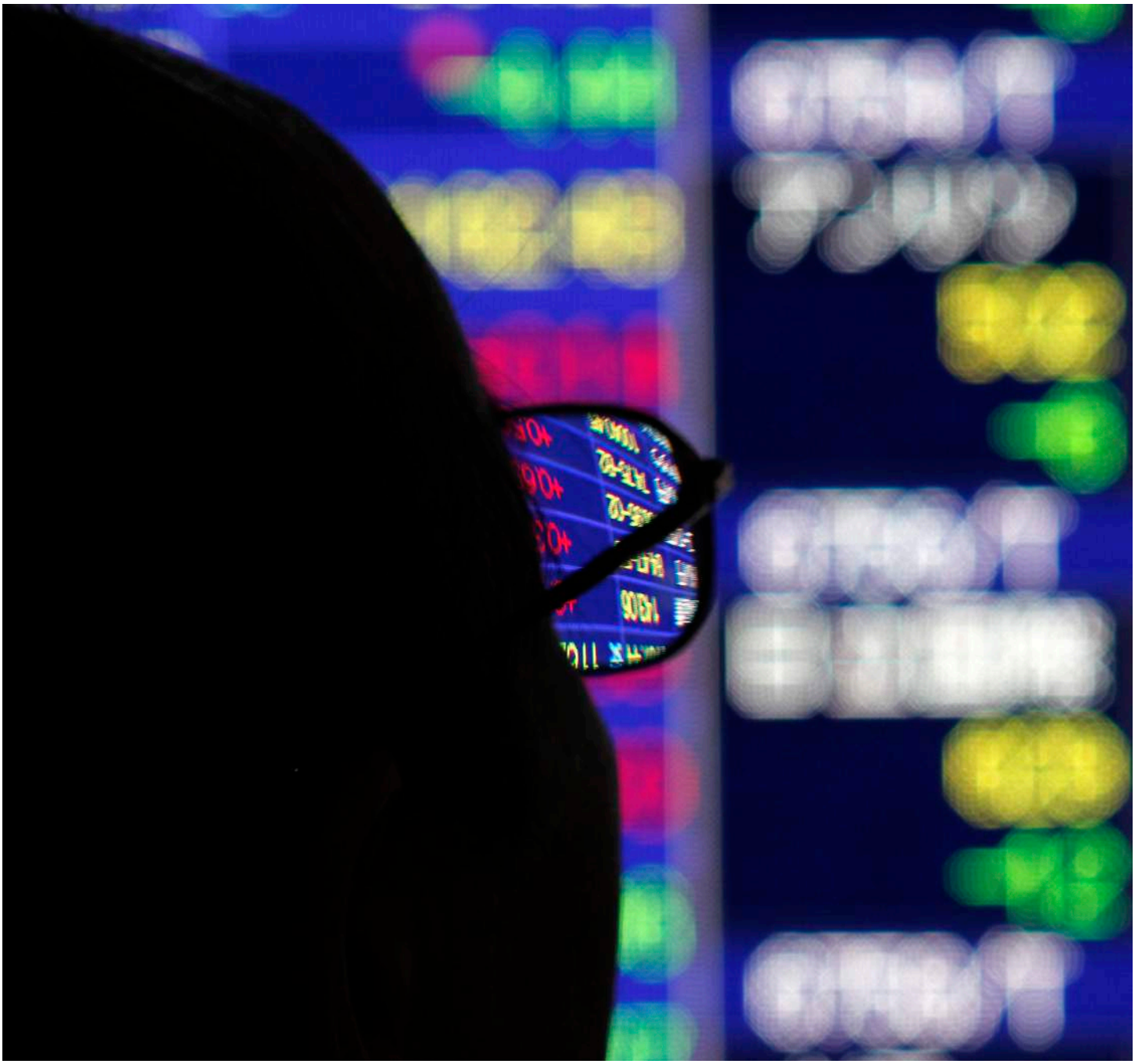


REUTERS/Kim Kyung-Hoon

CYBER CRIME: THE FAST-MOVING MENACE — A SPECIAL REPORT

THOMSON REUTERS™

REPORTING TEAM

BRISBANE
Niall Coburn

HONG KONG
Ajay Shamdasani

LONDON
Martin Coyle
Susannah Hammond
Rachel Wolcott

NEW YORK
Henry Engler
Stuart Gittleman

WASHINGTON, D.C.
Emmanuel Olaoye

EDITORS
Alexander Robson in London
and Randall Mikkelsen in Boston

DESIGN
Paige Nazinitsky

INTRODUCTION

Cyber crime is increasing in the financial sector. Thirty-nine percent of financial services respondents to PwC's 2014 Global Economic Crime Survey reported having been victims of cyber crime. The financial services sector may be ahead of many industries in the detection and prevention of economic crime, including cyber crime, but more could be done. "...this percentage of respondents is alarmingly low — our experience has shown that a clear majority of financial services organizations (especially retail banks) suffered cyber crime during the survey period," the survey said.

Clear weaknesses exist in some firms' risk assessments, whistle-blowing mechanisms and awareness of the pervasive and sustained cyber crime threat. "Clearly, financial services organizations believe that cyber crime is becoming a greater threat than ever before, and yet many do not believe it will happen to them," the survey said.

More recently, following an evidence session on fraud and cyber security at the start of November, Andrew Tyrie, chairman of the UK parliament's Treasury Select Committee, said: "The committee heard that the amount of fraud reported by banks may substantially understate the true scale of the problem. This is concerning. I will be writing to the banks and regulators to obtain a fuller picture on this issue."

This report identifies current trends in cyber crime and the regulatory response in Europe, Asia and the United States in the light of high-profile attacks on JPMorgan and Fidelity. It concludes with suggestions for strategies that compliance officers might adopt to counter the rapidly-growing problem and highlights the need for cooperation among firms, regulators and governments.

TABLE OF CONTENTS

3 INTRODUCTION

5 SHIFT TO INTELLIGENCE-LED SECURITY ESSENTIAL TO TAKE ON NIMBLE CYBER CRIMINALS

8 OVER-RELIANCE ON BIG DATA TOOLS MAY HAMPER BANKS' ABILITY TO DEAL WITH CYBER CRIME

9 U.S. LAWMAKERS, REGULATORS WORK TO BOLSTER FINANCE INDUSTRY DEFENSES AGAINST CYBER ATTACKS

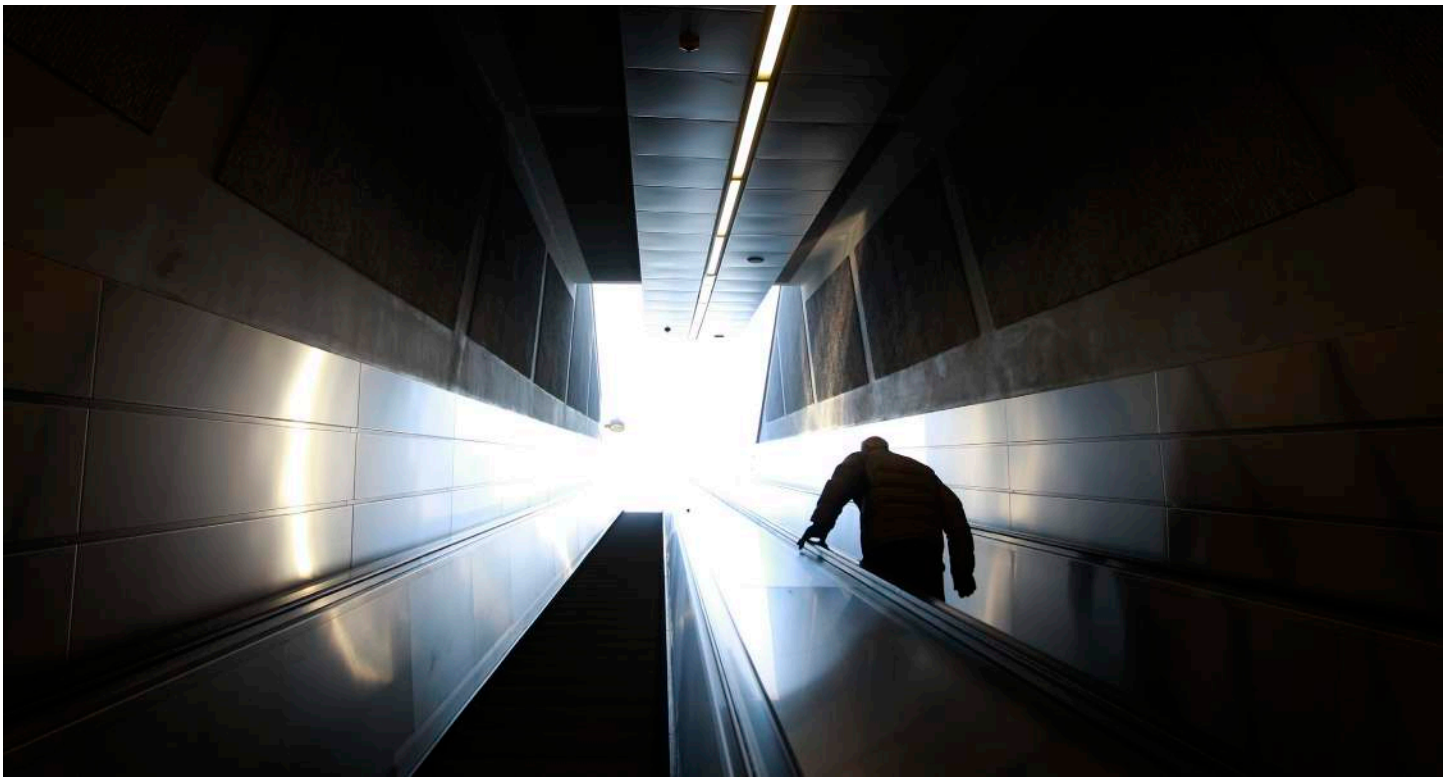
11 HEDGE FUNDS IMPLEMENT STRONGER CYBER SECURITY DEFENSES UNDER U.S. REGULATORY SPOTLIGHT

13 COOPERATION, NOT COMPETITION, WILL BE ESSENTIAL IN THE UK'S FIGHT AGAINST CYBER CRIME

14 ASIAN FIRMS PAYING INSUFFICIENT REGARD TO CYBER CRIME RISK

16 CYBER RESILIENCE — THE NEXT GREAT COMPLIANCE CHALLENGE?

18 CORPORATE GOVERNANCE OF CYBER SECURITY



REUTERS/ John Kolesidis

SHIFT TO INTELLIGENCE-LED SECURITY ESSENTIAL TO TAKE ON NIMBLE CYBER CRIMINALS

Even as technology advances rapidly, the fundamental methods used by cyber criminals to target the financial services sector have not changed much in the last couple of decades. Cyber criminals, be they state-backed cyber spies or members of criminal networks, use modified versions of established techniques or exploit lapses in security no one has fixed.

The difference in cyber space today is that criminals are focusing attacks on specific organizations, especially banks, and work to breach banks' networks, thereby staying several steps ahead of their security. Some of the larger banks have developed in-house cyber intelligence teams to gather information about current threats and threat actors. These teams are the exception, however, not the rule.

Most banks use vendor-provided security solutions, sometimes hundreds of them, to monitor potential threats passively. Cyber security experts argue that banks need to be active and use intelligence gathered in-house or by security intelligence providers to improve their understanding of and reaction to both developing and current cyber threats.

"Firms think if they buy a box and set it up that's going to tell them when some sketchy stuff happens. It's not that simple. It's an information and intelligence game. It's just now starting to become the paradigm for cyber security at these organizations," said John Solomon, head of threat finance research at World Check, a Thomson Reuters company.

LOW RISK, HIGH REWARD

Cyber criminals are also using some of the same old ruses when it comes to stealing bank customers' data and credit card numbers, compromising personal accounts and committing corporate account takeover. Targeting financial institutions is a low-risk, high-reward area for cyber criminals. Rarely are they caught or prosecuted.

"Seventy-five percent of cyber security problems are various kinds of Trojans, which are very effective. We keep seeing new forms of malware, but a lot of them are spin-offs from Zeus and some of the early things we saw. Also, the bad guys continue to find little security lapses in technology that was created years ago," said Shirley Inscoe, senior analyst, fraud and data security, at Aite Group.

Even though financial institutions spend millions on fraud prevention and cyber security each year, cyber crime has grown as a threat. Some banks even have a budget for buying back customer details and credit card numbers from fraudsters and criminals.

While banks have fairly strong cyber security controls in place, their size and complexity makes them difficult to secure. Despite the time, effort and money spent, as well as attempts to promote cyber "hygiene" (e.g., not clicking on suspect emails, installing security patches) banks will always be a target. They are, after all, where the money is.

Distributed denial of service (DDoS) attacks have declined since their peak during the Occupy Movement in 2011. Since then, however, Bank of America, Citigroup, JPMorgan, PNC Bank, U.S. Bancorp, Wells Fargo and others have all seen their websites hit with DDoS attacks by Iranian and Syrian groups, although these politically motivated attacks have decreased in intensity during the last 18 months.

Data theft is on the rise, as shown by the many high-profile breaches recently at big names such as JPMorgan, Fidelity Investments, Target, Sony and Citi. Many cyber criminals now seek to use customers' personal information and card details to commit a wide range of lucrative frauds.

"A random credit card stealing Trojan is an annoyance, but it's not going to put a bank out of business. But someone who wants to steal trading algorithms or someone who wants to steal consumer information so they can go spear-phish them all — those things happen infrequently but could have potentially catastrophic impact. We have to stop looking at the 'what' and look more at the 'who' and the 'why'," said Greg Day, vice president and chief technology officer at network security company FireEye.

IT'S PERSONAL

Organized crime groups have started to use the techniques, tactics and procedures developed by high-level espionage groups. When these tactics are reproduced on a smaller scale, cyber crime gangs use them to target oil companies, the power industry and of course banks. These groups now seek to make money by going after a few big paydays rather than lots of smaller frauds.

Cyber crime gangs tend to attack an organization with a specific goal in mind. Day said this approach was hard for many organizations to understand. If the criminals failed in their first attempt, they did not go away; they evolved the attack and came back to try again. Criminals will bang their head on the door any number of times with the goal of getting in.

"More attacks are being personalized, which indicates that if there is focus then there is persistence that goes with that. Over the last six months when I look at the attacks typically going into organizations, [in] about 85 percent of those we're only seeing one organization. That means the code or the binary code that contains the attack is focused on one company. Someone has taken the time to craft something specific to that company to evade traditional controls," Day said.

Another element of this personalized style of attack is the tendency to go after specific people within firms; this is called social engineering. Cyber criminals will target people, especially those who are more senior and have more access, using personal information which is easily available online, although it is not uncommon for criminals to exploit their targets' elderly or more vulnerable relatives to gather intelligence. In some instances, employees are either bribed or threatened by criminals to help commit cyber crime.

"Once you have someone's email address and you know a little about them then it's not difficult to get them to go to a website or send them an email. When they click on it, all of a sudden someone is in the system and network. The criminals keep looking for people with higher access and contacts and then tunnel through the whole network to get more and more access," Solomon said.

BANKS SLOW TO RESPOND TO NIMBLE CRIMINALS

Many banks, and other companies for that matter, are failing to do some of the basics to protect themselves from cyber criminals. The elderly technology still used by many banks presents a particular security problem. It is well-known that some banks' legacy technology and applications are 25 or 30 years old, and are therefore difficult to fix and protect. Ninety-nine percent of breaches used old vulnerabilities that governments, banks and companies failed to patch.

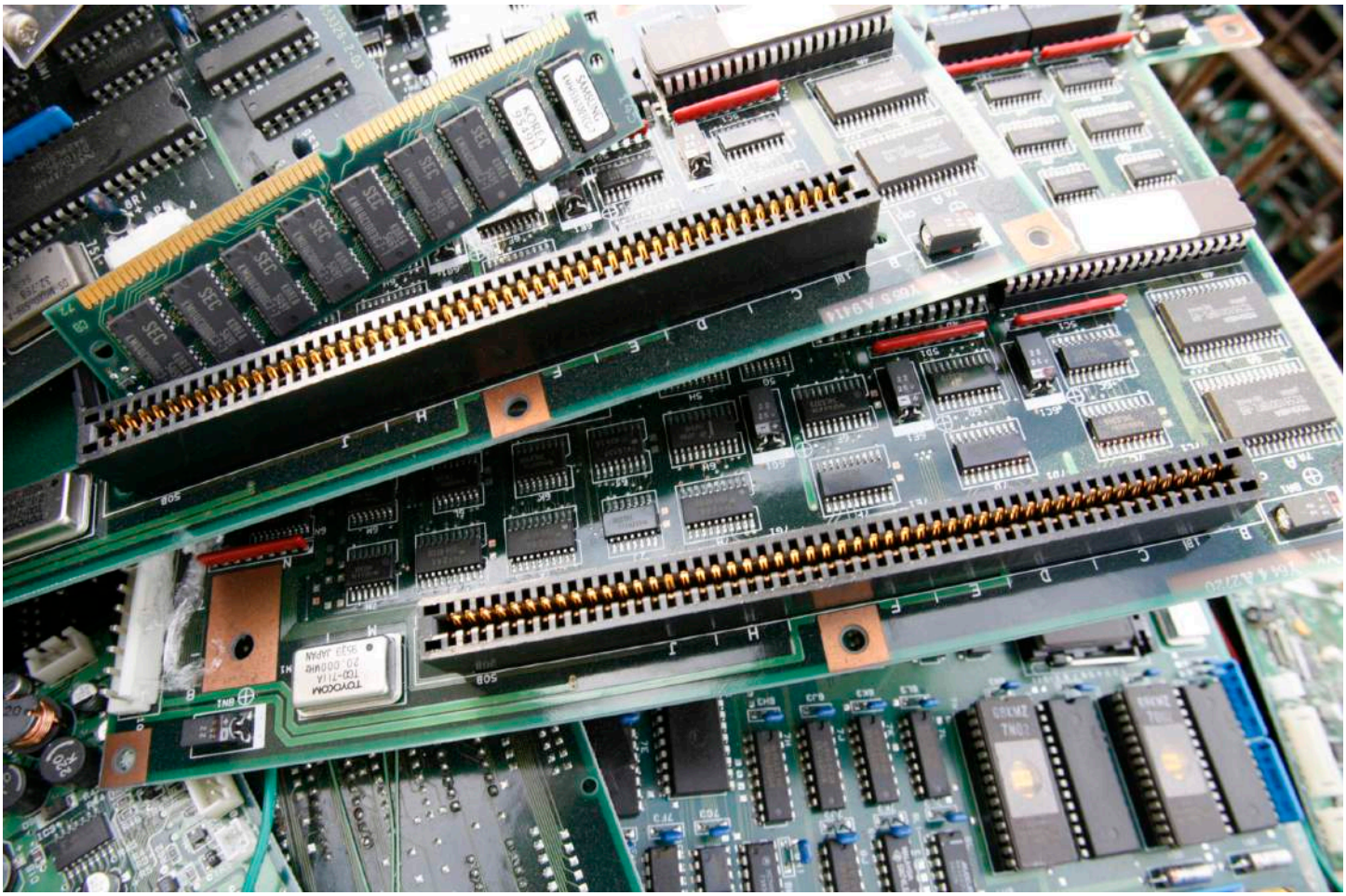
"The people who built [the technology] are retired, but banks can't touch it because it's critical to the business. They just have to accept that's the risk and think about how to mitigate the risk of it being breached or targeted. This is a big problem. We don't build secure and embed it in technology. It's always retrofitted, unfortunately," said Jason Steer, director of technology strategy at FireEye.

"Standard best practice just does not happen. We meet CIOs and CTOs all the time and ask them what are the top-five business systems you need to protect and [keep] up and running. Many of them don't know what or who they're protecting or what they're protecting them from. If you don't even know what you're protecting in your business you don't know where to start or where to draw the battle lines," Steer said.

SPEEDIER DECISION-MAKING PROCESSES ESSENTIAL

Decision-making and budget allocation regarding cyber security also slows down banks' ability to deal with cyber crime and fraud. It can sometimes take up to three years to fund and implement anti-fraud and other security programs.

"The biggest difference between a financial institution and a crime ring is that the financial institution needs to prepare a business case, get it approved, get the budget, then get a huge IT project moving to implement it. The crime ring just does it, whatever it is," Inscoe said.



REUTERS/Yuriko Nakao

INTELLIGENCE-LED SECURITY REQUIRED

Some of the world's largest banks have in-house cyber security teams working with their information technology teams on cyber defense. These teams go a step further, however, than those at less active banks. Staffed by former intelligence, government or military officials, many are looking not only at how to deter cyber crime, but also at how to prepare for, prevent, respond to and recover from it.

"They use tools to understand the threat actors that are out there. What are the networks that exist out there that are adversarial? Who are they targeting? Who are they talking about? Is there any commonality in that group? Is my peer bank being attacked and therefore should I be a little more cognizant of what's going on? That's happening at some of the largest banks that have the resources to have a cyber intelligence program, but it's very difficult," Solomon said.

Those firms with an intelligence-led approach know what issues are on the horizon and what they are dealing with. Solomon said firms should be aware of dates and timelines. Dates can have meaning to politically-motivated cyber criminals and hackers.

These more sophisticated cyber intelligence teams try to get as many sources as possible to identify threats and new threat actors. They attempt to be present in internet relay chat (IRC) conversations, and perform social media surveillance. Additionally, they work with traditional databases and investigate the carder websites where customer data and credit card details are bought and sold.

There is a huge amount of data, which means banks need to understand which threats should be prioritized. That edge comes from analysis, expertise and being able to contextualize information. That is where machines' usefulness is outmatched by that of humans.

OVER-RELIANCE ON BIG DATA TOOLS MAY HAMPER BANKS' ABILITY TO DEAL WITH CYBER CRIME

"Big data" is a term often bandied about in risk management circles as some kind of miracle cure for the difficulties banks face in assessing and understanding risk. Indeed, big data tools have been heavily promoted by IT vendors and are now widely used by banks to detect cyber security breaches. Unfortunately, however, these systems often tend to gather so much data that it is difficult for security analysts to pinpoint potential threats quickly enough.

"Banks' IT security systems have hard exteriors, but are soft and gooey on the inside. Now they're using big data to detect breaches, but those solutions are not useful for detecting something that hasn't been seen before and doing something about it. Big data tools throw up too many false positives and give security teams more information than they can handle," said Jason Steer, director of technology strategy at network security company FireEye.

Apart from a handful of banks that have invested in intelligence-led cyber security teams, most banks are still in defense mode. They are using an array of technologies to protect their systems and customers from cyber criminals and fraudsters. It is not that banks are failing to detect and respond to breaches; their anti-fraud and security systems catch new scams all the time. The problem is that criminals and fraudsters innovate more rapidly than banks' security systems, and have begun to target specific firms. They chip away at banks' defenses until they find a way in.

"We're heading into this dangerous territory where we're trying to find a needle in a haystack. Unfortunately, what we've done is bring out more and more tools that look for bad behavior, but each one is so voluminous and there is so much information it takes us so long to sift through and understand what could be a real incident. Just to run one query on a suspicious incident can take from one hour up to seven or eight hours," said Greg Day, vice president and chief technology officer at FireEye.

The larger firms will have tens of thousands of devices in their IT networks. This will include everything from desktops and laptops, to mobile devices, cash points, mainframes and data warehouses. Some of these will be the firms' own; some will have been supplied or used by contractors. Every day these devices and their users are generating potential security events — password failures, login failures, system crashes — perhaps 10 million events each day that are routed to a security operation center.

Analysts at such centers are charged with crunching internally-generated information into something meaningful. Information will also be coming in from the outside about new viruses, vulnerabilities and exposures, which the analysts will then need to collate against the messages they have received. Most security operation centers aim to get down to between five and 10 actionable events per day.

"Even if you have some of the best analytics and mathematics in the world, they're not always helping. You need to have the expertise, the human intelligence, the analytics and tools, and the data, the raw information. Organizations are usually bad, or less than perfect, in one of those. Then they can't deal with the threat. There's also an entrenched belief in IT security that it's more about taking a defensive approach than a proactive approach," said John Solomon, head of threat finance research at World-Check, a Thomson Reuters company.

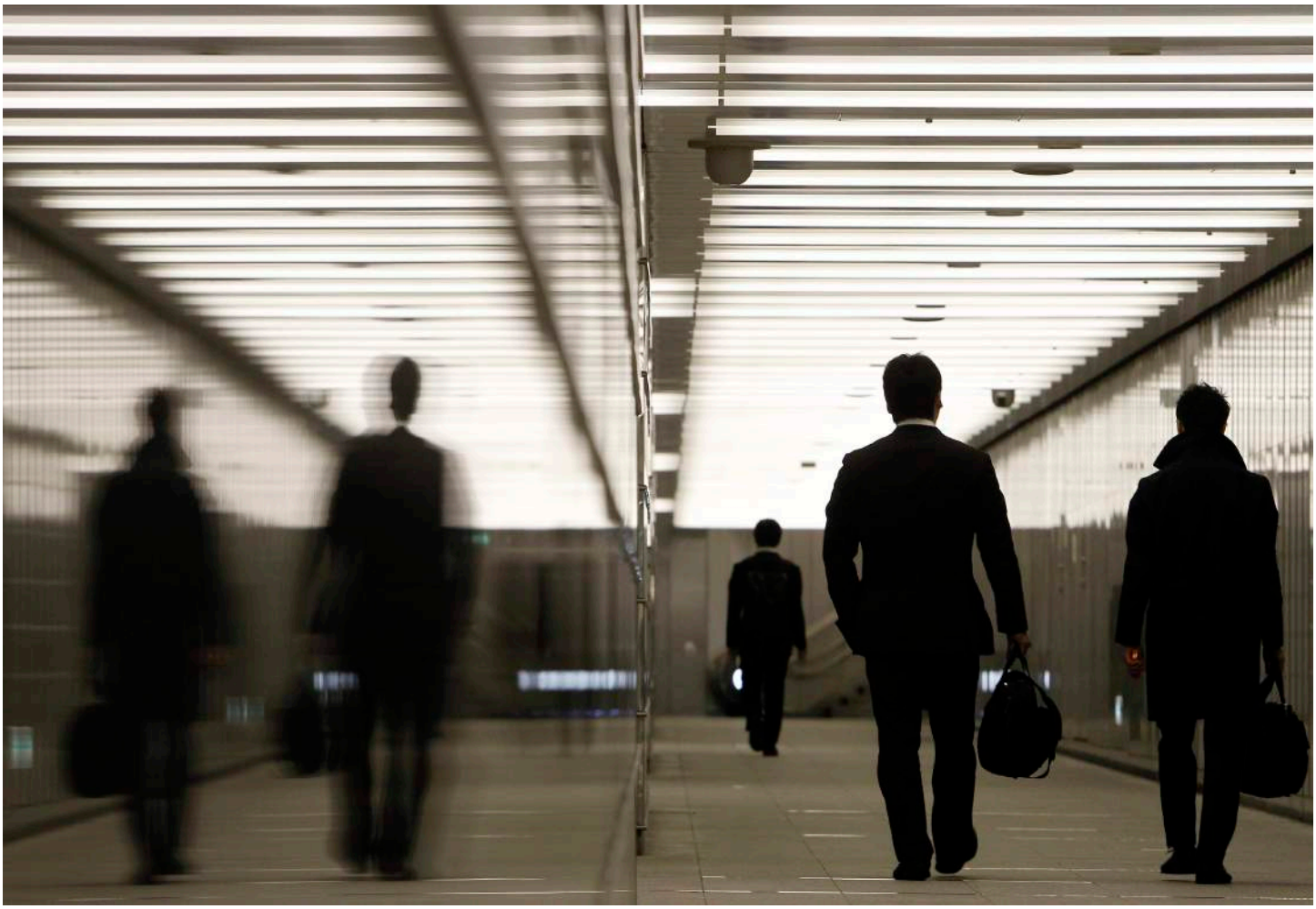
MEDIAN DETECTION TIME MORE THAN SEVEN MONTHS

Research from Mandiant, a cyber security consulting firm owned by FireEye, has suggested that, based on the incidents to which the firm has responded, the median time between breach and discovery is 229 days. That number has dropped in one year from 243 days: a 14-day improvement, albeit still slow. This means that although some breaches are detected and addressed immediately by companies' security systems, those that go undetected can stay undetected for months.

"There are number of reasons for this. One is the security industry has spent years preaching 'defend, defend, defend'. It's quite hard to do a bit of a U-turn and say, 'Yes, we have to accept things will get through. That's a bitter pill we need to swallow, along with contending with the information overload from all the security systems," Day said.

The outcome of the "defend, defend, defend" approach to cyber security is that banks have not built security into their technology platforms. It tends instead to be an afterthought fitted retrospectively onto creaking and elderly IT systems.

"Building effective security involves more than just installing tools. Firms need to build a capability that includes people, processes and tools. The tools that do big data have a role to play, but they're not a silver bullet. Tools in isolation aren't going to help companies be secure," said Richard Horne, a partner in PwC's cyber security practice.



REUTERS/Yuriko Nakao

U.S. LAWMAKERS, REGULATORS WORK TO BOLSTER FINANCE INDUSTRY DEFENSES AGAINST CYBER ATTACKS

Although U.S. lawmakers have considered cyber security legislation for years, disagreements about the role of the government in the private sector have hampered federal policy efforts to protect the financial industry from computer-based crime.

A spate of cyber attacks against high-profile banks and other businesses in the past year has created a sense of urgency among lawmakers and regulators, however. Attacks against JPMorgan that were identified in August compromised the personal information of 83 million households and small business accounts, and about a dozen other banks later confirmed that they too had been hacked.

Regulators are fighting back by gathering information from firms about their cyber security practices, and incorporating the findings into priorities for regulatory examinations in 2015. In Congress, momentum has built for legislative efforts to fight cyber crime.

"Cyber security has become a top concern to American companies, regulators and law enforcement agencies," U.S. Securities and Exchange Commission member Luis Aguilar told an agency roundtable in March that preceded new regulatory initiatives. "The constant threat of cyber attack is real, lasting and cannot be ignored."

In April, the SEC's Office of Compliance Inspections and Examinations published a set of questions that compliance officers could use to assess how ready their organization was to deal with a cyber attack. The alert included questions that OCIE might ask firms when it examined their cyber security practices. OCIE will also ask firms how they protect their networks, identify cyber risks and assess the risks involved when they outsource their operations to third parties.

On the broker-dealer side, the Financial Industry Regulatory Authority is working on guidelines that are based on a cyber security survey it sent to firms in January. FINRA is hiring examiners with technology expertise to look at what firms are doing to secure their clients' information. The findings are likely to be reflected in exam priorities due to be published in early 2015. Banking regulators are also gathering information from firms about their information security.

The Federal Financial Institutions Examination Council has warned firms that they should urgently assess potential vulnerabilities in their information systems. The FFIEC, which includes the U.S. Federal Reserve and the Office of the Comptroller of the Currency, said banks using third-party vendors should inform their vendors about vulnerabilities and take preventative action.

In November, the FFIEC issued advice for chief executive officers and board directors on how to ensure that their organization was prepared for a cyber attack. The council included questions that senior executives should be asking about their organization's risk management practices and cyber vulnerabilities. It urged senior managers to ask tough questions about how their firms' products, connection types and technology might be compromised.

"Today's financial institutions are critically dependent on IT to conduct business operations," the FFIEC said. "This dependence, coupled with increasing sector interconnectedness and rapidly evolving cyber threats, reinforces the need for engagement by the board of directors and senior management."

It said corporate leaders needed to understand the institution's inherent cyber security risk, routinely discuss cyber security issues in meetings, monitor and maintain sufficient awareness of threats and vulnerabilities, maintain a "dynamic" control environment, manage connections to third parties and implement business continuity and disaster recovery plans that incorporate scenarios involving cyber incidents.

The U.S. Commodity Futures Trading Commission (CFTC), the swaps and futures regulator, has been less vocal, but that may change if Congress approves its request for a bigger budget. The agency's new chairman, Timothy Massad, told a Senate hearing in September that the agency wanted to hire more examiners with expertise in technology so that it could do a better job of examining firms on cyber security.

The CFTC's Division of Swap Dealer and Intermediary Oversight this year shared a list of best practices for ensuring the security and confidentiality of customer information, and protecting against anticipated threats and unauthorized access to or use of such records.

A U.S. SENATE BILL

Lawmakers are just as keen as regulators to tighten up on cyber security. Sen. Dianne Feinstein of California, the Democratic chairman of the Senate Intelligence Committee, and Sen. Saxby Chambliss of Georgia, the committee's highest-ranking Republican, are pushing a bill that would require companies to monitor their computer networks, and those of consenting customers, for cyber threats.

The bill would also allow companies and individuals to share information on cyber threats with each other as well as with the government.

The committee has approved sending the bill to the full Senate, and voting is expected before the end of the year. If the House of Representatives fails to pass a measure for President Barack Obama's signature by year-end, the new Congress that takes office in January, with Republican majorities in both houses, will have to start the process again.

Despite the heightened attention from regulators and greater awareness at firms, efforts to fight cyber crime through joint government and industry efforts may have been weakened by a broader enforcement crackdown against the financial industry following the 2008 financial crisis. Firms are often reluctant to be overly cooperative with regulatory or law enforcement agencies, because when an inquiry begins, the firm does not know whether it is being considered as a possible victim or a possible defendant, attendees at a recent cyber security conference were told by a security expert.

Aly Song

HEDGE FUNDS IMPLEMENT STRONGER CYBER SECURITY DEFENSES UNDER U.S. REGULATORY SPOTLIGHT

Hedge funds and asset managers are noted for the sums they spend on trading technology. To gain an edge in an increasingly competitive, high-speed market environment, no expense seems too much when investing in sophisticated information and state-of-the-art trading systems. But when the conversation turns to building defenses against cyber crime, there tends to be a sudden silence.

Many hedge funds outsource their back-office IT infrastructure to third parties. This is particularly so for relatively small or medium-sized firms in terms of assets under management. Unlike the largest funds in the industry, which often maintain proprietary systems, the vast middle make up the lion's share of the sector and appear to be far behind in their defenses against cyber threats.

"There are three types of hedge funds. Those who are really on top of it — and these would include the biggest players and quant firms — but the majority are in the second bucket and somewhat confused and not sure what to do," said Raj Bakhru, chief executive of Aponix Financial Technologists, an advisory firm to hedge funds. "And then there is a significant 'head in the sand' bucket who don't care … . It's an educational process."

Until recently, cyber crime was considered as something more likely to affect large banking institutions, whose high profile was seen as making them prime targets for all kinds of hackers and terrorists. JPMorgan's admission that it had been on the receiving end of a massive attack earlier this year only underscored the threat such institutions face and the need for investment to keep pace with cyber criminals.

"CRYPTO LOCKER" MOST COMMON THREAT SEEN TO FUNDS

Hedge funds have increasingly come into focus, however. While the motivations of those wishing to penetrate a large hedge fund might vary, one of the more common forms of attack is called "crypto locker", a type of password kidnapping with the hackers seeking a large ransom to unlock the frozen data.

The software in a crypto locker is typically spread through infected attachments to emails, or as a secondary infection on computers which are already affected by viruses which offer a back door for further attacks.

When a computer is infected, it contacts a central server for the information it needs to activate, and then begins encrypting files on the infected computer with that information. Once all the files are encrypted, it posts a message asking for payment to decrypt the files — and threatens to destroy the information if the payment is not made.

Bakhru said although crypto locker attacks were the kind of attack he saw most often among hedge funds, other types of cyber crime included:

- attacks by those who have philosophical or political beliefs that are adverse to free markets and capitalism;
- internal threats from employees, which often result from an employee wishing to leave the firm with customer information they believe belongs to them;
- state-sponsored threats, although these are far less common and are rarely seen in this sector.

REUTERS/Yannis Behrakis

SEC INITIATIVE PROMPTS GREATER FOCUS AMONG FUNDS

Apart from incidents where firms have come under attack — whether from external blackmail or disgruntled employees — what has recently put the issue high on firms' radar is a cyber security initiative announced in April by the Securities and Exchange Commission.

The program, which is being overseen by the Office of Compliance Inspections and Examinations, outlines several key areas on which registered broker-dealers and investment advisers need to focus.

"In general, the SEC alert is a pretty good compilation of best industry practices," said Vikram Bhat, principal in Deloitte & Touche LLP Cyber Risk Services. "At the end of the day what the regulators are concerned about is whether they have sound risk management practices in place."

The alert included five major areas that firms should review when assessing their state of preparedness against cyber crime:

IDENTIFICATION OF RISKS/CYBER SECURITY GOVERNANCE

Every firm should have an inventory of all physical devices, systems, software platforms and connections to external sources catalogued and available for inspection. There also should be a written information security policy that outlines who is responsible for security and the governance structure in place.

PROTECTION OF FIRM NETWORKS AND INFORMATION

Firms must be able to identify the types of cyber security risk management process standards they use, such as those by the International Organization for Standardization (ISO). In addition, the practices and controls used for the protection of the firm's networks and information should be documented and readily available.

RISKS ASSOCIATED WITH REMOTE CUSTOMER ACCESS AND FUNDS TRANSFER REQUESTS

If firms offer customers online account access, they should provide the names of third parties that manage the service, the functionality available for customers and controls to protect PINs and other security policies.

RISKS ASSOCIATED WITH VENDORS AND OTHER THIRD PARTIES

If firms periodically conduct cyber security risk assessments of their vendors and third parties, they should be able to demonstrate what information is obtained and explain the policies and procedures which govern the process.

DETECTION OF UNAUTHORIZED ACTIVITY

Firms must demonstrate how such detection is carried out and identify the individuals responsible for monitoring and reporting suspicious activities. In addition, the type of testing used to detect any breaches should also be documented and made available.

Although it is early in the SEC exam process, firms need to understand that protecting client data and assets is paramount, and already enforceable, Bakhru said.

"It is largely an exploratory process right now. What we expect to come from the SEC is a more formalized guidance and regulation," Bakhru said. "But what a lot of people failed to recognize is that they need to protect client data and assets as it applies to cyber security. What we have been doing is training hedge funds that this is already enforceable."

REUTERS/Arko Datta

COOPERATION, NOT COMPETITION, WILL BE ESSENTIAL IN THE UK'S FIGHT AGAINST CYBER CRIME

Both the Bank of England and the UK's Financial Conduct Authority have expressed concern about the possible threats cyber criminals and organizations pose to financial services firms. Each was involved in the Waking Shark II exercise last year, which saw organizations play out a war game-type exercise designed to test the industry's contingency plans for a cyber attack.

The assessment, which involved participants from the wholesale banks, regulators and the government, involved a scenario where the financial sector was placed under severe stress following a cyber attack by a hostile nation state. Although the Bank said the findings were positive, it suggested that a single coordinating body was needed to manage communications during an incident. It said firms should be made aware of the need to report major incidents to the regulator as soon as possible, and of the need to engage with law enforcement authorities.

Speaking earlier this year Andrew Gracie, executive director, resolution, at the Bank, said cyber risk and had become a much stronger focus for regulators and firms. He stressed the importance of firms working together to ensure cyber resilience and said that it was an area where firms should collaborate rather than compete. "Indeed, given the prevalence of threats, silence on cyber risks would be a cause not for comfort but for concern," he said.

He said the Bank was worried about the impact a cyber attack might have on the financial system as a whole, and said it was particularly interested in firms' back-up plans as well as their upstream defenses and capacity to withstand attacks.

Andrew Tyrie, MP, called recently for the FCA to brief the all-party Treasury Select Committee, of which he is chair, on the systemic threats posed by cyber attacks. Tyrie, who has held a series of meetings with regulators regarding cyber issues, said he wanted an explanation of what the FCA was doing to deal with the issue and what specific resources it had in place.

Martin Wheatley, chief executive of the FCA, had previously told MPs that there had been an increase in the number of distributed denial of service attacks on firms, as well as the UK's wider infrastructure, and said the issue was a "major concern". The FCA said it planned to look at the resilience of legacy systems, cyber attacks and the visibility of these risks to firms' boards. Wheatley stressed the need for consumers to play their part in the process of ensuring cyber criminals could not breach security systems.

On the consumer side, the British Bankers' Association has launched a fraud awareness campaign to address areas where members of the public may unwittingly leave themselves vulnerable. With the help of retail banks, the City of London Police and the National Crime Agency, the BBA produced a leaflet setting out the do's and don'ts of online security. The campaign has warned of the dangers of clicking on unauthorized emails which ask people to log on to their account, or of emailing personal banking information, or of carrying out "test" transactions online.

At the end of October the biggest-ever cyber security exercise in Europe took place when more than 200 organizations and 400 cyber security professionals from 29 European countries tested their readiness to counter cyber attacks in a day-long simulation. The event dealt with more than 2,000 separate cyber incidents, including distributed denial of service attacks to online services, ex-filtration of sensitive information and attacks on critical infrastructure.

Exercise centers were set up across Europe to deal with the event and the exercise was backed by the European Commission. Neelie Kroes, the EC's vice-president, welcomed the coordinated approach: "The sophistication and volume of cyber attacks are increasing every day. They cannot be countered if individual states work alone or just a handful of them act together."

REUTERS/Ralph Orlowski

ASIAN FIRMS PAYING INSUFFICIENT REGARD TO CYBER CRIME RISK

The financial sector in Asia should take more steps to detect and prevent cyber crime given the region's higher degree of political volatility, officials have said. States such as North Korea and China have been accused in the West of sponsoring hackers that could potentially cripple infrastructure and inflict reputational losses on financial institutions worldwide, while "hacktivist" groups such as Anonymous have been known to target governments in Hong Kong and China.

When used to target the financial system, cyber attacks can affect payment-clearing systems, interbank transfers or undermine liquidity. Similarly, distributed denial of service (DDoS) attacks, such as those which temporarily affected HSBC's servers in 2012, could hurt retail banking as automated teller machines (ATMs) could go down and entire financial systems could be frozen. Cyber crime also has the potential to affect mobile banking.

"In addition to the DDoS attacks that we have seen recently targeting certain organizations in Hong Kong, we have seen cyber attacks that attempt to hijack individuals' mobile banking applications and lure the victims to transfer funds to third parties," said Kenneth Wong, a partner at PwC and its cyber security leader for China and Hong Kong.

Wong said what was at stake was no less than the ecosystem of the global capital markets; the recently disclosed security breach at JPMorgan had started with the intruders attacking the bank's outsourcing service providers, contractors and temporary systems. Once the systems had been compromised, the cyber criminals continued to obtain a higher degree of trust in the cyber space of the companies, allowing them to compromise systems containing data of a higher level of sensitivity, Wong said.

Japan's banking sector has also been targeted, with the Japanese National Police Agency reporting a loss of 1.42 billion Yen ($12.37 million) in the first half of 2014 — more than was recorded in the whole of 2013. These attacks have been put down to the VAWTRAK malware family, which attempts to block anti-virus software via a Windows vulnerability.

"Japan's financial services sector is second [only to the U.S.] in terms of the volume of targeting by financial malware," said Oliver Robinson, head of cyber threat intelligence at Control Risks in London. "Hong Kong is the fifth most frequently targeted country in the region, according to cyber security industry reports. Financial services remain the most targeted sector in the Asia region," he said.

PERVASIVE LACK OF CONCERN IN ASIA

Recent reports by accounting firms EY and PwC in Asia have found that few financial institutions and corporations in the region have rehearsed for a potential cyber attack as part of their crisis management exercises. In addition, many executives did not perceive cyber attacks to be high on their risk register.

"This can be attributed to the nature of the threat being misunderstood, with [most] respondents being concerned with the risks posed by hackers, compared with significantly lower proportions [that are] concerned by potentially more damaging threats such as organized crime or 'advanced persistent threats'," said Chris Fordham, head of EY's fraud, investigations and dispute services practice in Hong Kong.

In Asia, there was still a general perception that cyber crime involved only hacking and that DDoS attacks and were not directly linked to fraud, which was not the case, Fordham said.

The lack of cyber crime readiness is problematic because such attacks are often not one-off incidents but capable of repetition. As institutions get smarter and evolve their defenses, cyber criminals also have to evolve.

"Cyber attacks are not a one-time, all-or-nothing event. Most large organizations in Hong Kong are subject to a constant stream of attacks of varying levels," said Aaron Bleasdale, associate at Baker & McKenzie in Hong Kong.

In addition, if a hacker group has targeted a financial institution, even if the attack is detected and remedied, the attackers gain an understanding of that organization's systems and defenses, and are likely to make future attempts.

PERSONAL DATA

The theft of personal details has been a persistent problem in the financial services sector, and the details are usually used to commit identity fraud or facilitate unauthorized transactions, said Mark Parsons, partner at Hogan Lovells in Hong Kong.

"Some cyber attacks in the region have focused on hacking personal details of wealthier private banking clients, which to a thief have the attraction of greater potential rewards," he said.

An even bigger issue for banks may be that of disclosure and reporting. Once an institution realizes it has been the victim of cyber crime, what it does in the intervening hours, minutes and seconds may prove to be decisive in terms of its ability to ameliorate its losses, including any regulatory compliance fallout.

"Traditionally, these kinds of attacks have been kept under wraps, but the U.S. Securities and Exchange Commission is pushing for further disclosure by U.S.-listed companies," Bleasdale said.

He said there had been few disclosures of cyber attacks by financial institutions in Hong Kong, although that did not mean that they had not been attacked. "Often a victim may not even be aware of a breach," he said.

COMPLIANCE IMPLICATIONS

While the financial sector is at high risk of cyber crime, some have suggested that institutions, regulators and states in Asia still have a long way to go in terms of readiness, despite having being quick to pass laws mimicking those of more developed jurisdictions.

"Asian countries who are generally slow to respond to such technological changes have responded quickly with legislative change, [and] even countries such as Vietnam have instituted legislation on cyber crime," said Neil Ramchandran, managing partner for technology and delivery for Asia-Pacific at Capco.

He said cyber crime was a "high-impact area for compliance and risk staff" and most firms had instituted policies, using a range of measures such as software solutions, disaster recovery solutions, software polices and physical measures.

"While the view is that measures are comprehensive for now, it is widely felt that it is an area for continuous improvement and hence the focus is constant," Ramchandran said.

There was strong evidence to suggest cyber crime in Asia was well-organized, although attacks on financial institutions had, to date, been irregular and ill-coordinated, he said.

CYBER RESILIENCE — THE NEXT GREAT COMPLIANCE CHALLENGE?

Before the financial crisis compliance officers knew the boundaries of their roles. They were the second line of defence and they updated policies in line with changes in the relevant rulebook, monitored all aspects of conduct of business and reported up to the risk committee.

Often this was a very busy role, but one where the edges were clearly defined. The perimeter of today's compliance officer job description is much more nebulous and is driven by developing regulatory expectations about good customer outcomes and conduct risk.

In June 2014, Andrew Gracie, executive director, resolution, at the Bank of England, gave a speech entitled, "Managing cyber risk: the global banking perspective" at the British Bankers' Association Cyber Conference.

"What I have mentioned so far — information-gathering, testing and information-sharing — are essential ingredients to improving the sector's resilience to potential cyber threats. Underpinning all of these is a longer-term question about culture. Cyber risk is not just for technology specialists; this is part of a broader issue of how organisations defend themselves against attack," he told delegates.

COMPLIANCE APPROACH

Compliance officers do not need to become technological experts overnight but they do need to ensure that cyber risks are effectively identified, managed, offset, monitored and reported on within their firm's corporate governance framework. There are some basic measures which compliance officers and their firms need to consider, and they must be prepared for increasing levels of regulatory interest in these areas:

WHAT INFORMATION NEEDS TO BE PROTECTED?

Risk, compliance and IT control infrastructures can only be designed to protect processes and assets that are known. Everything from customer data to operational networks, the use of the cloud, systems (outsourced as well as in-house), links to payment infrastructures and exchanges, to levels of user access to information need to be mapped and included in the governance infrastructure. Care should be taken to ensure that manual work-arounds, often a legacy of businesses acquisitions, are not excluded. The process may be manual, and therefore not "cyber", but the human factor may well be the entry point into the firm's wider systems.

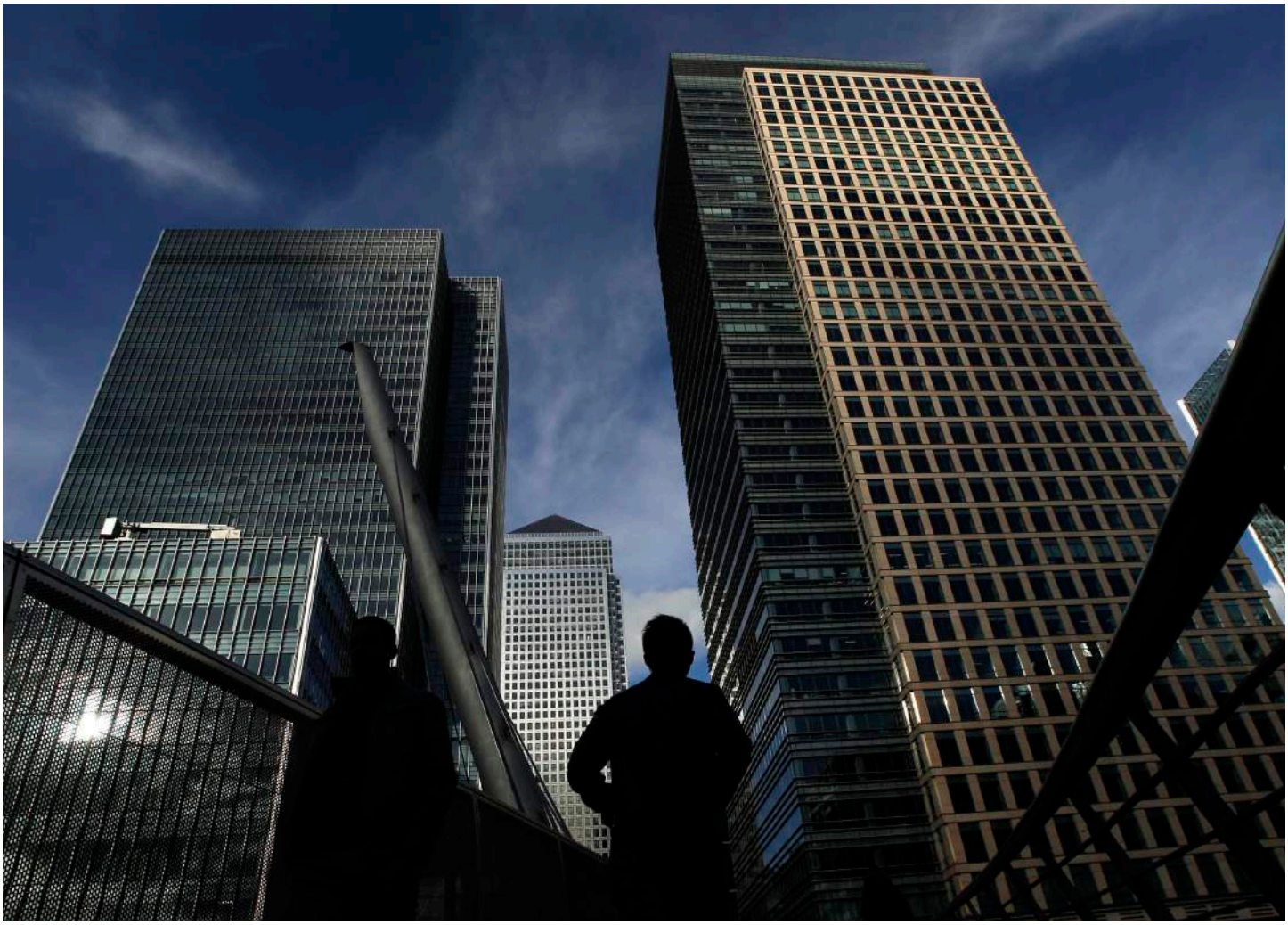
WHAT ARE THE RISKS TO THE FIRM'S INFORMATION AND HOW MUCH RISK IS THE FIRM WILLING TO ACCEPT?

Financial services firms are used to the concept of risk appetites which should, as a matter of course, be extended to all information assets. It is essential that all assessments keep pace with technological advances.

WHAT MEASURES ARE NEEDED?

Management information and reporting is not a one-size-fits-all and must reflect the precise nature and activities of the relevant firm. That said, firms could do worse than to use the document "Ten Steps to Cyber Security" produced in 2012 by a number of UK government bodies including GCHQ. For financial services firms these steps could be applied as follows:

- *Information risk management regime* Establish an effective governance structure and determine the firm's risk appetite, maintain the board's engagement with cyber risk and produce supporting information risk management policies.
- *Home and mobile working* Develop a mobile working policy and train staff to adhere to it, apply the secure baseline build to all devices and protect data both in transit and at rest.
- *User education and awareness* Produce user security policies covering the acceptable and secure use of the firm's systems, establish a staff training program and maintain awareness of cyber risks.
- *Incident management* Establish an incident response and disaster recovery capability, produce and critically test incident management plans and, where needed, include them in recovery and resolution planning or living wills.
- *Managing user privileges* Establish account management processes, monitor user activity, control access to activity and audit logs and ensure the complete removal of access as part of the leaving process.
- *Removable media controls* Develop and implement a policy to control all access to removable media.
- *Monitoring* Establish a thorough monitoring program using external expertise where needed by, for example, employing professional hackers to test system firewalls and other access controls.
- *Secure configuration* Ensure that security patches are applied in a timely manner and that the secure configuration of all relevant systems is maintained and evidenced.
- *Malware protection* Establish and maintain strong anti-malware defenses and ensure continuous scanning for malware across the firm.
- *Network security* Protect networks against external and internal attack, manage the network perimeter and regularly monitor and test all security controls.



REUTERS/Luke MacGregor

DO SECURITY MEASURES WORK?

A fundamental part of cyber resilience is testing to ensure that the measures in place work. Although it is not necessarily something for the compliance function itself to perform, the process does need to ensure that the effectiveness of, and adherence to, the control infrastructure is thoroughly tested, and any gaps or issues followed up. As has been shown on numerous occasions, physical disaster recovery plans may look fine on paper but often they do not work as designed in practice.

Firms also need to consider what they would do if the worst happened and they became victims of a full-blown cyber attack. Carefully thought-through and tested incident management and contingency plans need to be agreed, pre-emptively, at the highest levels of the firm. These should include communication protocols (to media, regulators and customers as well as other stakeholders) and the authority levels needed to invoke disaster or recovery plans (such as, say, the switching of operating systems to a secure back-up location). An inherent part of testing whether planned security measures work is the follow-up investigation to assess any attack and the lessons to be learned.

As regulators focus on the need for consistently good customer outcomes delivered by firms which have strong compliance cultures and a watertight approach to conduct risk, cyber risks have arrived rapidly on firms' risk radars. The compliance function needs to ensure cyber risks are expressly included in the range of risks considered by firms, and that the board is prepared to discuss the actions taken to ensure that all reasonable measures are in place to embed cyber resilience throughout the firm.

CORPORATE GOVERNANCE OF CYBER SECURITY

There is plenty of information on the impact of cyber crime and on its complexity, but little in the way of information that assists companies to align their corporate governance to deal with the threat. Companies in the future will have to give cyber security a more important profile within the organization as, ultimately, it is the board's responsibility.

Boards of directors can no longer afford to outsource the responsibility of this dynamic threat and are going to have to be more responsive to keep pace with developing issues that may affect their organizations. Cyber security governance structure will need to be less IT-centered and more properly aligned with other risk and control functions.

THE INTERNATIONAL THREAT

Cyber crime has developed over the last five years from interfering with systems to now online fraud, industrial espionage, theft of data, destruction of information and disruption of systems. A recent New York State, Department of Financial Services (NYSDFS) report on cyber security in banking said: "Cyber attacks against financial services institutions are becoming more frequent, more sophisticated and more widespread." Three main risks for banks are the need to understand the scope of the threat, industry interconnection and the compliance costs of preparing for an attack.

The International Organization of Securities Commissions (IOSCO) has predicted that the next big financial shock will come from cyber space in pursuit of attacks on financial institutions. It is clear, however, that all business sectors are affected: recently giant UK supermarket chain Tesco had to deactivate more than 2,000 accounts after log-in credentials were hacked and shared online by cyber criminals.

NEED FOR GOVERNANCE ALIGNMENT

The financial world appears more organized than most to deal with the mounting problem. For some time, regulators in all jurisdictions have been emphasizing the need for institutions to become active about cyber resilience. IOSCO has published a report exploring the evolving nature of cyber crime in securities markets, and the threats that it poses. Although cyber crime in securities markets has not had systemic impact so far, it appears that it is evolving in terms of increasing numbers of attacks each year, and more emphasis has been placed on the need for boards to exert leadership and governance to tackle the problem.

The NYSDFS report said that corporate governance for cyber security tended to be highly IT-centered, and that other employees in institutions appeared to be under-represented in the cyber security governance structure: specifically, general counsel, public information and corporate insurance. The report highlighted the need to realign governance in this area to be more inclusive of other disciplines, which would strengthen cyber security and ensure the organization was taking a holistic approach to managing risk.

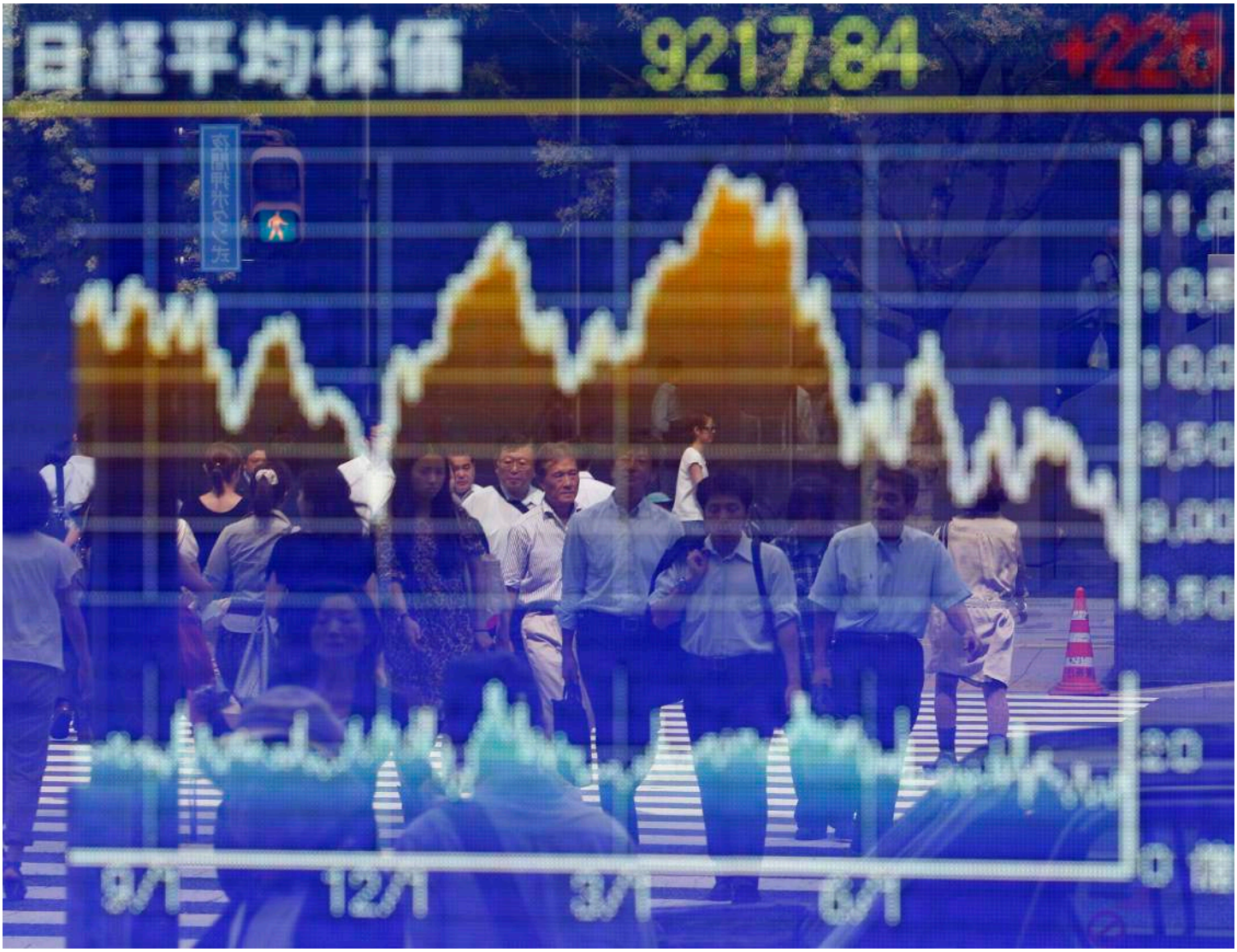
GIVE BOARDS MORE INFORMATION

The report also suggested that, within institutions, boards of directors tended to receive fewer updates about cyber security issues than senior management. More specifically, 73 percent of institutions reported that board members received information security updates only quarterly or annually, whereas 33 percent of institutions reported that senior managers received monthly updates. The report indicated that periodic information security updates should be provided to all levels of management, including boards of directors, to ensure that the institution's cyber risk was appropriately managed. Without these security updates the board and/or the executive management would not fully appreciate the risks involved, and if these risks were not readily apparent they would be less likely to understand why financial resources needed to be diverted to cyber security, the report said.

HOW CAN BOARDS AND EXECUTIVES PLAN FOR THE FUTURE?

The rapid pace of change in technology makes it more crucial than ever that boards of directors and senior managers ensure all functions are aligned and sufficiently resourced. Executive managers need to be more involved in identifying the institution's top cyber risks, and need to understand how the organization can combat them. A sound understanding of cyber protection procedures is essential, so that the board is fully aware of how ready — or otherwise — the institution is to deal with cyber risks. Executive managers should ensure:

- the board has an agreed approach toward the unique risk profile of the organization;
- there is a sound knowledge of IT management and governance throughout the institution, and that all necessary functions are aligned to deal with cyber risks;
- procedures for incident response and event management are in place;
- there is a sound understanding of access controls and network security;
- procedures for vendor management are in place;
- procedures for disaster recovery are in place.



REUTERS/Kim Kyung-Hoon

NEED FOR ORGANIZATIONS TO COOPERATE AND SHARE INFORMATION ABOUT CYBER ATTACKS

Directors can play a crucial leadership role by sharing information about cyber attacks and combining resources with their counterparts at similar organizations to find solutions; more minds are better than one. Attacks are well-publicized, but there is no dynamic information structure to help institutions and businesses to combine and cooperate. This certainly seems to be one of the main obstacles to tackling the problem. The issues are growing year by year, and will eventually become too great for any one organization to deal with, as seen perhaps in the JPMorgan case. If institutions begin to "put their heads together" and share information about cyber attacks and pool resources to find solutions, much could be achieved.

NEED TO REMAIN ALERT

No matter what the issues, executive managers will have to remain on the alert, and must be dynamic in the way that they deal with the risks involved. In time, this may require a new form of institutional governance that is concentrated not so much on getting business in the door but, rather, on saving it.

Boards are going to have to work harder to ensure that the corporate governance structure is fully aligned and that the measures they employ to counter attacks are constantly updated and designed to deal with the risks unique to that particular organization. As time goes on, organizations are likely to move away from the IT-centered model toward a leadership framework that will align all parts of the business to ensure stronger cyber security programs, and to pool resources with other organizations to enable them constantly to assess risks and threats, and to deal with them effectively.

RISK MANAGEMENT SOLUTIONS FROM THOMSON REUTERS

Risk Management Solutions bring together trusted regulatory, customer and pricing data, intuitive software and expert insight and services – an unrivaled combination in the industry that empowers professionals and enterprises to confidently anticipate and act on risks – and make smarter decisions that accelerate business performance.

For more information, visit risk.thomsonreuters.com

THOMSON REUTERS™