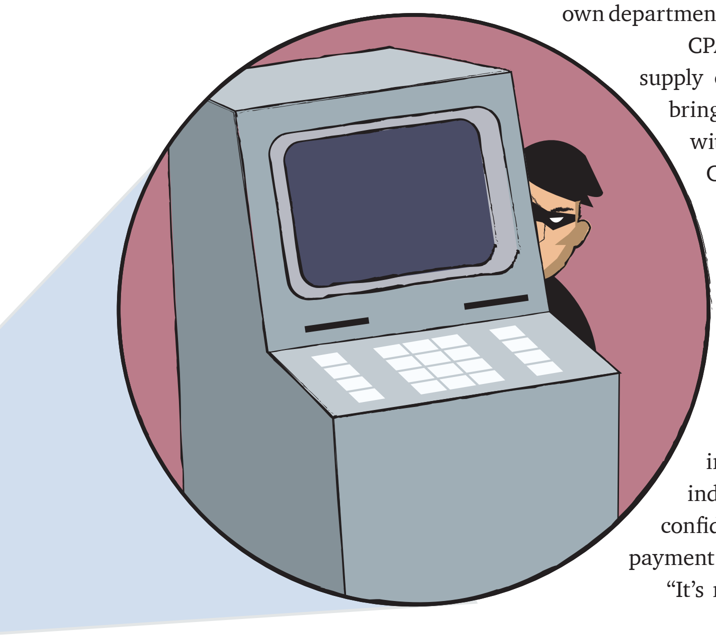
Koo at Deloitte says Institute members have unique training that makes them especially equipped to identify data breaches. "Many of our clients have corporate governance but it is often a stack of papers and policy procedures," he says, noting that CPAs have training in both corporate governance and data management."

## Deloitte Global Security Study 2013



Source: Deloitte

Cloud computing, outsourcing and so-called “big data” have brought their own risks, Koo adds. He recommends separating data into categories: dividing data for internal and external use as well as into general, classified and secret designations.



Access control is critical, Koo adds. “With role-based authentication control, I can access my own files and my own projects, while department heads can access their own department’s files.”

CPAs are often involved in supply chain management, which brings customer data in contact with third-party suppliers. Control over third parties has become increasingly important with the rise of legislation such as the Bribery Act in the United Kingdom, which makes a company responsible for breaches of the law not just by employees but anyone in the supply chain, such as individuals paid to provide confidential information or the payment of ransoms.

“It’s more of a due diligence issue,” says Bancroft at Kroll, “checking the reputation and integrity issues of suppliers, and also getting them to sign up to your own internal policies and procedures and ethics policies. CPAs can help ensure those necessary things are in place.”

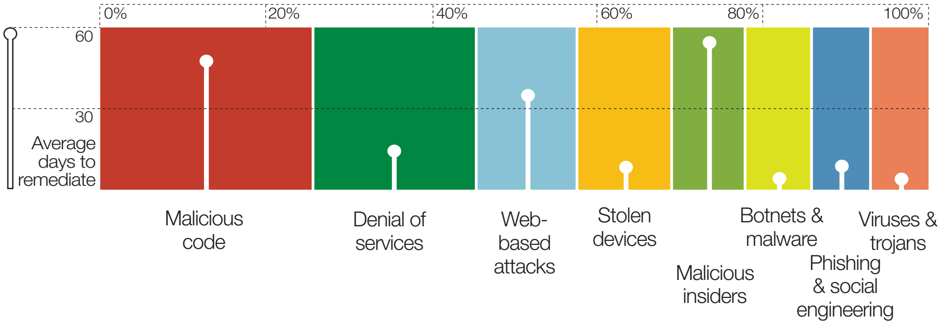
## Defensive manoeuvres

Hong Kong corporations and public bodies have also faced cyber attacks. Last year the Hong Kong Police Force website was hacked, as was a University of Hong Kong public opinion programme. In 2011, Hong Kong Exchanges and Clearing suspended trading after hackers broke into its website and prevented investors from accessing announcements.

The same year Sony’s PlayStation Network in Hong Kong was hacked, forcing it to shut down temporarily, while in 2009, according to claims made last year by U.S. National Security Agency whistle-blower Edward Snowden, American agents hacked into Pacnet, the Hong Kong-based operator of Asia’s largest privately owned submarine

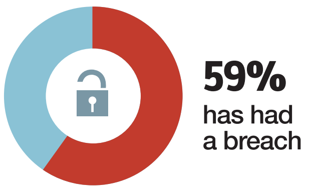
## Deloitte’s Study: Data Breach Costs Your Time and Money

### Deloitte “The Next Big Ideas in Cyber Security” / Ponemon Institute 2012 Cost of Cyber Crime Study: United States

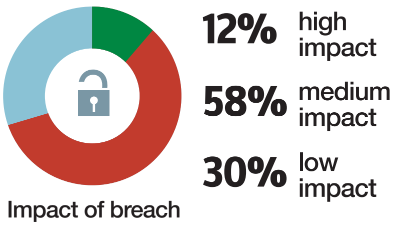


The average amount of time needed to resolve a cyber attack was 24 days with an average total cost of US$591,780.

### Deloitte 2013 Technology, Media and Telecommunications Industry Group Global Security Study



Percentage of respondents that had a breach



Impact of breach

59% of respondents had a data breach in the past 12 months. 70% were medium to high impact.

Source: Deloitte

telecommunications cable network.

The Hong Kong Police Force says it is stepping up its response capacity. By next year, the 100-strong technology crime division will be upgraded into a cybercrime investigation bureau composed of 175 police officers and civilian staff and led by a chief superintendent.

Cybercrime experts say the official Hong Kong figures understate the true extent of the problem. "Many companies get hit by hackers and are not even aware of the actual situation," says Koo at Deloitte. "A lot of companies that get hit carry out internal investigations and there is no report to any law enforcement organization."

Some organizations have experienced attacks that compromised customer information and choose not to tell anyone. "One large company had a serious data breach and made a conscious decision to sweep it under the carpet," recalls Olsen at Kroll.

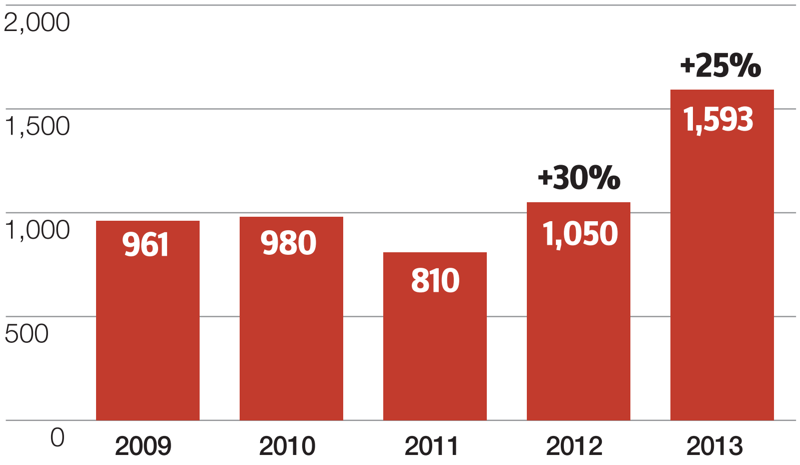
Even in the case of reported crimes, there are few convictions. "Only about 10 percent of Hong Kong's technology-related crimes are solved," says Olsen. "People might laugh at that, but the police are doing an awfully difficult job."

The job of law enforcement can only get harder. As the Hong Kong Department of Justice noted in its most recent annual report: "The future is the convergence of computing and telecommunications and the emergence of an 'Internet of things.' These developments will provide new opportunities for criminal exploitation."

This issue was highlighted by Google's US$3.2 billion purchase this year of Nest Labs, which connects thermostats and smoke detectors with the Internet. "Lots of things have cyber elements and they should all be treated as part of the general threat landscape," Olsen at Kroll warns. "Cybercrime," he adds, "is a methodology of crime, not a branch of crime."

CPAs need to be up to speed on such developments, experts say, but are in the box seat to help companies not only to prevent attacks but to provide early warning of them and minimize their effects. "A CPA thinks from a financial and reputational impact," says Jia at EY. "That's the high risks you are talking about here."

## Security incidents received by Hong Kong Computer Emergency Response Team



Source: Hong Kong Productivity Council

## SIMPLE CHECKLISTS CAN MAKE A BIG DIFFERENCE

Many companies – especially small- and medium-sized entities – hand over responsibility for information technology matters to the head of finance, who is often a Hong Kong Institute of CPAs member.

Many experts say accountants are in the box seat to make a difference when it comes to thwarting cybercrime attacks. Here are some expert recommendations:

Establish policies, procedures, and controls for employees to follow to prevent and detect cybercrime. "People are always the weakest link," says Alvin Li, a Manager at KPMG China specializing in cyber-security. "From a people perspective, organizations should put in sufficient resources to assess and improve security awareness of staff members."

Know your own data. Companies, especially those with limited budgets, should prioritize their data, according to its importance. "Only 20 percent of organizations classify their data and have procedures to protect their most important information," says Ramesh Moosa, a Forensic Services Partner with PricewaterhouseCoopers in Shanghai.

Outsource to reputable providers of data hosting and processing services. "Large cloud computing providers usually have sophisticated measures to deal with disasters," says James Ye, Practising Director at Mazars and a Hong Kong Institute of CPAs member. Clients should inspect providers' certifications and understand its procedures, he adds.

Implement data backup procedures and business continuity planning. "Clients should implement backup procedures and a BCP," urges Ye. This should include assigning responsible parties, providing the equipment and time to schedule backups, creating off-site storage facilities and creating data recovery procedures.

Enhance system security measures. "Make sure your antivirus software is up to date," advises Sam Olsen, Managing Director and Head of the Asia Security Practice at Kroll. "You'd be surprised how many people don't have that."